

Envio de documentos - FG

2 mensagens

tecnico <tecnico@fgcomercios.com.br>

13 de agosto de 2025 às 14:20

Para: selic.protocolo@gmail.com

Seguem em anexo os documentos que não foram enviados pelo portal para o item 1 da licitação 143/2025, da empresa FG SERVIÇOS E COMERCIO DE EQUIPAMENTOS DE SEGURANÇA E INFORMATICA LTDA.

https://drive.google.com/drive/folders/17jD2WI7Mbz-blCELUUx2rS-_hmYQDFEo?usp=sharing

Secretaria Adjunta de Licitações do Acre <selic.protocolo@gmail.com>

13 de agosto de 2025 às 14:34

Rascunho para: tecnico <tecnico@fgcomercios.com.br>

Recebido.

[Texto das mensagens anteriores oculto]



Genetec ClearID in Security Center SaaS

Click [here](#) for the most recent version of this document.

Document last updated: March 19, 2025

Contents

Legal notices 1

Getting started 2

Logging on to ClearID.	3
Logging off from ClearID.	4
About workflows.	5
Setting up visitor management.	6
Setting up data synchronization.	8

Requirements 10

Firewall ports.	11
Supported devices.	12

Managing identities and users 15

About webhooks.	16
Creating webhooks.	19
Modifying webhooks.	23
Viewing webhook logs.	24
Granting access to the web portal.	27
Granting user access to the web portal.	27
Granting administrator access to the web portal.	29
About access request workflow.	31
About email notifications.	32
Customizing the email banner for sites.	34
About identity request workflow.	36
About custom fields.	37
Modifying custom fields.	38
Custom fields relationships.	41

Managing sites 45

About sites.	46
Creating sites.	47
Adding site owners.	49
Enabling visitor management for sites.	50
Modifying sites.	66
Setting a maximum duration for site access.	68

Managing areas 69

About areas.	70
Creating areas.	71
Adding doors to areas.	74
Enabling visitor management for areas.	75
About nested areas.	76
Granting access to areas automatically.	77

Managing visitors 80

About visit request workflow.	81

About visit request watchlist workflow.	82
Inviting visitors.	83
Inviting visitors manually.	84
Inviting visitors using an imported visitor list.	89
SMS alerts.	95
Reviewing visit events.	98
Copying a visit event.	100
Modifying visit events.	101
QR codes as a credential for visitors.	103
Importing a custom card format (QR code credential) in Synergis.	103
Enabling QR code credentials for visitors.	107
Configuring Qscan devices for ClearID.	109
Configuring STid devices for ClearID.	114

Managing visitor watchlists 136

About watchlists.	137
Adding watchlist managers.	139
Adding watchlists.	141
Adding an individuals watchlist entry.	145
Adding a companies watchlist entry.	148
Importing watchlist entries from a file.	149
Exporting watchlist entries to a file.	151
Testing watchlist entries.	152
Deleting watchlist entries.	154
Modifying watchlists.	156
Deleting watchlists.	158
Screening visitors manually.	160
Unblocking visitors blocked by a watchlist.	164

Synchronizing data 168

Authenticating your connection.	169
Synchronizing identities using an API.	171
About the ClearID API.	171
Synchronizing identities using the SCIM integration.	172
About the SCIM standard.	172
About Microsoft Entra ID attribute fields.	172
Configuring the SCIM integration.	174
Resetting SCIM integration identity data.	188
Reviewing the SCIM integration synchronization status.	189
Synchronizing identities using One Identity.	191
About the One Identity Synchronization Tool.	192
About One Identity Synchronization Tool attribute fields.	195
About the Azure web app.	197
Installing the One Identity Synchronization Tool.	199
Configuring the One Identity Synchronization Tool.	208
Reviewing synchronization status.	236
About One Identity Synchronization Tool logs.	237
Viewing One Identity Synchronization Tool logs.	238
Updating existing identities from an external data source.	239

Self-Service Kiosk 240

About ClearID Self-Service Kiosk.	241
Self-Service Kiosk check-in.	242
Self-Service Kiosk self-registration.	243
Configuring the Self-Service Kiosk iPad.	245
Customizing the Self-Service Kiosk configuration.	247
Customizing the Self-Service Kiosk visitor badge logo.	249
Configuring the Self-Service Kiosk label printer (Brother QL-820NWBc, QL-820NWB, or QL-810W).	251
Configuring the Self-Service Kiosk label printer for Bluetooth mode (Brother QL-820NWBc or QL-820NWB).	252
Configuring the Self-Service Kiosk label printer for Wi-Fi mode (Brother QL-820NWBc, QL-820NWB, or QL-810W).	255
Configuring the Self-Service Kiosk label printer for Ethernet mode (Brother QL-820NWBc or QL-820NWB).	258
Configuring the Self-Service Kiosk label printer (Brother TD-4550DNWB).	260
Configuring the Self-Service Kiosk label printer for Bluetooth mode (Brother TD-4550DNWB).	261
Configuring the Self-Service Kiosk label printer for Wi-Fi mode (Brother TD-4550DNWB).	264
Configuring the Self-Service Kiosk label printer for Ethernet mode (Brother TD-4550DNWB).	267
Selecting a Self-Service Kiosk label printer.	270
Printing a test badge from the Self-Service Kiosk.	276
Resetting the Self-Service Kiosk mobile app.	280
Self-Service Kiosk options.	282
Kiosk floor stand.	284
Kiosk floor stand printer shelf.	288
Kiosk tabletop stand.	290
Identity document types.	293

Troubleshooting 319

Visit email notifications not received by visitors.	320
Visitor hosts fields in Genetec Operation are empty.	321
Connectivity issues (One Identity Synchronization Tool).	324
Data synchronization issues (One Identity Synchronization Tool).	325
Self-Service Kiosk issues.	327
Self-Service Kiosk label printer issues.	330

Legal notices

©2025 Genetec Inc. All rights reserved.

Genetec Inc. distributes this document with software that includes an end-user license agreement and is furnished under license and may be used only in accordance with the terms of the license agreement. The contents of this document are protected under copyright law.

The contents of this guide are furnished for informational use only and are subject to change without notice. Genetec Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

This publication may not be copied, modified, or reproduced in any form or for any purpose, nor can any derivative works be created therefrom without Genetec Inc.'s prior written consent.

Genetec Inc. reserves the right to revise and improve its products as it sees fit. This document describes the state of a product at the time of document's last revision, and may not reflect the product at all times in the future.

In no event shall Genetec Inc. be liable to any person or entity with respect to any loss or damage that is incidental to or consequential upon the instructions found in this document or the computer software and hardware products described herein.

Genetec™, AutoVu™, AutoVu MLC™, Citywise™, Cloud Link Roadrunner™, Community Connect™, Curb Sense™, Federation™, Flexreader™, Genetec Airport Sense™, Genetec Citigraf™, Genetec Clearance™, Genetec ClearID™, Genetec Cloudlink™, Genetec Mission Control™, Genetec Motoscan™, Genetec Patroller™, Genetec Retail Sense™, Genetec Traffic Sense™, KiwiVision™, KiwiSecurity™, Omnicast™, Privacy Protector™, Sipelia™, Stratocast™, Streamvault™, Streamvault Edge™, Synergis™, Valcri™, their respective logos, as well as the Mobius Strip Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.

Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

Patent pending. Genetec™ Security Center, Omnicast™, AutoVu™, Stratocast™, Genetec Citigraf™, Genetec Clearance™, and other Genetec™ products are the subject of pending patent applications, and may be the subject of issued patents, in the United States and in other jurisdictions worldwide.

All specifications are subject to change without notice.

Document information

Document title: Genetec ClearID in Security Center SaaS

Original document number: N/A

Document number: N/A

Document update date: March 19, 2025

You can send your comments, corrections, and suggestions about this guide to documentation@genetec.com.

Getting started

Logging on to ClearID

Log on to your Genetec ClearID™ account to submit visitor or access requests.

Before you begin

- Enable cookies in your web browser.

Procedure

- 1 In your web browser, enter or select the required host.

For example:

- United States: <https://portal.clearid.io/>
- Australia: <https://portal.au.clearid.io/>
- Canada: <https://portal.ca.clearid.io/>
- Europe: <https://portal.eu.clearid.io/>

NOTE: If a corporate log on (single sign-on using Microsoft Office 365 or similar) is used, the account is automatically activated and no activation email is received.

- 2 On the *login* page, enter your *username* and click **Logon**.

You're redirected to your user account's logon page.

- 3 (Optional) Select an account.

- The account ID is shown in the URL of every page.

For example, <https://hostname/accountid/currentpage>.

- The account ID can change depending on the user account that is logged on.

TIP: If you have more than one account, you can switch accounts by clicking **Change account** from the account options under the user ID.

The *My requests* page is displayed and you're ready to use ClearID.



Logging off from ClearID

To exit from Genetec ClearID™, you can log off from your user account.

What you should know

You are logged off from the system automatically after a specified period of inactivity. The inactivity period varies depending on your environment configuration. The default is 30 minutes.

Procedure

- At the top of the page, click your name, and then click **Log off**.

TIP: After you log off from of your account, close all browser windows that were used for ClearID.

About workflows

Genetec ClearID™ uses workflows to process and approve or reject, access, visit, or identity requests.

NOTE: Depending on your site and area configurations, some workflow processes might not apply.

The following workflows are provided to support the different request types:

Access request workflow

An access request workflow is a series of activities performed by the system or authorized people during the life cycle of an access request. The activities can change the state and properties of access requests, affect other entities in the system, or wait for a condition to be met.

Visit request workflow

A visit request workflow is a series of activities performed by the system or authorized people during the life cycle of a visit request. The activities can change the state and properties of visit requests, affect other entities in the system, or wait for conditions to be met.

Visit request watchlist workflow

A watchlist workflow is a series of activities performed by the system or authorized people during the life cycle of a visit request if watchlists are enabled. The activities can change the state and properties of watchlists, affect other entities in the system, or wait for conditions to be met.

Identity request workflow

An identity request workflow is a series of activities performed by the system or authorized people during the life cycle of an identity request. The activities can create an individual identity, or multiple identities using a CSV import, and add each new identity to a role to inherit relevant access for a specified period.

Related Topics

[About access request workflow](#) on page 31

[About visit request workflow](#) on page 81

[About visit request watchlist workflow](#) on page 82

[About identity request workflow](#) on page 36

Setting up visitor management

Setting up visitor management in Genetec ClearID™ involves learning some concepts, planning your sites and areas, and configuring options that are relevant for your organization.

1. Learn about key concepts:
 - [About workflows](#)
 - [About email notifications](#)
2. Review the ClearID requirements:
 - [Firewall ports](#)
 - [Supported devices](#)
3. [Sign in to ClearID.](#)
4. [Grant access to the web portal.](#)
5. Configure and manage your sites:
 - a. [Learn about sites.](#)
 - b. [Create your sites.](#)
 - c. [Add site owners.](#)
 - d. [Enable visitor management for sites.](#)
 - e. [View sites where a user can invite visitors.](#)
 - f. [Set a maximum duration for site access.](#)
 - g. [Customize your sites email banner.](#)
6. Configure and manage your areas:
 - a. [Learn about areas.](#)
 - b. [Create your areas.](#)
 - c. [Add doors to areas.](#)
 - d. [Enable visitor management for areas.](#)
 - e. [Learn about nested areas.](#)
 - f. [Grant access to areas automatically.](#)
7. Manage your visitors:
 - a. [Invite visitors for a site visit or event.](#)
 - b. [Review visit events.](#)
 - c. [Copy a visit event.](#)
8. Set up QR code as a credential for visitors:

If required, customers can use a QR code as a credential for visitors to simplify access to doors, parking entrance barriers, turnstiles, or gated facilities.

 - a. [Learn about QR codes as a credential for visitors.](#)
 - b. [Import the custom card format.](#)
 - c. [Enable QR code credentials for visitors.](#)
 - d. [Configure your Qscan devices for ClearID.](#)
 - e. [Configure your STid devices for ClearID.](#)

9. Screen and manage visiting individuals or companies of interest using watchlists:
 - a. [Learn about watchlists.](#)
 - b. [Add your watchlist managers.](#)
 - c. [Add your watchlists.](#)

TIP: To accelerate your watchlist configuration and setup, you can [import your watchlist entries from a .CSV file.](#)
 - d. [Screen your visitors manually.](#)
 - e. [Unblock visitors blocked by a watchlist.](#)
10. Manage and configure the Genetec ClearID™ Self-Service Kiosk:
 - a. [Learn about the ClearID Self-Service Kiosk.](#)
 - [Self-Service Kiosk check-in](#)
 - [Self-Service Kiosk self-registration](#)
 - b. [Learn about Self-Service Kiosk options.](#)
 - c. [Learn about Identity document types.](#)
 - d. [Configure the Self-Service Kiosk iPad.](#)
 - e. [Configure the Self-Service Kiosk label printer \(Brother QL-820NWBc, QL-820NWB, or QL-810W\).](#)
 - f. [Configure the Self-Service Kiosk label printer \(Brother TD-4550DNWB\).](#)
 - g. [Select a Self-Service Kiosk label printer.](#)
 - h. [Print a test badge from the Self-Service Kiosk.](#)
 - i. [Resetting the Self-Service Kiosk mobile app.](#)
11. (Optional) Troubleshooting information.
 - [Visit email notifications not received by visitors](#) on page 320
 - [Visitor hosts fields in Genetec Operation are empty](#) on page 321
 - [Self-Service Kiosk issues](#)
 - [Self-Service Kiosk label printer issues](#)

Setting up data synchronization

Setting up data synchronization in Genetec ClearID™ involves learning some concepts, configuring the synchronization solution for your identity data, and the webhook integration options that are relevant for your organization.

1. [Review the firewall port requirements.](#)
2. [Sign in to ClearID.](#)
3. [Grant access to the web portal.](#)
4. [Authenticate your non-user system connections to synchronize data or issue API commands.](#)
5. Choose a synchronization solution for your identity data:
 - Synchronize identity attributes using the ClearID API:
 - [Synchronize identities using an API.](#)
 - [Learn about the ClearID API.](#)
 - Synchronize identity attributes using the ClearID SCIM integration:
 - [Synchronize identities using the SCIM Integration.](#)
 - [Learn about the SCIM standard.](#)
 - [Learn about Microsoft Entra ID attribute fields.](#)
 - [Configure the ClearID SCIM integration.](#)
 - [Generate a SCIM key.](#)
 - [Create a Microsoft Azure enterprise application.](#)
 - [Connect your ClearID SCIM integration to Microsoft Azure.](#)
 - [Disable your Microsoft Entra ID groups setting.](#)
 - [Configure your Microsoft Entra ID user settings.](#)
 - [Configure your ClearID SCIM integration synchronization settings.](#)
 - [\(Optional\) Reset your ClearID SCIM integration identity data.](#)
 - [Review the ClearID SCIM integration synchronization status.](#)
 - Synchronize identity attributes using the ClearID One Identity Synchronization Tool:
 - [Synchronize identities using the One Identity Synchronization Tool.](#)
 - [Learn about the One Identity Synchronization Tool.](#)
 - [Learn about the One Identity Synchronization Tool Attribute fields.](#)
 - [Learn about the Azure web app.](#)
 - [Install the One Identity Synchronization Tool.](#)
 - [Configure the One Identity Synchronization Tool.](#)
 - [Review your synchronization status.](#)
 - [Learn about One Identity Synchronization Tool logs.](#)
 - [View the One Identity Synchronization Tool logs.](#)
 - [Update existing identities from an external data source.](#)
6. Configure and manage your webhook integrations:
 - [Learn about webhooks.](#)
 - [Create your webhooks.](#)
 - [Modify your webhooks.](#)
 - [View the webhook logs.](#)

7. (Optional) Troubleshooting information.
 - a. [One Identity Synchronization Tool: Connectivity issues](#)
 - b. [One Identity Synchronization Tool: Data Synchronization issues](#)

Requirements

Firewall ports

To ensure that Genetec ClearID™ works as designed, the following ports, URLs, and network requirements must be met.

ClearID web portal

The following network configuration is required for the web portal:

- TCP Port 443 outbound
- *.clearid.io - Allow all outbound traffic for this domain
- *.core.windows.net - Allow all outbound traffic for this domain
- *.launchdarkly.com - Allow all outbound traffic for this domain

Genetec ClearID One Identity Synchronization Tool

The following network configuration is required for the One Identity Synchronization Tool:

- TCP Port 443 outbound
- *.clearid.io - Allow all outbound traffic for this domain

Genetec ClearID Self-Service Kiosk

The following features or network configuration are required for the Self-Service Kiosk:

- TCP Port 443 outbound
- *.clearid.io - Allow all outbound traffic for this domain
- *.azurewebsites.net - Allow all outbound traffic for this domain
- Label Printer **(Wi-Fi mode only)** Bonjour - used for device search
- Label Printer **(Wi-Fi mode only)** SNMP - used for checking printer status information
- Label Printer **(Wi-Fi mode only)** UDP or TCP Port 9100 - used for sending print data

Other requirements

The following resources are used by ClearID to enhance the user experience, but they aren't mandatory.

Google Maps:

- <https://www.google.com/>
- <https://maps.googleapis.com>
- <https://fonts.googleapis.com/>
- <https://maps.gstatic.com/>

Microsoft Application Insights:

- <https://dc.services.visualstudio.com/>
- <https://dc.applicationinsights.azure.com/>
- <https://dc.applicationinsights.microsoft.com/>

NOTE: These resources don't prevent you from using the ClearID portal. However, some elements of the user interface might not format correctly if these resources are unavailable.

Supported devices

Use this supported devices list to choose hardware devices for Genetec ClearID™ or the Genetec ClearID™ Self-Service Kiosk.

For each device, the corresponding firmware and certification level are listed.

- **Certified:** Genetec Inc. has tested and validated the device.
- **Supported by design:** The device has the same design characteristics as a certified device, but Genetec Inc. has not tested or validated the device.

Kiosk devices

The following iPad devices are supported for use with the ClearID Self-Service Kiosk.

Manufacturer	Model	Device type	Version
Apple	Not applicable	• iPad 10.9 inches¹ • iPad 10.2 inches²	Certified: iOS 16.1 or later

¹ Other iPad devices might also be supported (without kiosk stand) if they are running the Minimum iOS version required for the Kiosk mobile app. For example, the iPad Pro could be used. However, due to the iPad Pro physical dimensions it isn't compatible with the Kiosk stand.

² You can no longer purchase the 10.2 inch iPad or the associated kiosk stand enclosure from us.

For information about iPad power adapter requirements, see **CD-KIOSK-WORLD-ADAPTER-KIT** in [Self-Service Kiosk options](#) on page 282.

Kiosk label printer

The following label printer devices are supported for use with the ClearID Self-Service Kiosk.

Manufacture	Model	Device type	Version
Brother	QL-820NWBc (Network, Wi-Fi, Bluetooth) NOTE: Only DK-2205 or DK2251 (62mm Black or Red and Black) labels are supported for this printer.	Thermal Label Printer	Supported by design
Brother	QL-820NWB (Network, Wi-Fi, Bluetooth) DEPRECATED: You can no longer purchase the QL-820NWB printer from Brother. The QL-820NWBc replaces the discontinued QL-820NWB printer.	Thermal Label Printer	Supported by design
Brother	QL-810W (Wi-Fi only)	Thermal Label Printer	Supported by design
Brother	TD-4550DNWB (Network, Wi-Fi, Bluetooth)	Thermal Label Printer	Supported by design

Manufacture Model	Device type	Version
NOTE: Only RD001U1S (57mm Black) labels are supported for this printer.		

QR code (2d barcode reader) devices

The following Qscan devices are supported for use with ClearID when using QR codes as a credential for visitors. The Zebra device is also supported to simplify looking up visitors in Security Center SaaS.

Manufacturer	Series	Model	Device type	Version
IBC	Qscan	Qscan (for parking lots)	Barcode scanner	Supported by design: Firmware qswie26m.bin
IBC	Qscan	QscanT (for turnstiles)	Barcode scanner	Supported by design
IBC	Qscan	QscanI (indoor version)	Barcode scanner	Supported by design
Zebra	DS9300	DS9308	Barcode scanner	Supported by design

STid OSDP devices

The following STid OSDP devices are supported for use with ClearID when using QR codes as a credential for visitors.

Manufacturer	Series	Model	Part Number	Device type	Version
STid	Architect®	ARC-AQ	SY-ARC-W33-AQPH5-7OS1	QR code reader - Classic Reader - QR Code Module	Supported by design All STid readers Firmware version 10 or later ¹
STid	Architect®	ARC-BQ	SY-ARC-W33-BQPH5-7OS1	QR code reader - Keypad Reader - QR module	Supported by design All STid readers Firmware version 10 or later ¹
STid	Architect® Blue	ARCS-AQ/BT	SY-ARCS-W33-AQBT1-7OS1	QR code reader - Classic reader - Crypto processor - QR Code module	Supported by design All STid readers Firmware version 10 or later ¹

Manufacturer	Series	Model	Part Number	Device type	Version
				Bluetooth	
STid	Architect® Blue	ARCS-BQ/BT	SY-ARCS-W33-BQBT1-7OS1	QR code reader - Keypad reader - Crypto processor - QR Code module - Bluetooth	Supported by design All STid readers Firmware version 10 or later ¹
STid	SECard ² - High security programming kit (Configuration software for the QR code reader)	Not applicable	KIT-SECARD-BT-V3.X	- STid ARC-G USB encoder - USB key containing SECard software	Supported by design Software version 3.5 or later.

STid model codes explained:

- ARCS = Crypto Processor
- AQ = reader + QR code
- BQ = Keypad reader + QR code
- BT = Bluetooth

¹ If you are re-using existing readers, refer to *STid documentation* about how to upgrade your reader to firmware version 10 or later.

IMPORTANT: ² Genetec Inc. does not provide support for the STid SECard solution. Customers require the stand-alone STid SECard software to configure the STid OSDP readers to work with the ClearID ACS panel solution.

Related Topics

[Self-Service Kiosk options](#) on page 282

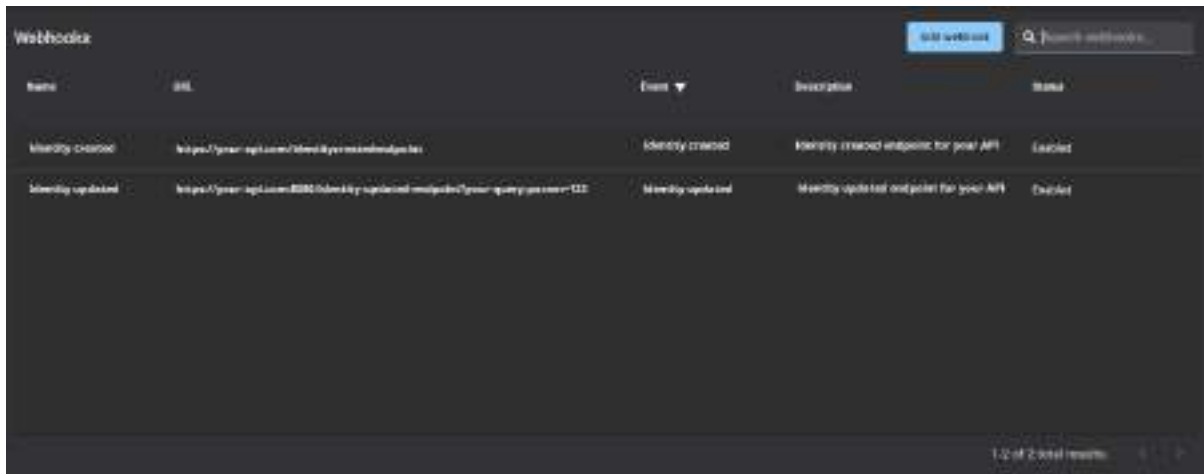
Managing identities and users

About webhooks

A webhook is a user-defined HTTP callback. A webhook can be triggered by an event in a web application and can be used to send data or notifications to a third-party Application Programming Interface (API).

Webhooks in ClearID

In Genetec ClearID™, webhooks can be created and used to notify third-party APIs when specific events occur.



Name	URL	Event	Description	Status
Identity created	https://your-api.com/webhooks/identity-created	Identity created	Identity created endpoint for your API	Enabled
Identity updated	https://your-api.com/webhooks/identity-updated	Identity updated	Identity updated endpoint for your API	Enabled

1/2 of 2 total results

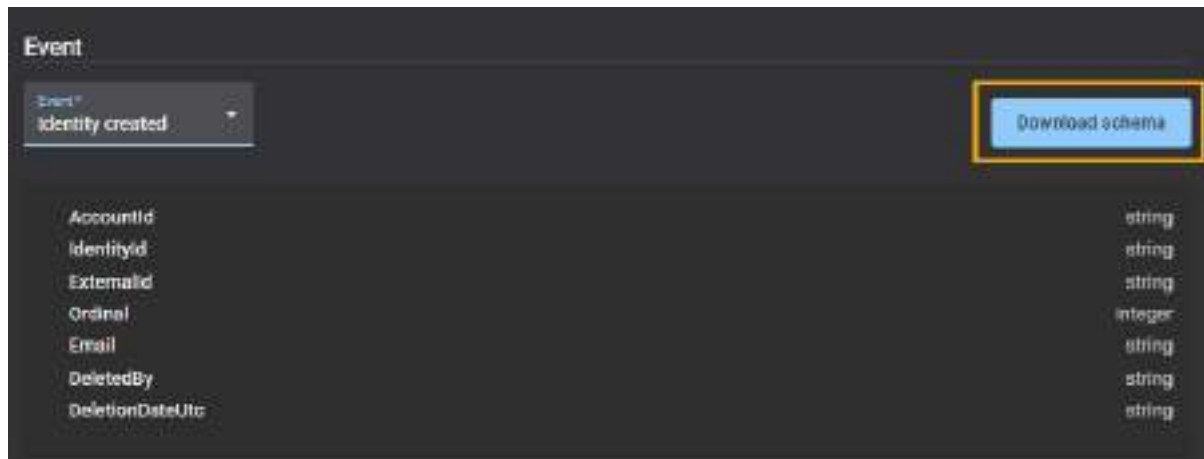
For example, an email notification with a link to detailed information about an identity could be sent when an **Identity updated** event occurs, or if you require other stakeholders to be notified after an **Identity requests created** or **Identity requests updated** event occurs.

Webhook processing

After the webhook is created, the webhook service listens for a subset of specified events coming from other ClearID services. When the specified event occurs, the webhook service notifies the API specified in the *Webhook details* section **URL** field.

Webhook event schemas

The schema describes the object that is sent through the webhook and the contents of the schema vary depending on the event type specified. The webhook event schema can be downloaded from the *Event* section of the webhook to help understand the data structure of the events so that they can be retrieved and processed correctly on the user's side of the webhook integration.



For more information about downloading the schema, see [Creating webhooks](#) on page 19.

Webhook logs

Third-party API owners can use webhook logs to verify the status of every HTTP callback request sent to the third-party URL and to troubleshoot unreceived webhooks or other associated issues. For example, sender issues, receiver issues, and so on.

Webhook logs include the following:

- **Callback date:** When the callback was sent (includes date range filters).
- **URL:** The URL used to forward the webhook event notification to the relevant third-party API (program or application).
- **Response:** The response state indicates whether the third-party API successfully received the HTTP callback or not. For example, accepted, bad request, internal server error, and so on.

Callback date	URL	Response
March 14, 2022 at 1:07 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
March 4, 2022 at 3:56 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
March 4, 2022 at 1:10 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
March 3, 2022 at 10:17 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
March 2, 2022 at 3:57 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
March 2, 2022 at 10:50 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
February 28, 2022 at 4:13 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
February 14, 2022 at 1:16 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
February 11, 2022 at 9:56 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
February 9, 2022 at 10:54 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest

1-10 of 47 total results.

NOTE: The webhook *Logs* section is only displayed at the end of the webhook details after the first callback has occurred.

Creating webhooks

You can create webhooks in Genetec ClearID™ to integrate with third-party solutions APIs so that you can notify interested parties when specific events occur.

Before you begin

[Learn about webhooks.](#)

What you should know

- Only an account administrator can create webhooks in ClearID.
- External organizations are responsible for developing their own third-party solution APIs (programs or applications) that consume ClearID webhook HTTP callback notifications.

Procedure

- 1 From the *Home* page, click **Administration** > **Webhooks**.
- 2 Click **Add webhook**.

The screenshot shows the 'Administration / Webhooks / New' page in the Genetec ClearID interface. The page is dark-themed and contains several sections for configuring a new webhook:

- General**: A toggle switch labeled 'Enabled' is turned on.
- Name**: A text input field.
- Description**: A text input field.
- Webhook details**:
 - URL**: A text input field.
 - Secret**: A text input field.
- Additional headers**: A table with two columns, 'Name' and 'Value'. An 'Add header' button is located to the right of the table. Below the table, it says 'No additional headers found'.
- Event**: A dropdown menu labeled 'Event' with a right-pointing arrow. An 'Event list reference' button is located to the right of the dropdown.

- 3 In the *General* section, complete the fields:
 - a) (Optional) Move the **Enabled** slider to enable or disable the webhook.
NOTE: When the webhook is *disabled*, the HTTP callback doesn't happen.
 - b) In the **Name** field, enter a meaningful Name so that you can easily identify your webhook later on.
For example, **Identity updated** or **Identity requests created webhook** and so on.
 - c) In the **Description** field, enter a Description that describes the purpose of the webhook.
For example, what the webhook is for, and what API (program or application) it notifies when events occur.
- 4 In the *Webhook details* section, complete the fields:
 - a) Enter a valid *HTTPS://* URL for your API (program or application).
URLs can include ports and query parameters as follows:
 - Example 1: *https://my-api.com/identityupdatedendpoint*
 - Example 2: *https://my-api.com:8080/identity-updated-endpoint?my-query-param=123*

This URL is used to forward the webhook event notification to the relevant third-party API (program or application).

NOTE: Your organization is responsible for providing the URL that you want the webhook event notifications forwarded to.
 - b) (Optional) Enter the Secret (App key) if required by the third-party API.
The secret (App key) is used to authenticate communications between the ClearID webhook and your organizations third-party API.

- 5 (Optional) In the *Additional headers* section, complete the fields:

Extra custom HTTP headers can be added in the HTTP callback request so that they can be used by the third-party API on the user's side of the integration.

NOTE: If you enter an invalid or reserved header, the following message is displayed The submitted HTTP request header is invalid or misused.

The screenshot shows the 'Additional headers' interface. At the top, there are two input fields: 'Name' with the value 'Accept' and 'Value' with the value 'json'. To the right of these fields is a blue 'Add header' button. Below the input fields, a red-bordered box contains the error message: 'The submitted HTTP request header is invalid or misused.' Below this, there is a table with two columns: 'Name' and 'Value'. The table is currently empty, with the text 'No additional headers found' at the bottom.

- a) Enter the header parameter Name.

For example, if you had one event coming from multiple sources, extra HTTP request headers could be used to specify where event is coming from (ClearID or external API).

Example:

The screenshot shows the 'Additional headers' interface. At the top, there are two input fields: 'Name' and 'Value'. To the right of these fields is a grey 'Add header' button. Below the input fields, there is a table with two columns: 'Name' and 'Value'. The table contains one row with the value 'Source' in the 'Name' column and 'ClearID' in the 'Value' column. To the right of this row is a red 'X' icon, which is used to remove the header.

- b) Enter the header parameter Value.
- c) (Optional) Click **Add header** to add extra HTTP request headers as required.
- For example, if your API is expecting or requires a specific set of headers (Host, Origin, Language, and so on).
- d) (Optional) Click **X** to remove any headers that are no longer required.

6 In the **Event** section, configure the settings you require:

- a) From the **Event** list, select an event that you want this webhook to listen for.
- b) Click **Download schema** and follow your browser prompts.

BEST PRACTICE: Use the downloaded schema information to understand the data structure of the events so that they can be retrieved and processed correctly on the user's side of the integration.

The following example shows an extract from a *schema-identitycreated.json* file:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "IdentityDeletedCallbackModel",
  "type": "object",
  "additionalProperties": false,
  "required": [
    "AccountId",
    "IdentityId",
    "DeletedBy",
    "DeletionDateUtc"
  ],
  "properties": {
    "AccountId": {
      "type": "string",
      "description": "The account id for which this identity is member of.",
      "minLength": 1
    },
    "IdentityId": {
      "type": "string",
      "description": "A unique id to identify the identity.",
      "minLength": 1
    },
    "ExternalId": {
      "type": [
        "null",
        "string"
      ],
      "description": "External ID"
    },
    "Ordinal": {
      "type": [
        "integer",
        "null"
      ],
      "description": "Commit ordinal in the storage.",
      "format": "int64"
    },
    "Email": {
      "type": [
        "null",
        "string"
      ],
    },
  }
}
```

7 Click **Save**.

Your webhook is now configured to integrate with a third-party API (program or application) to notify interested parties when specific events occur.

After you finish

Using the downloaded schema, configure your third-party API to receive and process the webhook notifications.

Modifying webhooks

After you create your webhooks, you might need to modify the webhook details. You can deactivate or activate a webhook, and modify the webhook details or event type if required.

Before you begin

[Create your webhooks.](#)

What you should know

Only an account administrator can modify webhooks in Genetec ClearID™.

Procedure

- 1 From the *Home* page, click **Administration** > **Webhooks**.
- 2 Select the webhook that you want to modify.
TIP: If the list is long, use the **Search** field to find the webhook that you require.
- 3 In the *General* section, modify the fields as required.
 - a) (Optional) Move the **Enabled** slider to enable or disable the webhook.
NOTE: When the webhook is *disabled*, the HTTP callback doesn't happen.
- 4 In the *Webhook details* section, modify the fields as required:
- 5 (Optional) In the *Additional headers* section, modify the fields as required:
- 6 In the *Event* section, modify the settings as required.
- 7 Click **Save**.

Viewing webhook logs

To troubleshoot unreceived webhooks or other associated issues, third-party Application Programming Interface (API) owners can use the webhook logs to verify the status of every HTTP callback request sent to the third-party URL.

Before you begin

[Create your webhooks.](#)

What you should know

- Only an account administrator or third-party API owner can view webhook logs in Genetec ClearID™.
- The webhook *Logs* section is only displayed at the end of the webhook details after the first callback has occurred.

Procedure

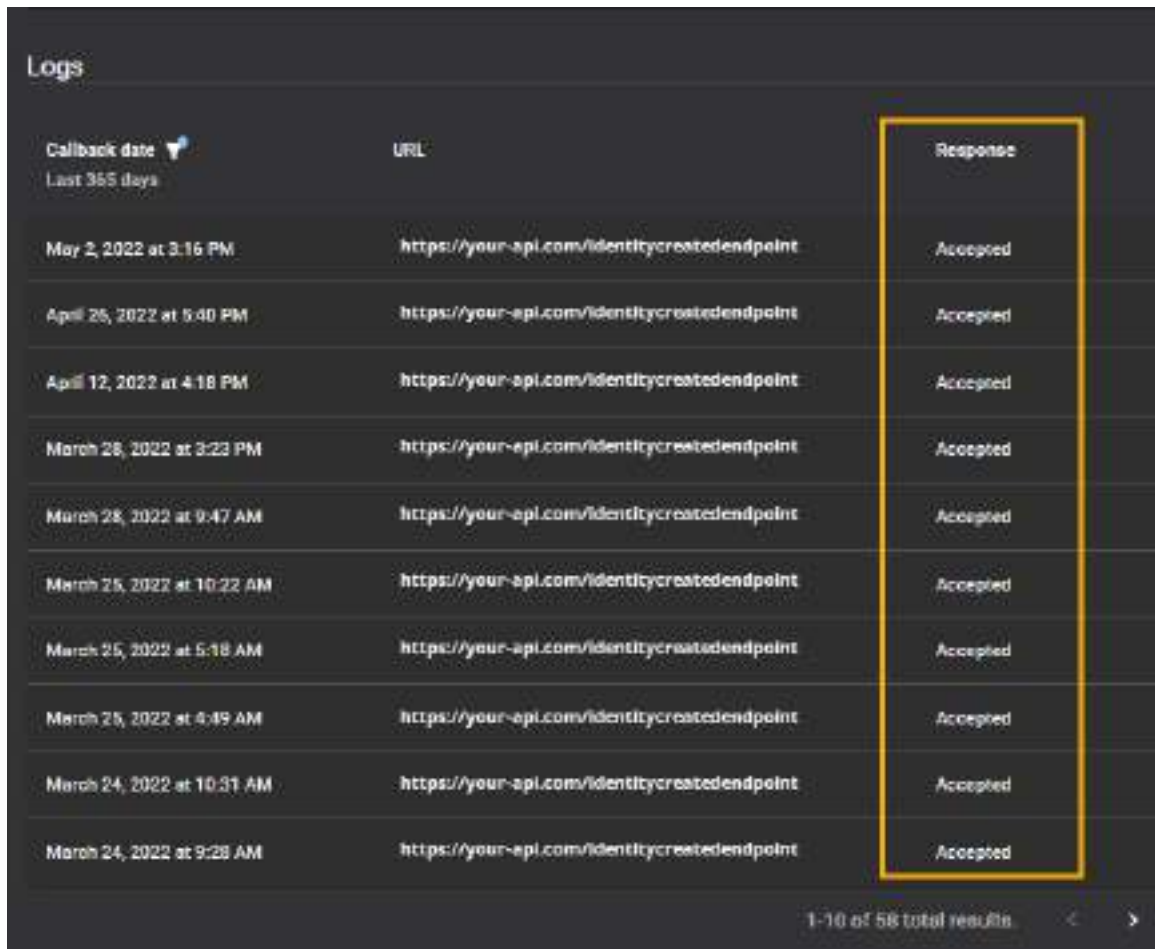
- 1 From the *Home* page, click **Administration > Webhooks**.
- 2 Select the webhook that you want to troubleshoot.

TIP: If the **Webhooks** list is long, you can use the **Search** field to find the webhook that you require.

- 3 In the *Logs* section **Callback date** column, click  to select a specified range or use the **Date range** picker to specify your own range.

NOTE: The callback data range time period is limited to a maximum of 1 year and the callback information is displayed in reverse chronological order.

The following image shows callback logs containing *Accepted* responses.



Callback date  Last 365 days	URL	Response
May 2, 2022 at 3:16 PM	https://your-api.com/identitycreatedendpoint	Accepted
April 26, 2022 at 5:40 PM	https://your-api.com/identitycreatedendpoint	Accepted
April 12, 2022 at 4:18 PM	https://your-api.com/identitycreatedendpoint	Accepted
March 28, 2022 at 3:23 PM	https://your-api.com/identitycreatedendpoint	Accepted
March 28, 2022 at 9:47 AM	https://your-api.com/identitycreatedendpoint	Accepted
March 25, 2022 at 10:22 AM	https://your-api.com/identitycreatedendpoint	Accepted
March 25, 2022 at 5:18 AM	https://your-api.com/identitycreatedendpoint	Accepted
March 25, 2022 at 4:49 AM	https://your-api.com/identitycreatedendpoint	Accepted
March 24, 2022 at 10:31 AM	https://your-api.com/identitycreatedendpoint	Accepted
March 24, 2022 at 9:28 AM	https://your-api.com/identitycreatedendpoint	Accepted

1-10 of 58 total results

The following image shows callback logs containing *BadRequest* responses.

Callback date Last 365 days	URL	Response
March 14, 2022 at 1:07 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
March 4, 2022 at 3:56 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
March 4, 2022 at 1:10 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
March 3, 2022 at 10:17 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
March 2, 2022 at 3:57 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
March 2, 2022 at 10:00 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
February 28, 2022 at 4:13 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
February 14, 2022 at 1:16 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
February 11, 2022 at 9:56 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest
February 9, 2022 at 10:54 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	BadRequest

1-10 of 47 total results.

4 Review the **Logs** information as follows:

- In the **Callback date** column, check when the callback was sent (includes date range filters).
- In the **URL** column, for the URL used to forward the event notification, verify that the specified event occurred and a notification was sent to the relevant third-party API (program or application).
- In the **Response** column, review the states to verify whether the third-party API successfully received the HTTP callback or not. For example, **Accepted**, **BadRequest**, **InternalServerError**, and so on.
- (Optional) Navigate through the callback logs (forwards or backwards in time) by clicking the **Next page** or **Previous page** icons.

Granting access to the web portal

Before a user can access the Genetec ClearID™ web portal, you must grant them the required *User* or *Administrator* permissions for the website.

What you should know

- The identity that you want to grant access to must exist in the system.
- To grant a *User* or an *Administrator* permission to access the website, you must be an account administrator.

Procedure

- Choose one of the following:
 - [Grant user access to the web portal](#)
 - [Grant administrator access to the web portal](#)

The selected identity now has access to the web portal with either **User** or **Administrator** privileges.

After you finish

[Log on to the web portal.](#)

Related Topics

[Viewing sites where a user can invite visitors](#) on page 65

Granting user access to the web portal

Before a user can access the Genetec ClearID™ web portal, you must grant them the required permissions for the website.

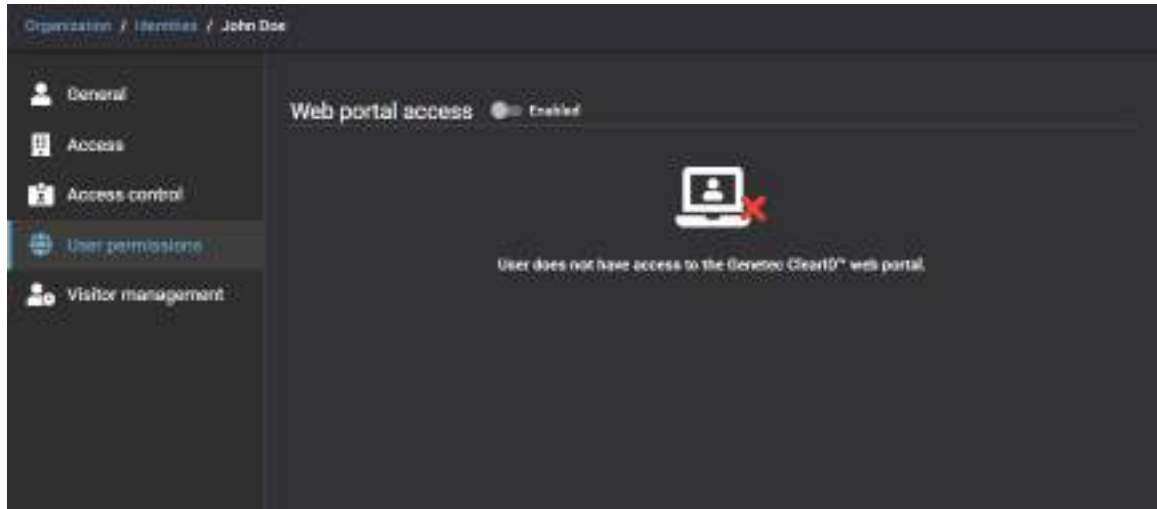
What you should know

- The identity that you want to grant access to must exist in the system.
- To grant a user permission to access the website, you must be an account administrator.
- Some organizations don't enable web portal access for some or all of their identities because their organization does not require employee requests or web portal access.

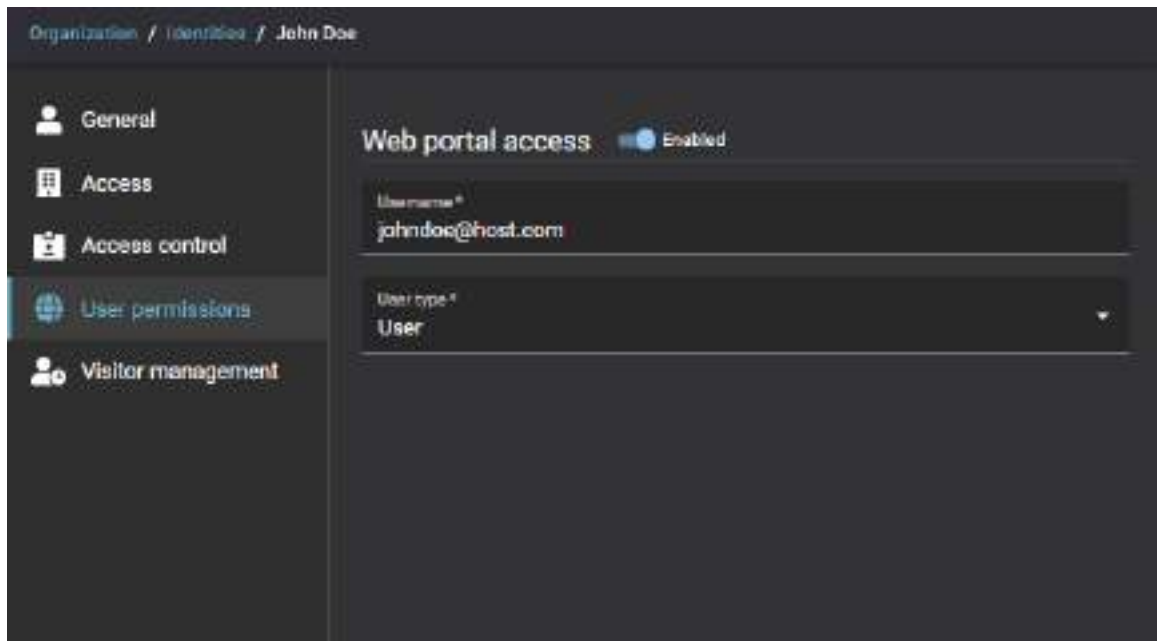
Procedure

- 1 Click **Organization > Identities**.
- 2 Search for a user or select one from the Identities list.

3 Click **User permissions**.



- 4 In the *User permissions* section, click or slide the **Web portal access** slider to **Enabled** to grant access to the web portal.
If the slider is disabled the identity cannot access the web portal.
- 5 In the **Username** field, enter a valid email address.
- 6 In the **User type** list, select **User** for default user access to the web portal.
- 7 Click **Save** to confirm your changes.



The selected identity now has access to the web portal with the default **User** privileges.

Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



After you finish

[Log on to the web portal.](#)

Granting administrator access to the web portal

Before an administrator can access the Genetec ClearID™ web portal, you must grant them the required permissions for the website.

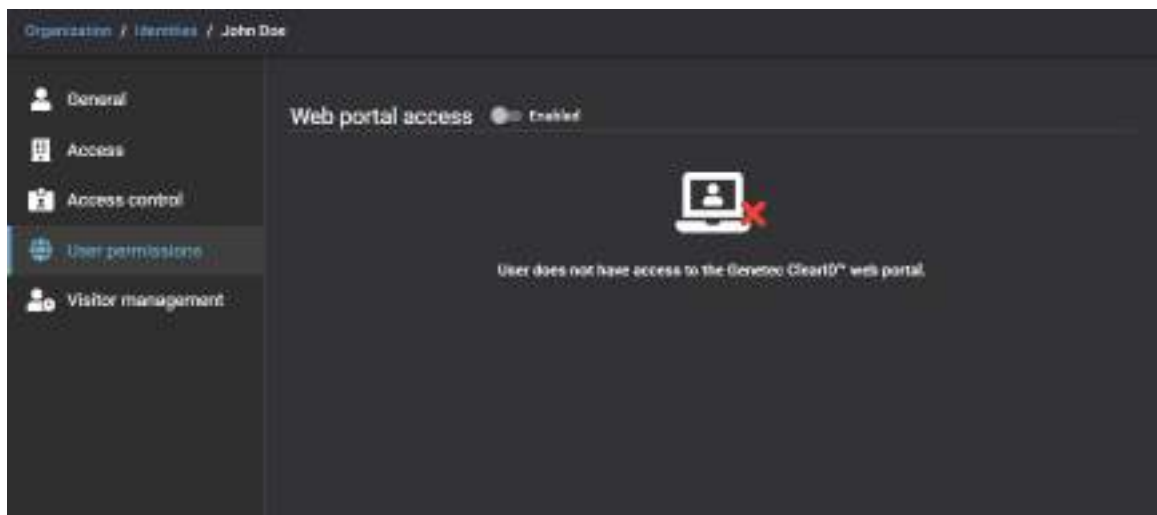
What you should know

- The identity that you want to grant access to must exist in the system.
- To grant an administrator permission to access the website, you must be an account administrator.
- Some organizations don't enable web portal access for some or all of their identities because their organization does not require employee requests or web portal access.

IMPORTANT: When a new account is created, an end user designated as the account administrator receives a [Welcome to Genetec ClearID](#) and a [New ClearID Account - ACCOUNTNAME](#) email notification. By default, Administrator access is given to the end user that receives the email. If a system integrator or other identity also requires administrator access, their administrator access must be added by the end user (account administrator).

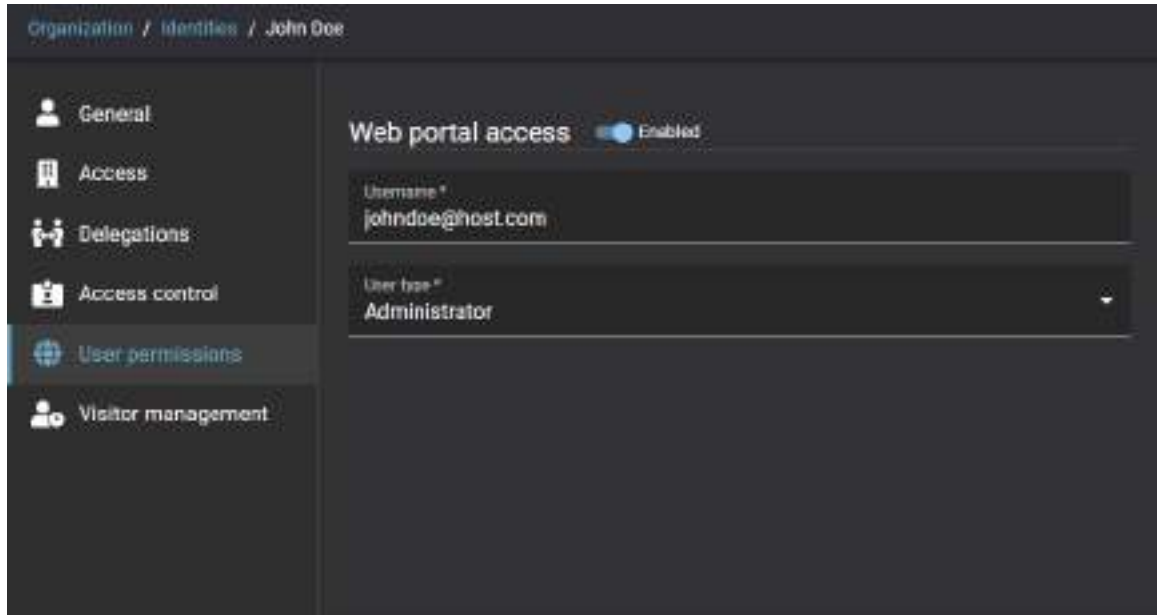
Procedure

- 1 Click **Organization > Identities**.
- 2 Search for a user or select one from the Identities list.
- 3 Click **User permissions**.



- 4 In the *User permissions* section, click or slide the **Web portal access** slider to **Enabled** to grant access to the web portal.
If the slider is disabled the identity cannot access the web portal.
- 5 In the **Username** field, enter a valid email address.
- 6 In the **User type** list, select **Administrator** for Administrator access to the web portal.

- Click **Save** to confirm your changes.



The identity now has access to the web portal with **Administrator** privileges.

Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



After you finish

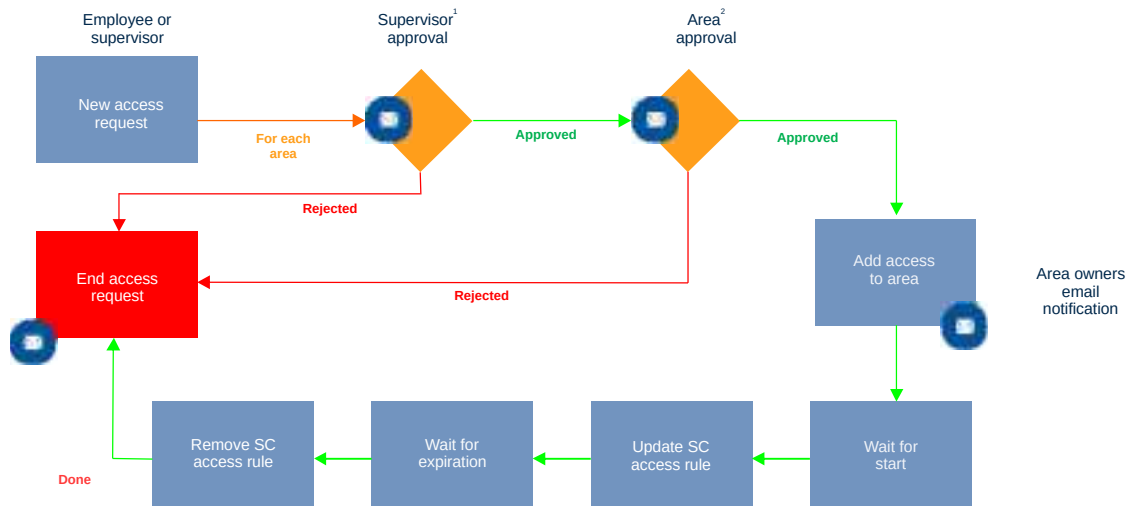
[Log on to the web portal.](#)

About access request workflow

An access request workflow is a series of activities performed by the system or authorized people during the life cycle of an access request. The activities can change the state and properties of access requests, affect other entities in the system, or wait for a condition to be met.

The workflow helps automate tasks like approving or rejecting access requests freeing up time to focus on other tasks.

The following diagram illustrates the access request workflow that occurs in Genetec ClearID™ and Synergis™.



¹ (Optional) Supervisor approval can be enabled for the area.

² (Optional) Area approval can be enabled for the area.

NOTE: By default, access requests are limited to the minimum access required. This minimum access limits what a user can do with an access card.

Related Topics

[About workflows](#) on page 5

About email notifications

To inform users about specific events in the Genetec ClearID™ system, email notifications are sent.

Email notifications are triggered and sent for the following situations:

Email notification	Notification recipients
Access for an identity	
Account is created for an identity ¹	Identity - Administrators only
Area access request for an identity is submitted	Identity requester
Area access request for an identity is canceled	Identity requester, area approvers, and area owners
Area access request for an identity requires approval or deny	Depending on workflow settings: • Supervisor and or area approver • No email if auto approved
Area access request for an identity is approved or denied	Identity and area owners (Submitter and <i>Access for</i> requester if they are different)
Area access for an identity is granted	Identity and their supervisor
Area access for an identity is revoked (or expired) ²	Identity and their supervisor
Access for a role	
Access request submitted for a role	Requester (requester is one of the role managers)
Area access request for a role requires approve or deny	Access request requires an approval or denial from Supervisors: • Denied: All role managers get email Access request requires an approval or denial from Area approvers: • Denied: All role managers get email • Approved: All role managers get email
Area access request for a role is approved or denied	Approved by Supervisor: • Area approvers get email Denied by Supervisor: • All role managers get email
Area access granted for role	After an area approver approves the request or if the area is set to automatically approve: • Sent to all role managers After the role is granted access to an area manually: • Sent to all role managers
Area access revoked for a role	All role managers get email

Email notification	Notification recipients
Identity added to role membership	Identity - notifications are configurable in the role
Identity removed from role membership	Identity - notifications are configurable in the role
Identity requests	
Identity requested	Requester Depending on the approval workflow configured in the identity template: - Supervisors - Identity approver NOTE: If one of the requested identities is canceled, all the configured approvers are added to the cc list for the email notification titled: "Identity request for <i>identity</i> has been updated".
Visit events	
Visit created	Requester and hosts
Visit requires approve or deny	Depending on workflow settings: - Supervisors - No email if auto approved
Visit approved or denied	Requester and hosts
Visitor confirmation	Visitors get an email if their visit is approved
Visit request requires approve or deny	Depending on the visitor management workflow for each setting in each area: - Area or visit approvers for all areas listed in visit - No email if auto approved
Visitor checked-in	Hosts
Visitor watchlist alert (notify or block)	If a <i>person of interest</i> or <i>company of interest</i> from the watchlist is triggered Watchlist manager
Access reviews	
Access review pending	Area approver and role manager

IMPORTANT: ¹ If a corporate log on (single sign-on using Microsoft Office 365 or similar) is used, the account is automatically activated and no activation email is received.

² Access expired emails are sent at midnight based on the time zone specified for the site.

Email notifications are sent from noreply@clearid.io. If you don't receive email notifications in either your Inbox or Spam (Junk) folders, contact your account administrator.

Customizing the email banner for sites

You can customize the email banner image that is used for access requests and visitor requests email notifications sent for the site.

Before you begin

[Configuring the Self-Service Kiosk iPad](#) on page 245

TIP: Ensure that your email banner image meets the requirements described in the  tooltip on the **Images** page of the Genetec ClearID™ web portal.

What you should know

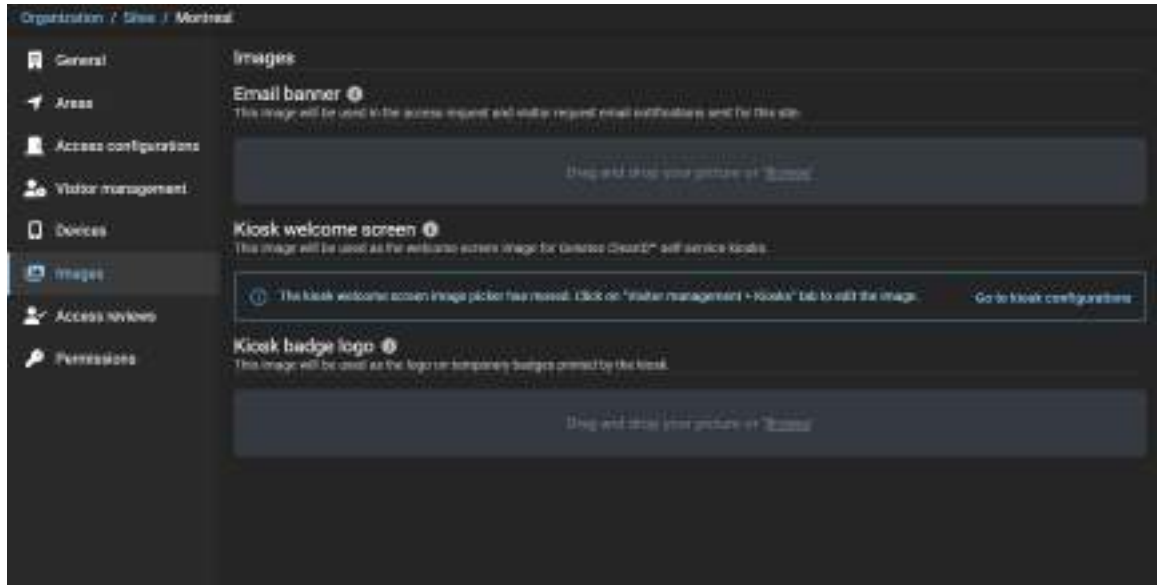
Only a site owner or account administrator can customize email banners.

- Customized email banner changes are synchronized with your site every 60 seconds.

BEST PRACTICE: For optimum results, use transparent *.PNG* images when customizing your email banner.

Procedure

- 1 In the ClearID web portal, click **Organization > Sites**.
- 2 Search for and select a site.

3 Click **Images**.

- In the *Email banner* section, drag and drop your picture or browse to select the **Email banner** image.
- Click **Save**.

The following example shows an email banner with a custom image.

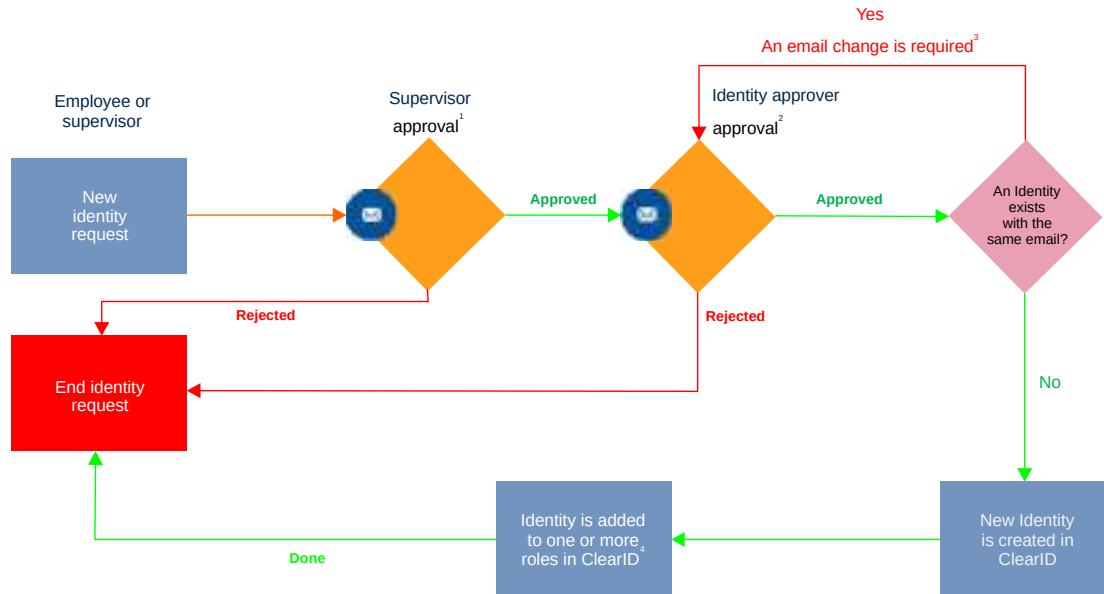


About identity request workflow

An identity request workflow is a series of activities performed by the system or authorized people during the life cycle of an identity request. The activities can create an individual identity, or multiple identities using a CSV import, and add each new identity to a role to inherit relevant access for a specified period.

The workflow helps automate tasks like approving or rejecting identity requests freeing up time to focus on other tasks.

The following diagram illustrates the *identity request workflow* that occurs in Genetec ClearID™.



¹ (Optional) Supervisor approval can be enabled and disabled for each identity template.

² (Optional) Identity approver approval can be enabled and disabled for each identity template.

³ (Optional) Email address must be unique in the system.

⁴ (Only if applicable) Cardholder is added to corresponding cardholder group in Security Center SaaS.

Related Topics

[About workflows](#) on page 5

About custom fields

A custom field is a user-defined property associated with an entity type. Custom fields are useful for storing additional information.

In Security Center SaaS, Genetec ClearID™ uses custom fields for visitors, credentials, and cardholders. The group name **ClearID** identifies the custom fields associated with ClearID, and can be found in the **Group name/Priority** column.

IMPORTANT: ClearID custom fields should be used as read-only fields. ClearID populates and manages the custom field values. If you have existing custom fields, and the name and entity type matches the ClearID custom fields, ClearID uses the existing custom fields. Ensure that any custom fields you create do not match ClearID custom fields, otherwise your data in Security Center SaaS can be overwritten during synchronization.

You can see the complete list for your organization in Genetec™ Configuration desktop. In the *System* task, click **General settings** > **Custom fields**.

[illegible]

NOTE: Only users with the privilege to *Modify custom field definitions* can view custom fields.

Modifying custom fields

You can modify Genetec ClearID™ custom fields in Genetec™ Configuration desktop so that they are displayed to specific groups or users. For example, you might display visit reason, registration code, expected arrival, and expected departure to a group that contains your security team or building reception team.

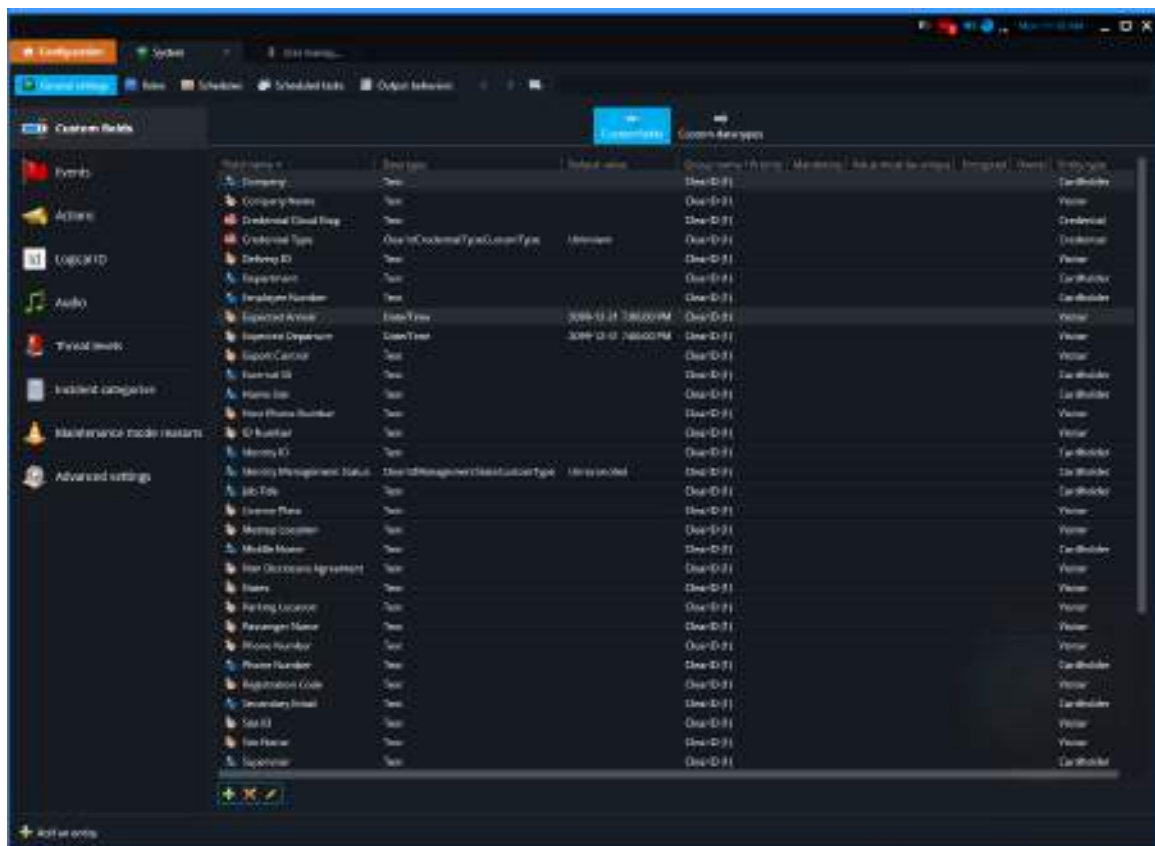
What you should know

Only users with the privilege to *Modify custom field definitions* can view custom fields.

- At least one identity must have been synchronized before any custom fields are displayed.

Procedure

- In Genetec Configuration desktop, Open the *System* task.
- Click **Custom fields**.



- In the **Custom fields** tab, double-click a **Field name** to select the custom field that you want to modify.

4 In the *Edit custom field* dialog, make any changes that you require.

a) In the *Definition* section, make any changes that you require.

IMPORTANT: Do not select the **Mandatory** checkbox for custom fields. In ClearID, custom fields must not be mandatory or unique otherwise synchronization issues can occur.

The screenshot shows the 'Edit custom field' dialog box. The 'Definition' section contains the following fields: 'Entry type' (Visitor), 'Data type' (DateTime), 'Name' (Expected Arrival), and 'Default value' (2099-12-31 07:00:00 PM). The 'Mandatory' checkbox is highlighted with a yellow box and is unchecked. The 'Encrypted' checkbox is also unchecked. The 'Layout (Optional)' section contains 'Group name' (ClearID) and 'Priority' (1). The 'Security' section shows 'Visible to administrators and' checked, with 'Genetec Receptionists' listed as a user group. At the bottom, there are 'Cancel' and 'Save and close' buttons.

b) In the *Layout* section, make any changes that you require.

For example, you could add a group name to categorize your custom fields. Alternatively, you could remove a custom field from a group when a grouping is no longer applicable.

c) In the *Security* section, make any changes that you require.

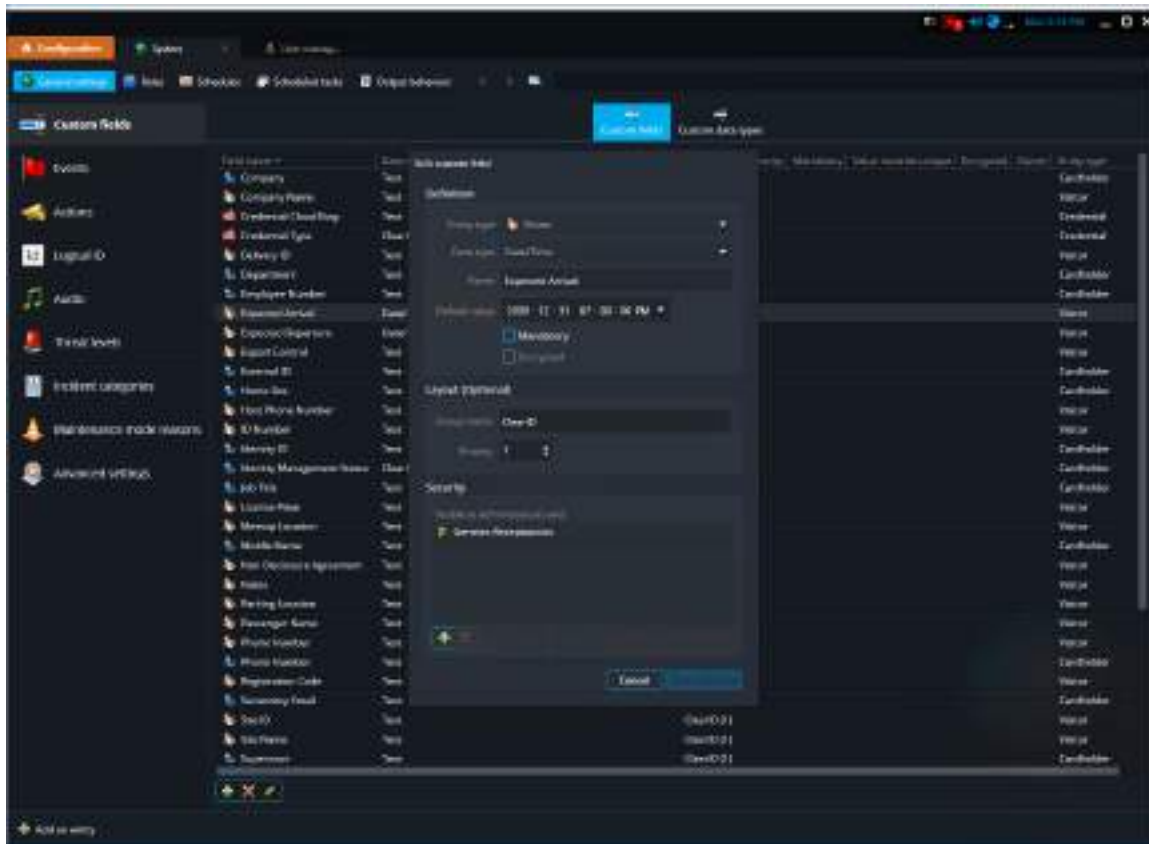
For example, you might add users or user groups in the *Security* section so that the custom field is displayed to them.

For more information about *user groups* or *custom fields*, see "Creating user groups" or "About custom fields" in the *Security Center Administrator Guide*.

d) Click **Save and close**.

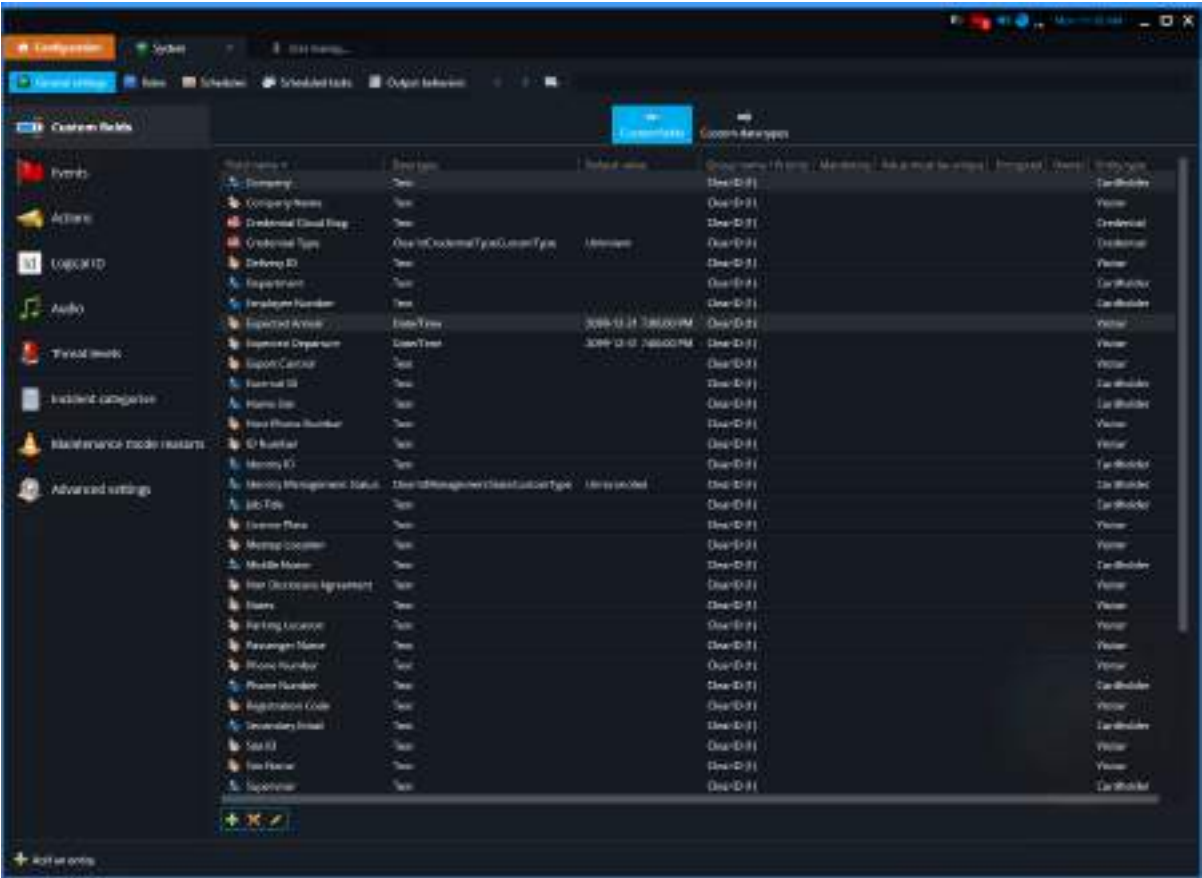
Example

The following example shows the *Expected arrival* custom field. Using the *Security* section of the *Edit custom field* dialog, the **Genetec Receptionists** user group has been added so that the *Expected arrival* custom field can be displayed to members of the group.



Custom fields relationships

Use the following custom fields information to understand the relationship between Genetec ClearID™ identity field names and Security Center SaaS entity type fields.



Cardholder fields

Cardholder fields are used to synchronize cardholder information with an identity in ClearID.

Field name	Data type	Default value	Group name (And Priority)
Company	Text		ClearID (1)
Department	Text		ClearID (1)
Employee Number	Text		ClearID (1)
External ID	Text		ClearID (1)
Home Site	Text		ClearID (1)
Identity ID	Text		ClearID (1)
Identity Management Status	ClearIdManagementStateCustomType	Unreconciled	ClearID (1)

Field name	Data type	Default value	Group name (And Priority)
Job Title	Text		ClearID (1)
Middle Name	Text		ClearID (1)
Phone Number	Text		ClearID (1)
Secondary Email	Text		ClearID (1)
Supervisor	Text		ClearID (1)
Worker Type Code	Text		ClearID (1)
Worker Type Description	Text		ClearID (1)

Cardholder group fields

Cardholder group fields are used to synchronize cardholder group information with a role in ClearID.

- The **Team ID** represents the role ID in ClearID.
- The **Team Management Status** indicates whether ClearID is managing cardholders and credentials or not (managed by ClearID, not managed by ClearID, deleted by ClearID, or unreconciled).

Field name	Data type	Default value	Group name (And Priority)
Team ID	Text		ClearID (1)
Team Management Status	ClearIdManagementStateCustomType	Unreconciled	ClearID (1)

Credential fields

Credential fields are used by ClearID to keep the credentials up to date.

Field name	Data type	Default value	Group name (And Priority)
Credential Cloud Etag	Text		ClearID (1)
Credential Type	ClearIdCredentialTypeCustomType	Unknown	ClearID (1)

Visitor fields

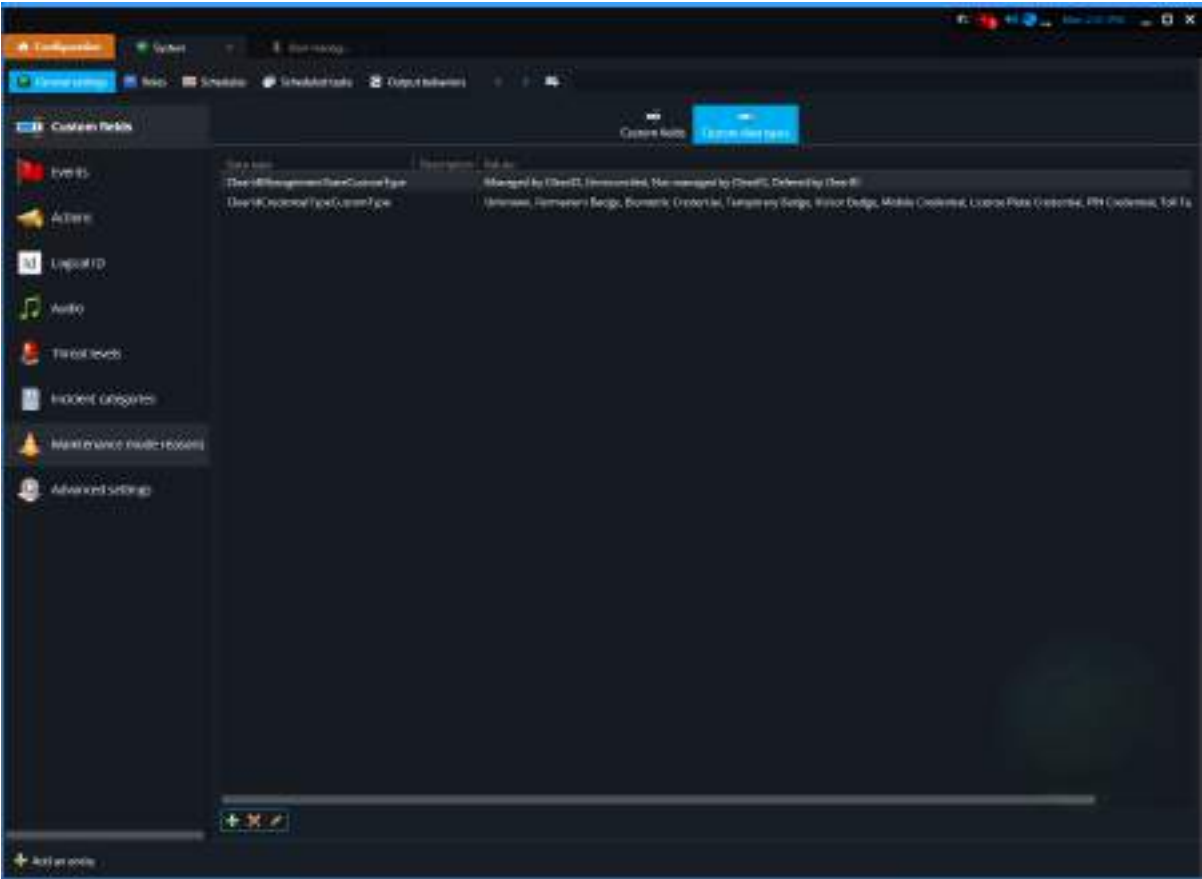
These visitor fields are used to synchronize visitor information.

Field name	Data type	Default value	Group name (And Priority)
Company Name	Text		ClearID (1)
Expected Arrival	Date and time	12/31/2099 7:00:00 PM	ClearID (1)

Field name	Data type	Default value	Group name (And Priority)
Expected Departure	Date and time	12/31/2099 7:00:00 PM	ClearID (1)
Export Control	Text		ClearID (1)
Host Phone Number	Text		ClearID (1)
Meetup Location	Text		ClearID (1)
Non Disclosure Agreement	Text		ClearID (1)
Notes	Text		ClearID (1)
Parking Location	Text		ClearID (1)
Registration Code	Text		ClearID (1)
Site ID	Text		ClearID (1)
Site Name	Text		ClearID (1)
Visit Event Name	Text		ClearID (1)
Visit Reason	Text		ClearID (1)
Visitor ID	Text		ClearID (1)
Watchlist Status	Text		ClearID (1)

Custom data types

Custom data types are used for some custom fields to define the accepted values associated with the data types.



NOTE: All custom fields are labels used to define a property associated with a Security Center SaaS entity type that might be useful to an organization. The fields included in the description here are merely descriptive labels. All the custom data types might not be applicable to or used by ClearID.

Data type	Values
ClearIdManagementStateCustomType	Managed by ClearID, Unreconciled, Not managed by ClearID, Deleted by ClearID
ClearIdCredentialTypeCustomType	Unknown, Permanent Badge, Biometric Credential, Temporary Badge, Visitor Badge, Mobile Credential, License Plate Credential, Pin Credential, Toll Tag, QR Code

Managing sites

About sites

In Genetec ClearID™, a site is a logical entity. Sites include one or more areas. Each site and area can have a different owner.

A site typically represents either a building or a campus:

- If you have multiple buildings managed by one security team or one set of policies for visitors, consider setting them up using one site.
- Each site can have its own set of policies and site owners.
- If you have different buildings spread throughout a city, consider implementing one site per building.
- Multiple sites can be associated with the same Security Center SaaS access control system.

IMPORTANT: Your implementation choices can affect the Genetec ClearID™ solution costs.

Creating sites

Before you can configure your areas in Genetec ClearID™, you must create the sites that you want to associate your areas with.

What you should know

To create sites in ClearID, you must be an account administrator.

- An account administrator can choose the site owners and configure visitor management for the site.
- A *site* is associated with a Security Center SaaS access control system.
- Multiple sites can be associated with the same Security Center SaaS access control system.

Procedure

- 1 Click **Organization > Sites**.
- 2 Click **Add site**.

- 3 In the *General* section, complete the fields.

NOTE: Mandatory fields are highlighted in the user interface with an asterisk (*).

- **Name:** Enter a name for your site.
- **Description:** Enter a description that indicates the geographical location of the building or physical location of the site.
- **Access control system:** Select the system that you require from the **Access control system** list.

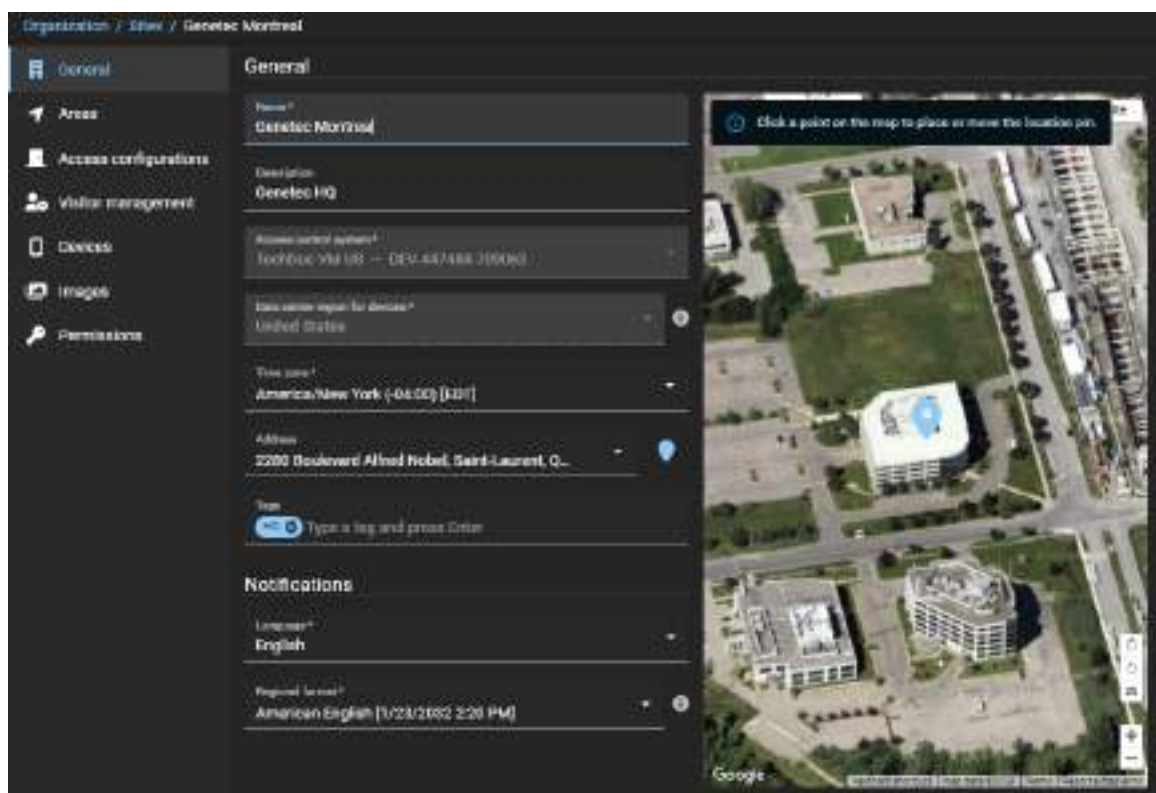
NOTE: This access control system is used to synchronize changes in ClearID back to Security Center SaaS.

- **Data center region for devices:** Select a data center region from the drop-down. This option is typically set to the geographical location of your system or where you want your data stored.
NOTE: The data center option isn't available if your account is deployed in the Europe only architecture.
- **Time zone:** Select a time zone from the drop-down. The time zone options are represented using the Internet Assigned Numbers Authority (IANA) format.
NOTE: When you submit an access request or visitor request from anywhere in the world, the time zone of the requested site access or visit is used to ensure that the date and times are correctly applied to the request.
- **Address:** Enter an address for the site. As you type, Google Maps integration auto-complete processes the information and displays available addresses.
 - **Center map:** Click  to find the address on the map, and center the map on that address.
- **Tags:** Enter alternative keywords or search term categorizations that might be used to find the site.

4 In the *Notifications* section, complete the fields.

- **Language:** Select a notification language from the drop-down. This setting is used for email notifications and SMS alerts. The notifications language selection is unique to a site and you can choose from English, French, Spanish, Portuguese, Italian, German, Dutch, and Japanese.
- **Regional format:** Select a regional date and time format to use in email notifications for this site. The default regional format is American English (en-us). For example, 1/23/2032 2:20 PM.

5 Click **Save**.



Organization / Sites / Genetec Montreal

General

Name* Genetec Montreal

Description Genetec HQ

Access control system* Techdocs vM 10 - DEV-447488-20X06

Data center region for devices* United States

Time zone* America/New York (-04:00) [EST]

Address 2200 Boulevard Alfred Nobel, Saint-Laurent, Q...

Map  Click a point on this map to place or move the location pin.

Tags  Type a tag and press Enter

Notifications

Language* English

Regional format* American English [1/23/2032 2:20 PM]

Your site has been created in ClearID.

Name	Address	Description	Access control system
Bore	2255 Boulevard Alfred Nobel, Saint-La...		TechDoc VM US
Bistro	2255 Boulevard Alfred Nobel, Saint-La...	This is our Bistro.	TechDoc VM Europe
Genetec Albert Einstein	Rue Albert Einstein, Saint-Laurent, QC...	Genetec Building 2	TechDoc VM US
Genetec Alfred Nobel	2255 Alfred Nobel		TechDoc VM Europe
Genetec BAH3	2255 Alfred Nobel	description	TechDoc VM Europe
Genetec Head Office	2255 Boulevard Alfred Nobel, Saint-La...	Head Office	TechDoc VM US
Genetec Head Office	2255 Boulevard Alfred Nobel, Saint-La...		TechDoc VM Europe
Genetec Montreal	2255 Boulevard Alfred Nobel, Saint-La...	Genetec HQ	TechDoc VM US

After you finish

[Add your site owners.](#)

Related Topics

[Modifying sites](#) on page 66

[IANA Time Zone Database](#)

Adding site owners

In Genetec ClearID™, a site owner is an identity that has authority over areas associated with a specific site. Before you can assign or modify area owners, configure specific area settings that are exclusive to site owners, or manage site access reviews you must add your site owners.

Before you begin

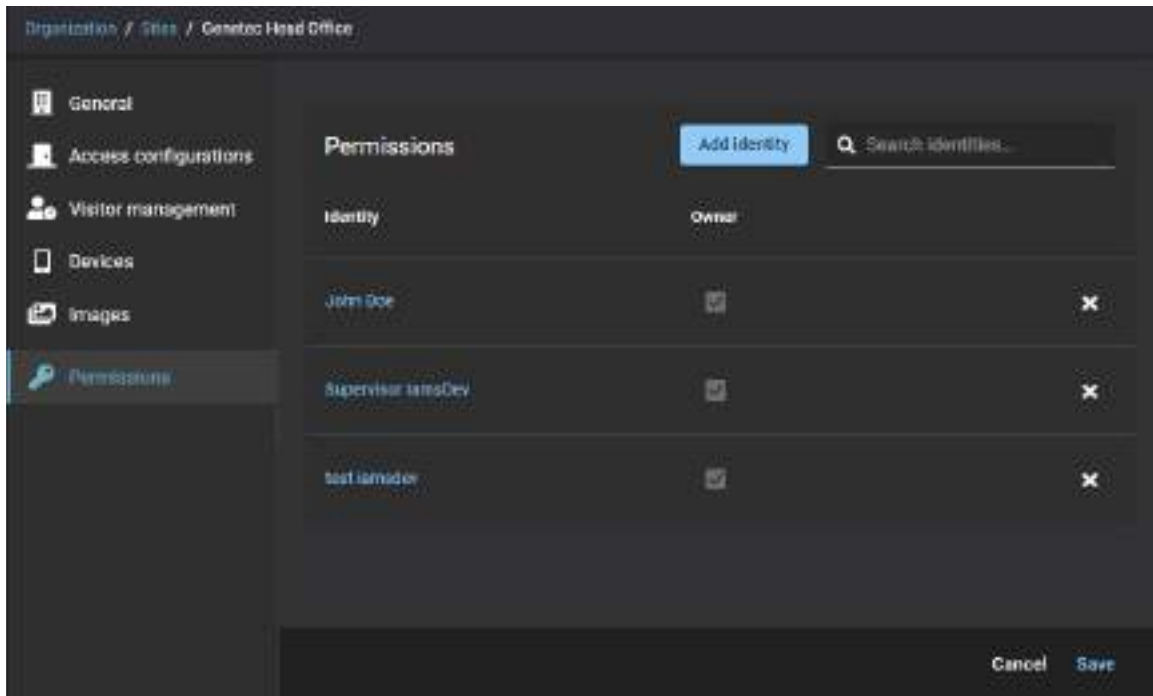
[Create your sites.](#)

What you should know

To add site owners in ClearID, you must be an account administrator.

Procedure

- 1 Click **Organization** > **Sites**.
- 2 Select your site and click **Permissions**.
- 3 Click **Add identity** to add site owners to the site **Permissions** list.



- a) Search for or select the identities that you require and click **Add**.
TIP: Click the identity hyperlink in the **Identity** column to review identity details (company, department, home site, supervisor, and email) and to verify that you have the correct identities in the list.
- 4 Select or clear the checkboxes next to the identities to assign the permissions that you require.
 - a)
 - 5 (Optional) Click  to remove all permissions from an identity when they are no longer required.
 - 6 Click **Save**.

Enabling visitor management for sites

Before users can invite visitors, you must configure the visitor management settings for your site.

Before you begin

[Create your sites.](#)

What you should know

- Visitor management is disabled by default.
- Only account administrators or *site owners* can enable or configure visitor management for sites in Genetec ClearID™.
- The options displayed when a visit request is created vary depending on the users requesting access and also the settings that you configure here.
- Only account administrators can grant user permissions to invite visitors using roles.
- Users are automatically granted *Invite visitors* permissions for their home site by default.

Procedure

- 1 Click **Organization > Sites**.
- 2 Search for and select a site.
- 3 Click **Visitor management** to configure the visitor management options for a site.
- 4 Click the **Settings** tab.

The screenshot shows the 'Visitor management' settings for a site named 'Genetec Albert Einstein'. The interface is divided into two main sections: 'Basic' and 'Advanced'.

Basic section:

- Enable visitor management for this site:** A checkbox that is checked.
- Site name displayed to visitors:** A text field containing 'Genetec Albert Einstein'.
- Check-out:** A section with two options:
 - Automatic check-out time:** A dropdown menu set to 'Automatic check-out on the last day of the visit at the end of day'.
 - Grace period:** A section with two input fields: '00' for hours and '00' for minutes.

Advanced section:

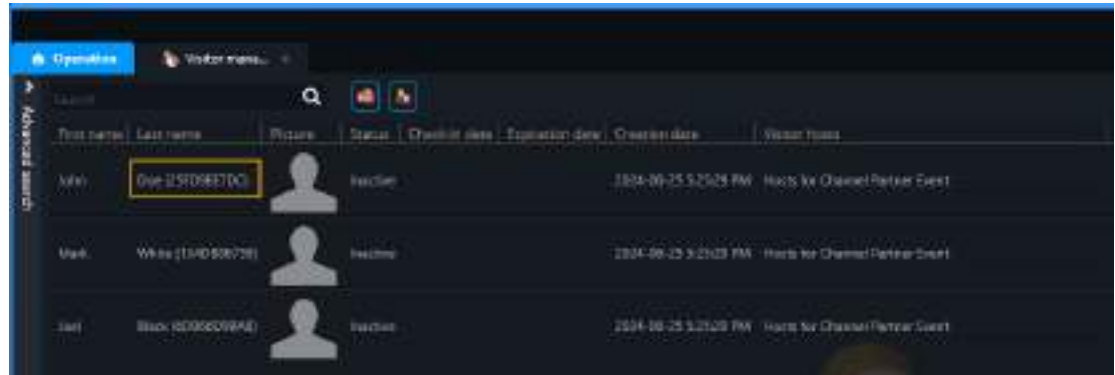
- Visit event approval workflow:** A dropdown menu set to 'No approval required'.
- Visitor escort requirement:** A dropdown menu set to 'Visitor badge without escort'.
- Users can only invite guests to visit areas that user has access to:** An unchecked checkbox.
- Automatically create QR code credentials for visitors:** An unchecked checkbox.
- Display registration code in visitor last name field (Visitor management task in Security Desk):** A checked checkbox.

- In the *Basic* section, configure the options you require:
 - Enable visitor management for this site:** Select this checkbox to enable visitor management for this site.
 - Site name displayed to visitors:** Enter the site name that you want displayed externally to visitors.
- In the *Check-out* section, configure the options you require:
 - Automatic check-out time:**
 - Automatic check-out on the last day of the visit at the end of the day:** The visitor is checked out automatically on the last day of the visit at midnight.
 - Automatic check-out at the scheduled visit end time:** The visitor is checked out at the specified visit end time.
Visitor's temporary access rights and QR code credential are deactivated during automatic check-out. If a grace period is activated, visitors are checked out after the additional grace period lapses after the visit end time.
 - Grace period:** Adds extra time to the scheduled end time of the visit event. After the grace period lapses, the visitor is checked out.
- (Optional) In the *Advanced* section, configure the options you require:
 - Visit event approval workflow:** Select the approval workflow that you require:

- **No approval required:** No approval is required to complete visit event approval. For example, to simplify employees inviting visitors at any time.
- **Supervisor approval required:** Supervisor approval is required to complete visit event approval.
- **Visit event approver approval required:** Visit event approver approval is required to complete visit event approval.
NOTE: If an area is selected during the visit event creation, it can trigger its own approval workflow.
- **Visit escort requirement:** Select the badge type that you require:
 - **Visitor badge without escort:** Typically used for visitors who don't require an escort and who don't need door access to secure or sensitive areas.
 - **Visitor badge with escort:** Typically used for visitors who do require an escort or who need door access to secure or sensitive areas.
NOTE: The **visitor escort rule** must also be turned on for the areas in Synergis™ to enforce the visitor escort rule. For the escort function to work properly, the **Cardholder groups can escort visitors** option must also be enabled in the **General settings** of the *Access control* task in Genetec™ Configuration desktop.
- **Users can only invite guests to visit areas that they have access to:**
 - If the checkbox is selected, users can only invite guests to visit areas that the requesting user has access to. This setting is enforced when a guest visit request is created.
 - If the checkbox is cleared, users can invite guests to visit any area in ClearID that allows visitors.
- **Automatically create QR code credentials for visitors:** If the checkbox is selected, ClearID automatically creates a QR code credential for visitors when a visit request is created. Visitors can then use the QR code contained in the visitor confirmation email to access specific parking entrances, turnstiles, or gated facilities. The QR code can also be used during check-in with security, at a reception, or at a Genetec ClearID™ Self-Service Kiosk.
- **Display registration code in visitor last name field (Visitor management task in Genetec™ Operation desktop):**

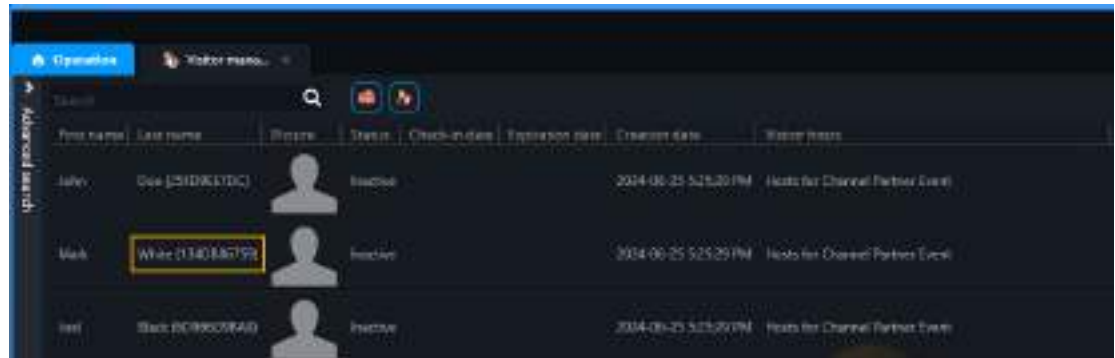
- If the checkbox is selected, the last name field displays the last name of the visitor and the QR code value. This checkbox is selected by default.

The checkbox must be selected for a QR code scanner to successfully scan and locate a pre-registered visitor in Genetec Operation desktop.



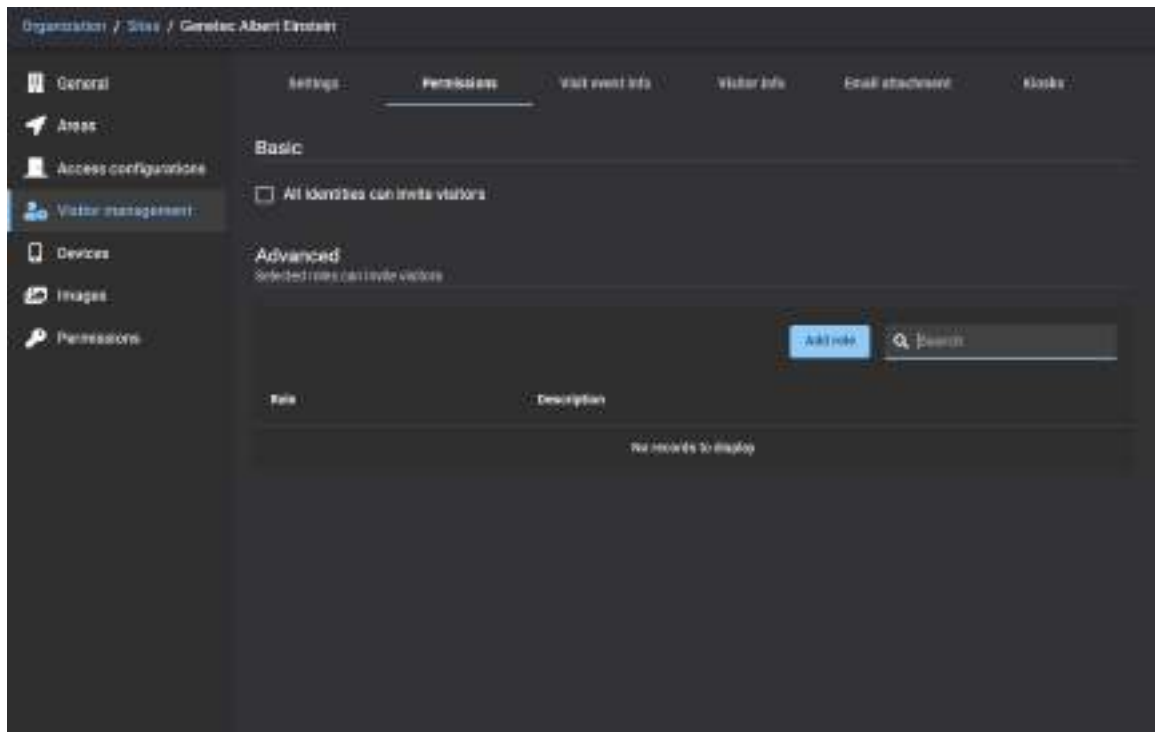
TIP: You can use a Zebra QR code scanner to enter the QR code in the **Last name** field for you. In the *Visitor management* task in Genetec Operation desktop, click in the **Search** field, scan the QR code and press **Enter**.

- If the checkbox is cleared, the last name field displays only the last name of the visitor.



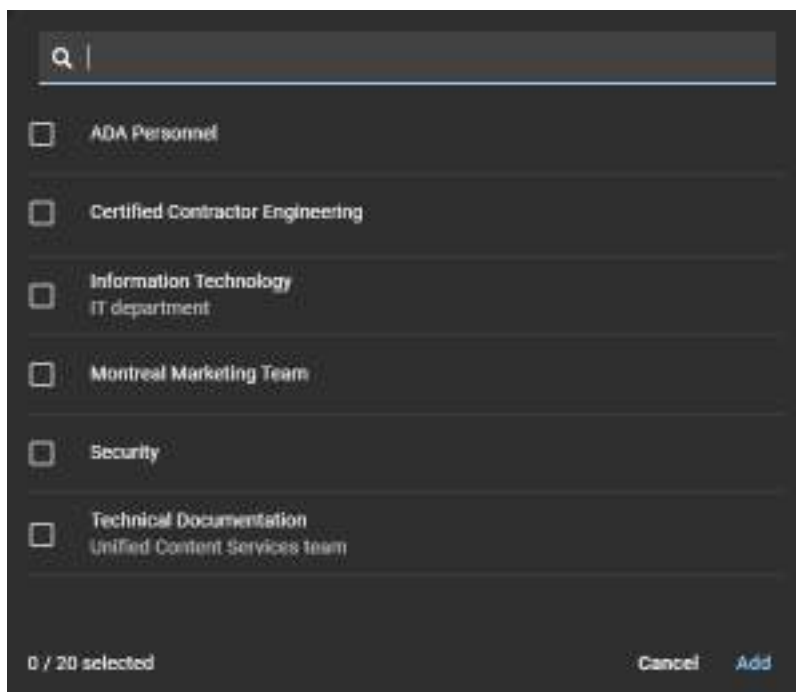
NOTE: When the registration code option is changed, only visitors created after the change are modified, previously created visitors remain unchanged.

- 5 (Optional) Click the **Permissions** tab.



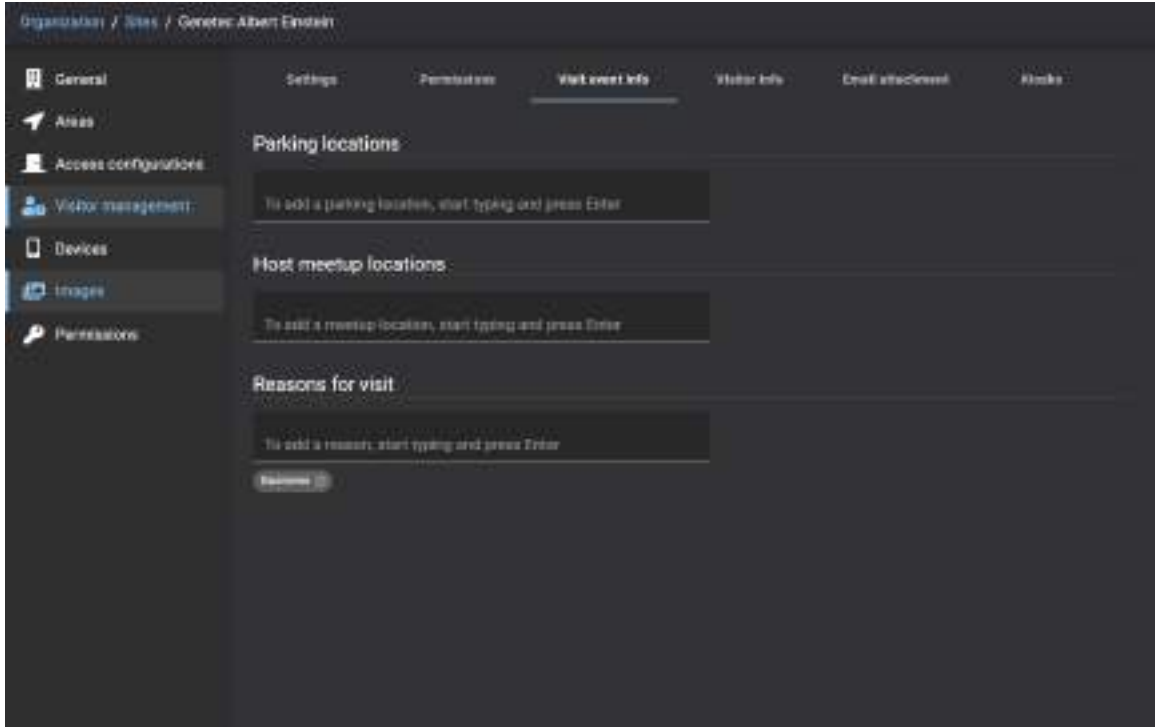
Do one of the following:

- In the *Basic* section, select the **All identities can invite visitors** checkbox if you want all identities to be able to invite visitors to this site.
- In the *Advanced* section, click **Add role** if you want to use roles to manage who can invite visitors to this site. You can then search for or select the roles that you require and click **Add**.



TIP: When adding new role permissions, advise role members to sign out and sign in, if they want to load the new visitor invite permissions immediately.

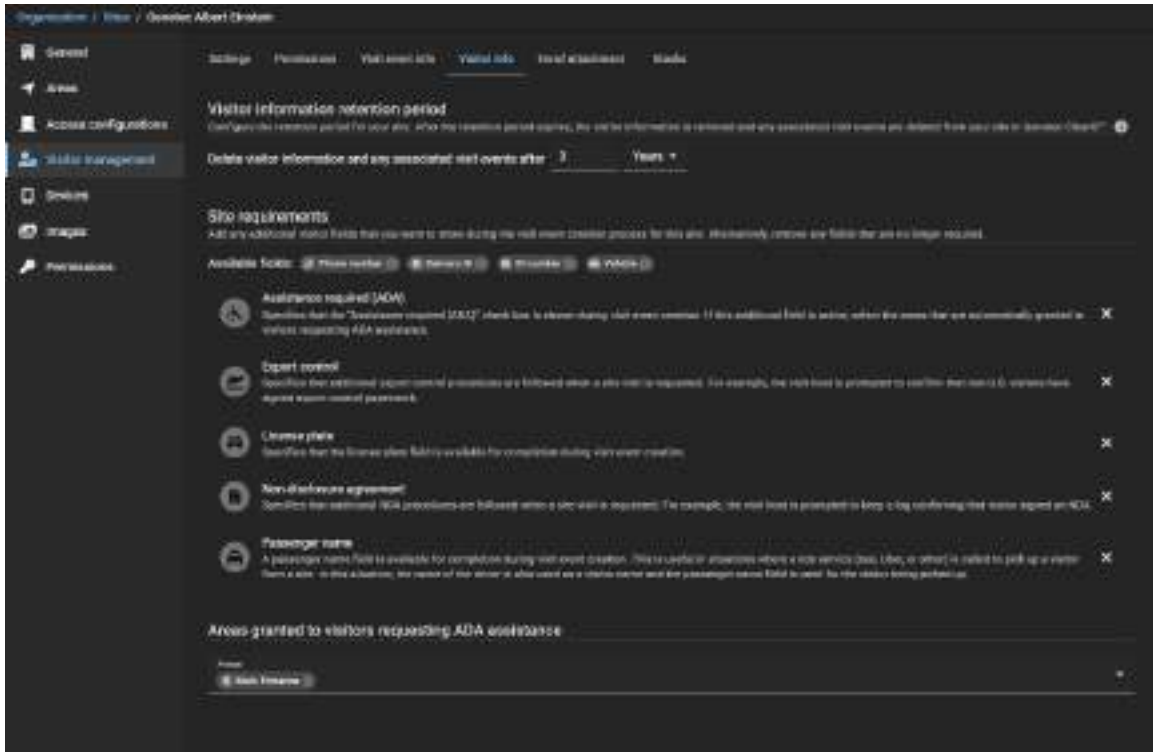
- 6 (Optional) Click the **Visit event info** tab and configure the options you require:



The screenshot shows the Genetec ClearID interface for configuring a site. The left sidebar contains a menu with options: General, Areas, Access configurations, Visitor management (highlighted), Devices, Images, and Permissions. The main content area has a breadcrumb trail: Organization / Sites / Genetec Albert Einstein. Below this is a tabbed interface with tabs for Settings, Permissions, Visit event info (selected), Visitor info, Email attachment, and Roles. The 'Visit event info' tab is active, displaying three sections: 'Parking locations', 'Host meetup locations', and 'Reasons for visit'. Each section has a text input field with a placeholder 'To add a [location], start typing and press Enter' and an 'Enter' button. The 'Reasons for visit' section also includes a 'Remove' button.

- In the *Parking locations* section, add parking locations.
- In the *Host meetup locations* section, add meetup locations.
- In the *Reasons for visit* section, add the typical reasons for visits to your site.
For example, customer meeting, partner meeting, job interview, delivery, taxi pickup, Uber pickup, lift pickup, and so on.

- 7 (Optional) Click the **Visitor info** tab and configure the options you require:



- a) In the *Visitor information retention period* section, select a retention period in days, months, or years. The default retention period is 1 year and the maximum is 3 years.
- NOTE:** You can configure the retention period for each individual site to comply with the different data laws that might apply in your region.
- b) In the *Site requirements Available fields* section, click  to add each additional field that you want to include during the visit event creation process for your site.

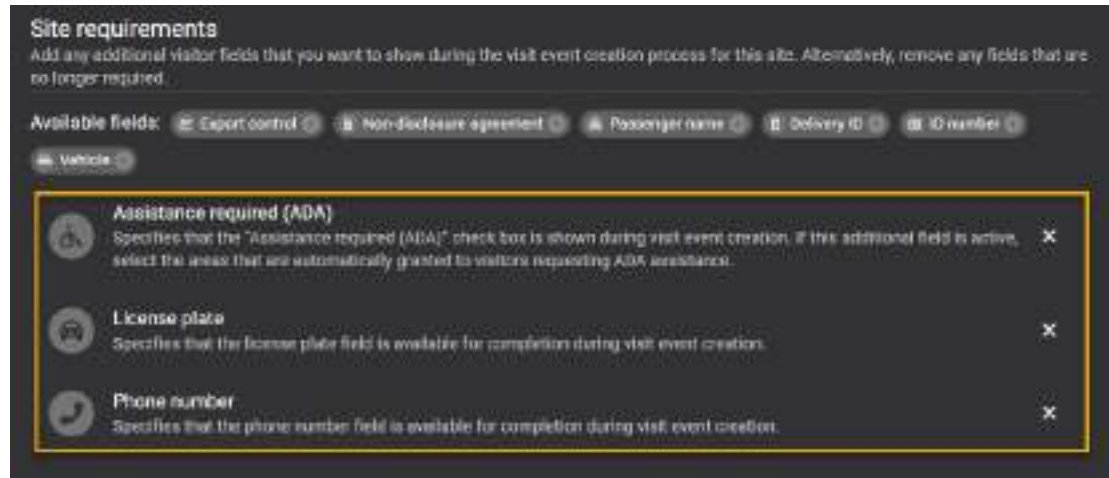


- **License plate:** If selected, a license plate field is provided when a site visit is requested.
- **Phone number:** If selected, a phone number field is provided when a site visit is requested.
- **Assistance required (ADA):** If selected, an *Areas granted to visitors requesting ADA assistance* section is displayed.
NOTE: This assistance option is used to comply with the Americans with Disabilities Act (ADA).
- **Export control required:** If selected, extra export control procedures are followed when a site visit is requested. For example, the visit host is prompted to confirm that non-U.S. visitors have signed export control paperwork.
- **Non-disclosure agreement:** If selected, extra NDA procedures are followed when a site visit is requested. For example, the visit host is prompted to keep a log confirming that the visitor signed an NDA.
- **Passenger name:** If selected, a passenger name field is provided when a site visit is requested. This passenger name field is useful in situations where a ride service (taxi, Uber, or other) is called to

pick up a visitor from a site. In this situation, the name of the driver is also used as a visitor name and the passenger name field is used for the visitor being picked up.

- **Delivery ID:** If selected, a delivery ID field is provided when a site visit is requested.
- **ID number:** If selected, an ID number field is provided when a site visit is requested.
- **Vehicle:** If selected, an extra expected vehicle details field is provided when a site visit is requested.

NOTE: As fields are added, they are displayed in the *Available fields* later in the section.



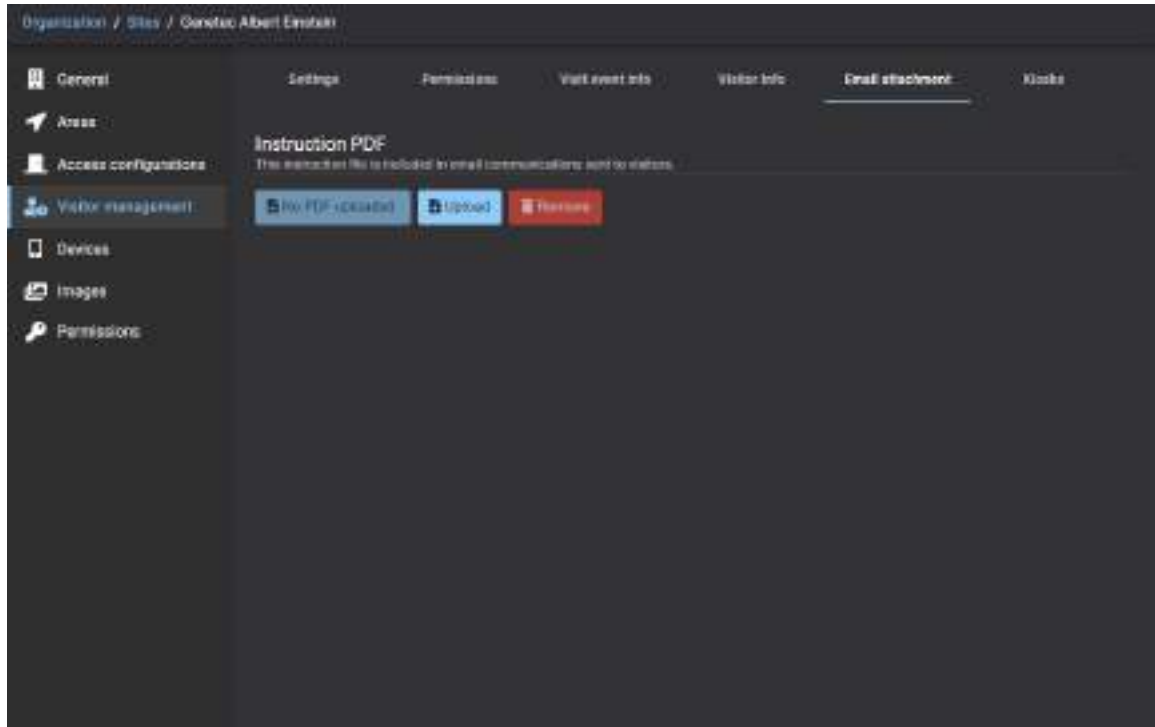
- c) (Optional) If you added **Assistance required (ADA)** to your site requirements, in the *Areas granted to visitors requesting ADA assistance* section, add areas that should automatically be granted to visitors requesting ADA assistance.

NOTE: When an employee invites a visitor that requires accessibility assistance to the site, the visitor is automatically added to the list of ADA areas.

For example, If there's a special door for wheelchair access, the people responsible for the site or facilities add that door for wheelchair access in a specific area and then add the area to the list of areas granted to visitors that request ADA assistance. If a visitor checks in with ADA enabled, ClearID grants the visitor access to this door, but not other visitors.

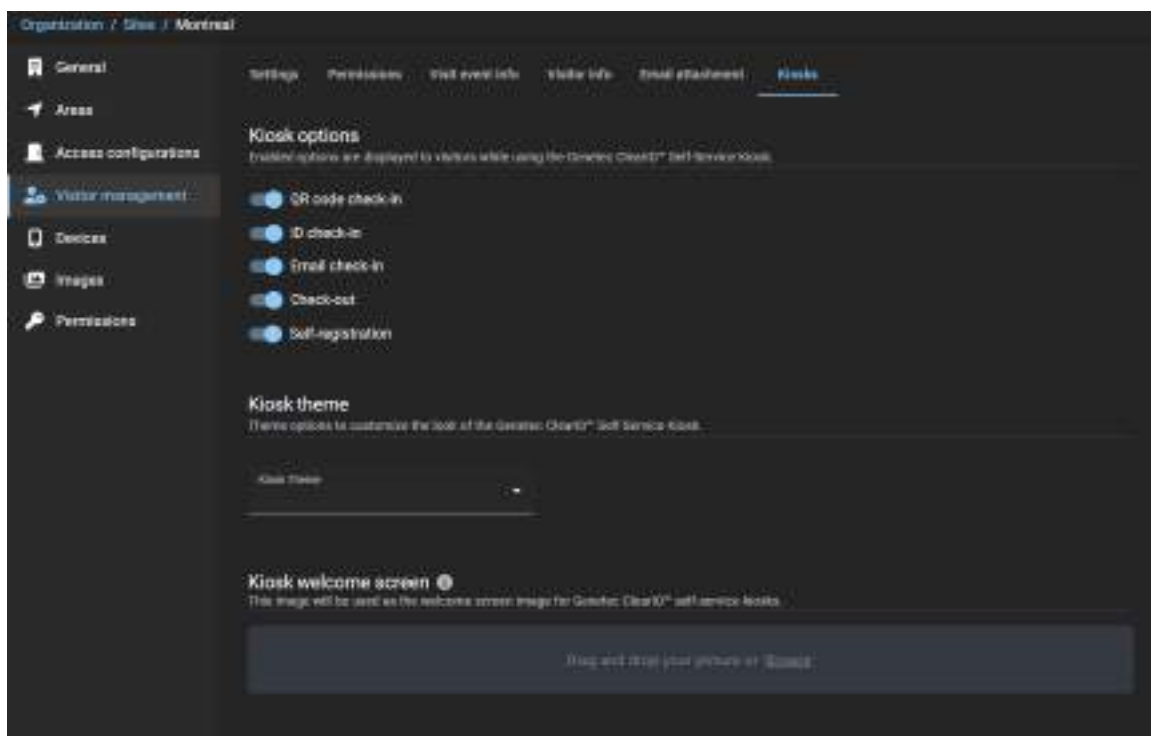
- d) (Optional) Click  to remove any visitor fields that are no longer required.

- 8 Click the **Email attachment** tab and select the options you require:



- **Instruction PDF:** This instruction file is used if you want to automatically include a Visit Instructions File PDF in email communications with visitors. For example, location details, site map, travel instructions, and so on. Regardless of the uploaded file name, the downloadable instruction file is saved as *VisitInstructionsFile.pdf*.
 - **No PDF uploaded:** A PDF instruction file hasn't been uploaded yet.
 - **VisitInstructionsFile.pdf:** Click to download a copy of the *VisitInstructionsFile.pdf*.
NOTE: This button is only visible and active after an Instruction PDF has been uploaded.
 - **Upload:** Click to upload a PDF instruction file.
BEST PRACTICE: If your instruction file is a word document, click **Save as Adobe PDF** before uploading to ensure that visitors can't modify the procedure.
 - **Remove:** Click to remove a Visit Instructions File PDF from email communications with visitors.

- 9 Click the **Kiosks** tab to customize your kiosk configuration.

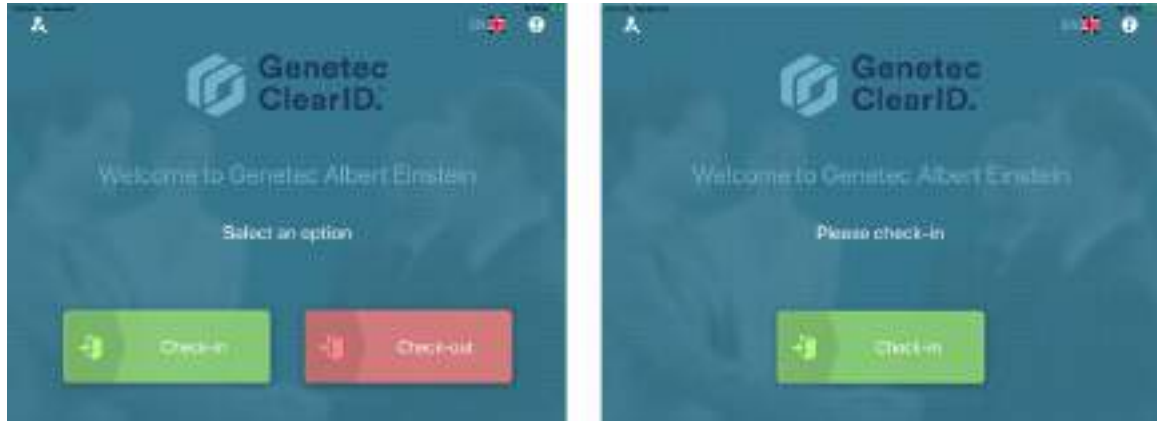


10 (Optional) Customize the **Kiosk options**.

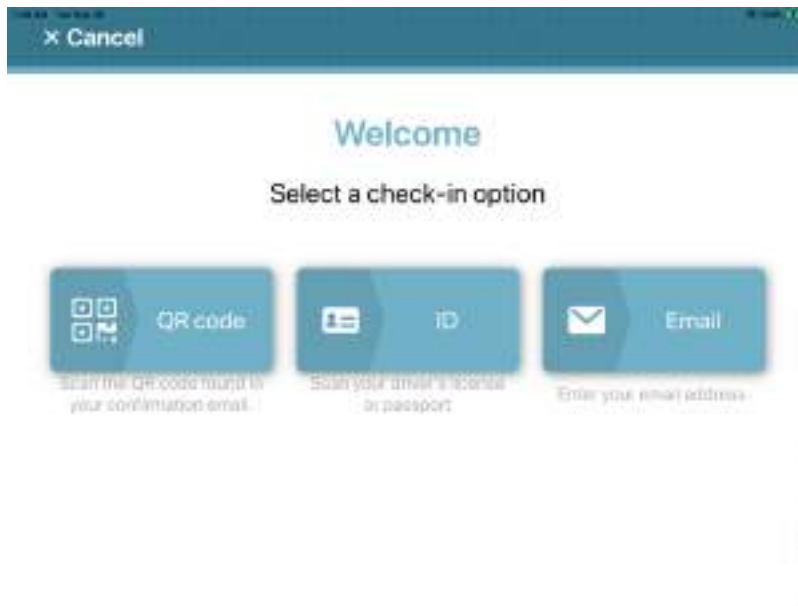
These options customize the choices that are displayed to your visitors on your ClearID Self-Service Kiosk during the check-in or check-out process.

NOTE: The self-registration option is only displayed when all other check-in options aren't applicable.

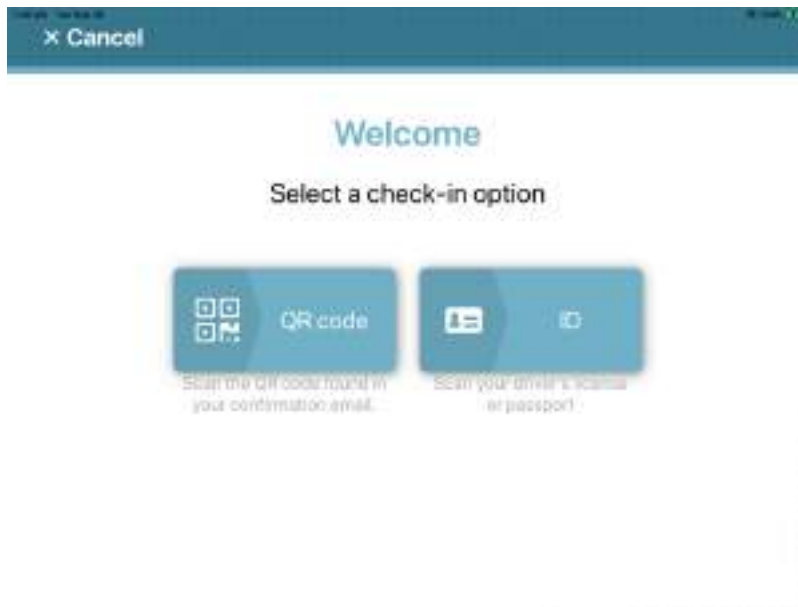
The following example shows the initial check-in or check-out screen customized for two different scenarios.



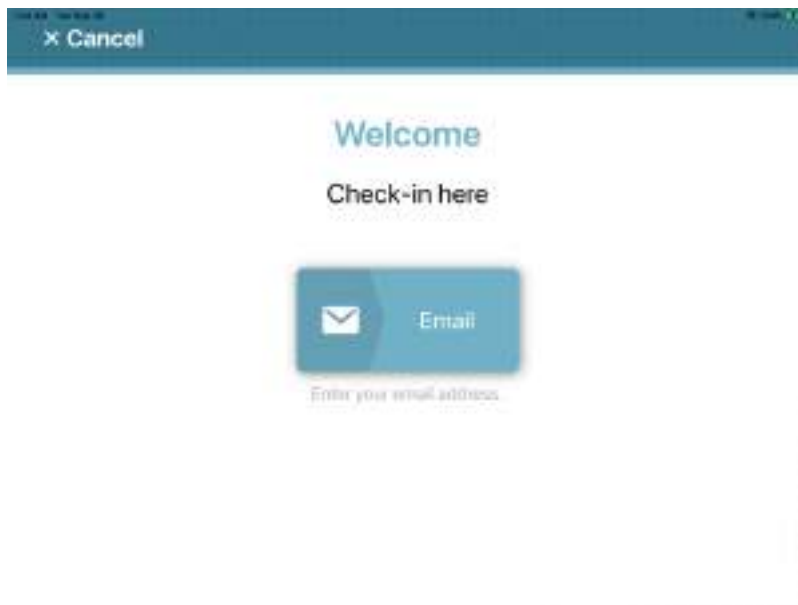
The following example shows the **Kiosk options** customized with **QR code**, **ID**, and **Email** check-in options enabled.



The following example shows the **Kiosk options** customized with **QR code** and **ID** check-in options enabled.



The following example shows the **Kiosk options** customized with only the **Email** check-in option enabled.



11 (Optional) Customize the **Kiosk theme**.

a) In the *Kiosk theme* section, choose a theme from the following:

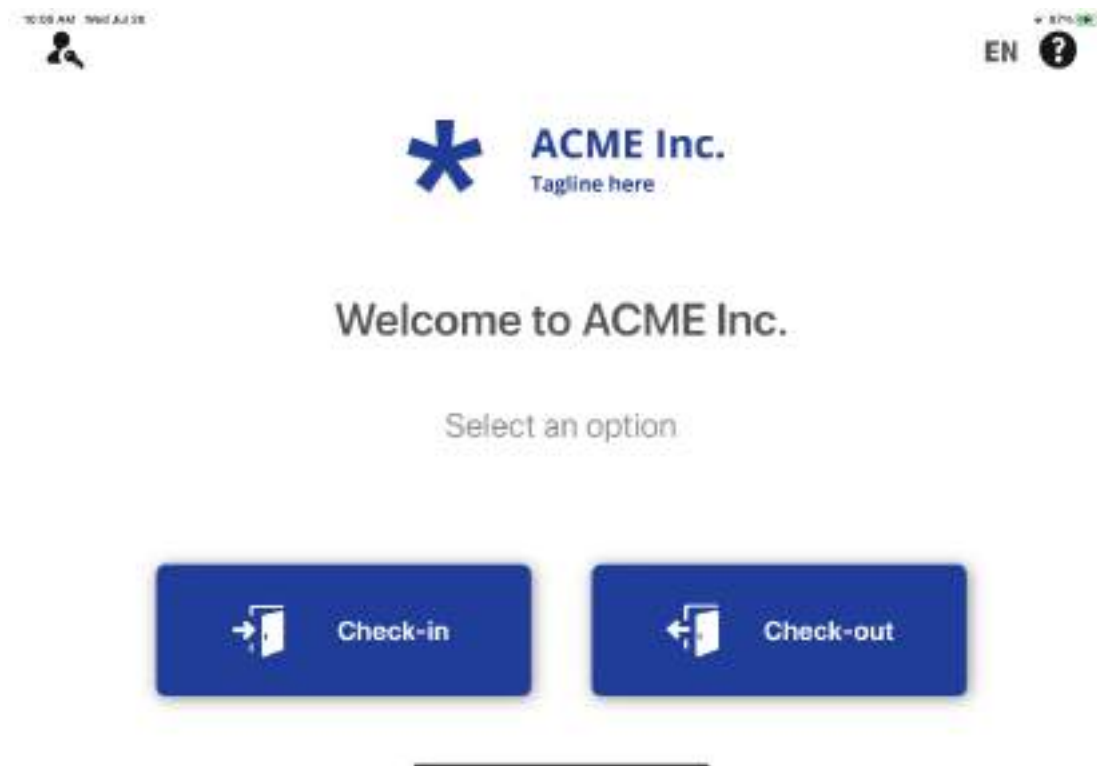
- **ClearID:** The ClearID theme (HEX color code 35768D) has no accent color.
- **White:** The white theme includes extra controls to pick an accent color. For example, to align with your corporate branding.

b) If you chose the **White** kiosk theme, select an accent color.



The accent color is applied to the buttons displayed on the ClearID Self-Service Kiosk.

The following example shows the white theme with blue accent color to match the blue corporate branding seen in the example.



The following example shows the white theme with red accent color to match the red corporate branding seen in the example.

10:38 AM Wed Jul 26



100%

EN



ACME Inc.
Tagline here

Welcome to ACME Inc.

Select an option



Check-in



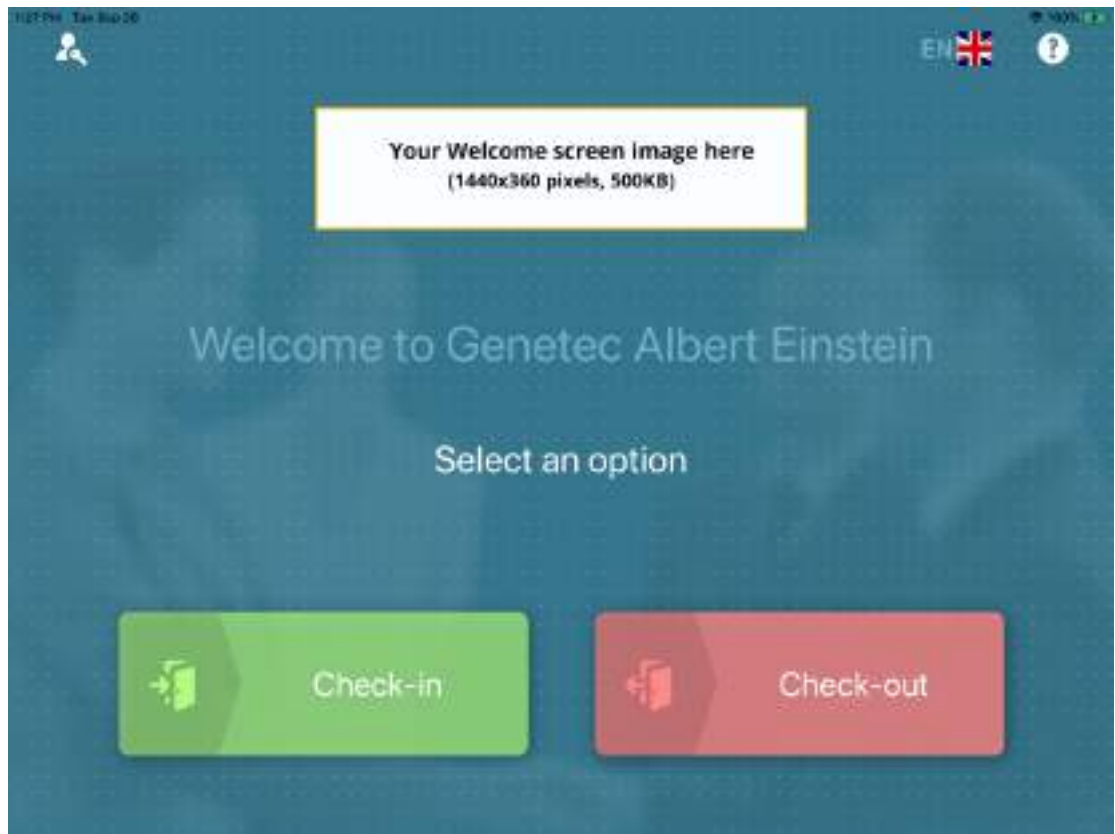
Check-out

12 (Optional) Customize the **Kiosk welcome screen**.

- a) In the *Kiosk welcome screen* section, drag and drop your picture or browse to select a **Kiosk welcome screen** image.

This image is used as the welcome screen *company name* or *logo* for the kiosk.

The following example shows the welcome screen with a custom logo image.



13 Click **Save**.

NOTE: Kiosk options changes are synchronized with your kiosk every 60 seconds.

Visitor management is enabled for the site.

After you finish

Submit an access request or visit request for this site.

Related Topics

[Introduction to the ADA](#)

[About workflows](#) on page 5

[Inviting visitors](#) on page 83

[Self-Service Kiosk check-in](#) on page 242

[Enabling QR code credentials for visitors](#) on page 107

Viewing sites where a user can invite visitors

An account administrator might need to view the list of sites where a user can invite visitors so that they can verify or update access if required.

Before you begin

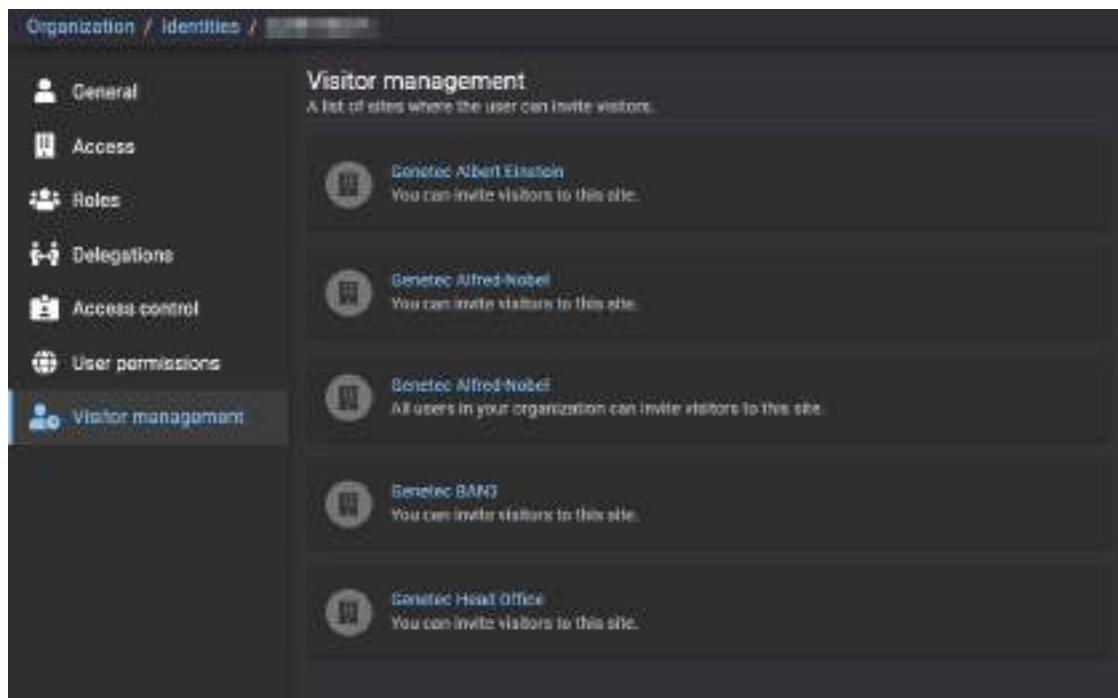
- [Configure your visitor management settings.](#)

What you should know

- Only account administrators can view the list of sites where a user can invite visitors or grant user permissions to invite visitors using roles.
- Users are automatically granted *Invite visitors* permissions for their home site by default.

Procedure

- 1 From the *Home* page, click **Organization > Identities**.
- 2 Search for or select a user.
- 3 Click **Visitor management** to display the list of sites where the user can invite visitors.



Related Topics

[Granting access to the web portal](#) on page 27

Modifying sites

After you add your sites, you can modify the settings of each site individually. An account administrator or site owner can modify the site owners, site properties, and change visitor management options for the site.

Before you begin

[Create your sites.](#)

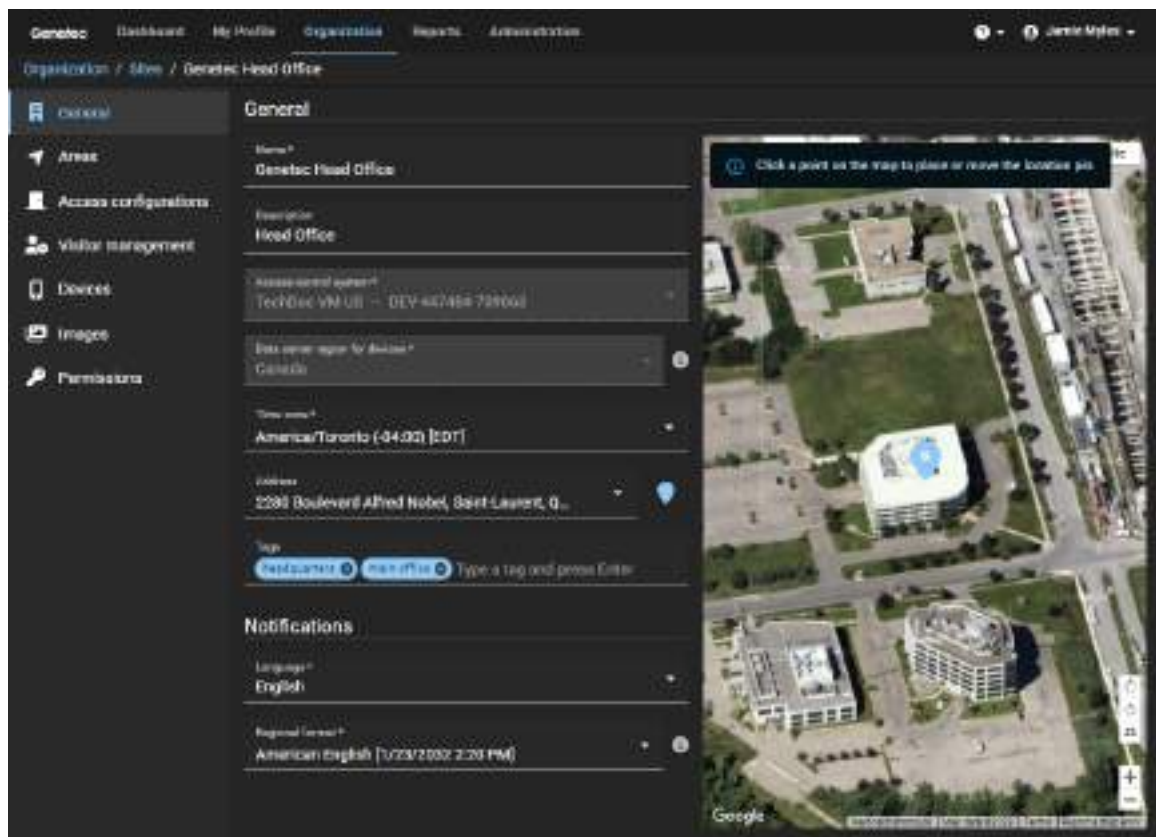
What you should know

To modify sites in Genetec ClearID™, you must be an account administrator or site owner.

- A *site* is associated with a Security Center SaaS access control system.
- Multiple sites can be associated with the same Security Center SaaS access control system.

Procedure

- 1 Click **Organization > Sites**.
- 2 Search for a site using the search field or select a site from the **Site** list.



- 3 In the *General* section, modify the fields as required.
- 4 In the *Notifications* section, modify the fields as required.
- 5 Click **Save**.

Your site settings have been changed.

Related Topics

[Creating sites](#) on page 47

Setting a maximum duration for site access

To enforce a limit for identities with temporary access, you can set a site access duration. When the maximum duration limit is reached, their access expires.

What you should know

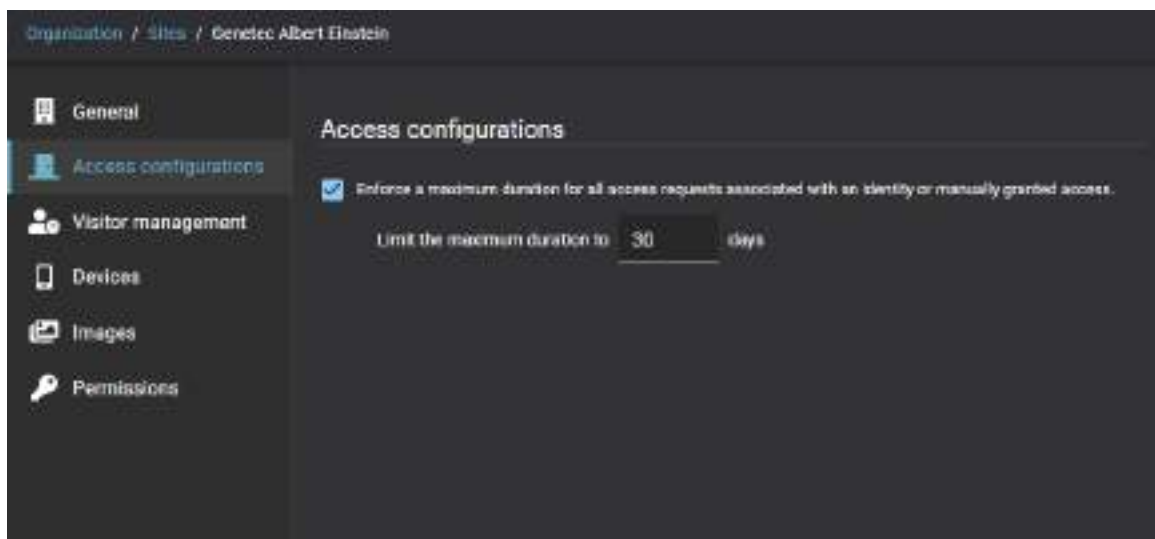
If the maximum duration for site access function has been activated for your account, the maximum duration limit for site access is enabled by default.

- To set a maximum duration period for site access in Genetec ClearID™, you must be a site owner.
- This access duration period only applies to individual identities or access that was manually granted.
- This access duration period doesn't apply to role access.

TIP: Use role groups when you have people who require permanent access to a site.

Procedure

- 1 Click **Organization > Sites**.
- 2 Search for and select a site.
- 3 Click **Access configurations**.



- a) Select the **Enforce a maximum duration for all access requests associated with an identity or manually granted access** checkbox.
- b) In the **Limit the maximum duration to** field, enter the maximum duration in days.
You can enter a value in days from 1 to 365. The default value is 30 days.

Managing areas

About areas

In Genetec ClearID™, an area is a logical entity that defines the relationship between Synergis™ doors and area owners. Areas are managed by the area owner.

Doors are not managed in Genetec ClearID™. Doors are managed in Security Center SaaS.

- Managing doors from ClearID is impractical due to the distance from the hardware.
- A door must be properly configured in Security Center SaaS and linked to the hardware physically managing the door.
- After areas are created in ClearID and synchronized in Security Center SaaS, doors can then be added to those areas in Security Center SaaS.

NOTE: Doors moved under areas inherit the access rules of the area.

- Door setup is performed in Security Center SaaS separately from the areas. After both *doors* and *areas* are present in Security Center SaaS, doors must be added to areas.

Related Topics

[Adding doors to areas](#) on page 74

Creating areas

In Genetec ClearID™, an area is a logical entity that defines the relationship between Synergis™ doors and area owners. Areas are managed by the area owner.

Before you begin

- [Create your sites.](#)

What you should know

- Only account administrators or site owners can create areas in Genetec ClearID™.
- In Genetec ClearID™, an area owner is an identity with authority over an area. The owner can define the policy for an area, assign area managers, give or remove access, and approve or deny access requests for an area.
- An area is bound to or associated with a Security Center SaaS system.

Procedure

- 1 Click **Organization** > **Areas**.
- 2 Click **Create area**.

NOTE: Mandatory fields are highlighted in the user interface with an asterisk (*).

- 3 In the *Site* section, complete the information fields:

- **Site:** From the **Site** list, select the site that you want to associate your area with.
 - **Access control system:** This field is prefilled based on the previously selected site. This access control system is used to synchronize changes in ClearID back to Security Center SaaS.
NOTE: If a warning message is displayed instead of the associated ACS information, click the link to return to the site configuration and enter the associated ACS information.
- a) In the *General settings* section, complete the information fields:
- **Name:** Enter an area name.
 - **Description:** Enter a description that indicates the geographical location of the building or physical area.
 - **Tags:** Enter alternative keywords or search term categorizations that might be used to find the area.
- b) In the *Advanced settings* section, select the options that you require:
- **Request approval workflow:** Choose the approval workflow option that you require:
 - **Automatic approval:** Area requests are automatically approved using a role-based policy.
 - **Area approvers:** Area requests are manually approved by authorized area approvers.
 - **Supervisor and area approvers:** Area requests are manually approved by supervisor and area approvers.
 - **Supervisors:** Area requests are manually approved by supervisors.
 - **Visibility:** Choose the visibility option that you require:
 - **Public:** The area is visible to everyone and access requests can be created for the area. Public is the default setting.
 - **Private:** The area is private and should be hidden and access requests aren't supported for the area.

4 Click **Save**.

When the area is saved, commands are automatically sent to create an area in Security Center SaaS.

Organization / Area / Sistro

TechDoc VM US Apply area Select area

General

Name*
Sistro

Description*
Cordon Bleu Sistro

Tags
Add a tag, start typing and press Enter

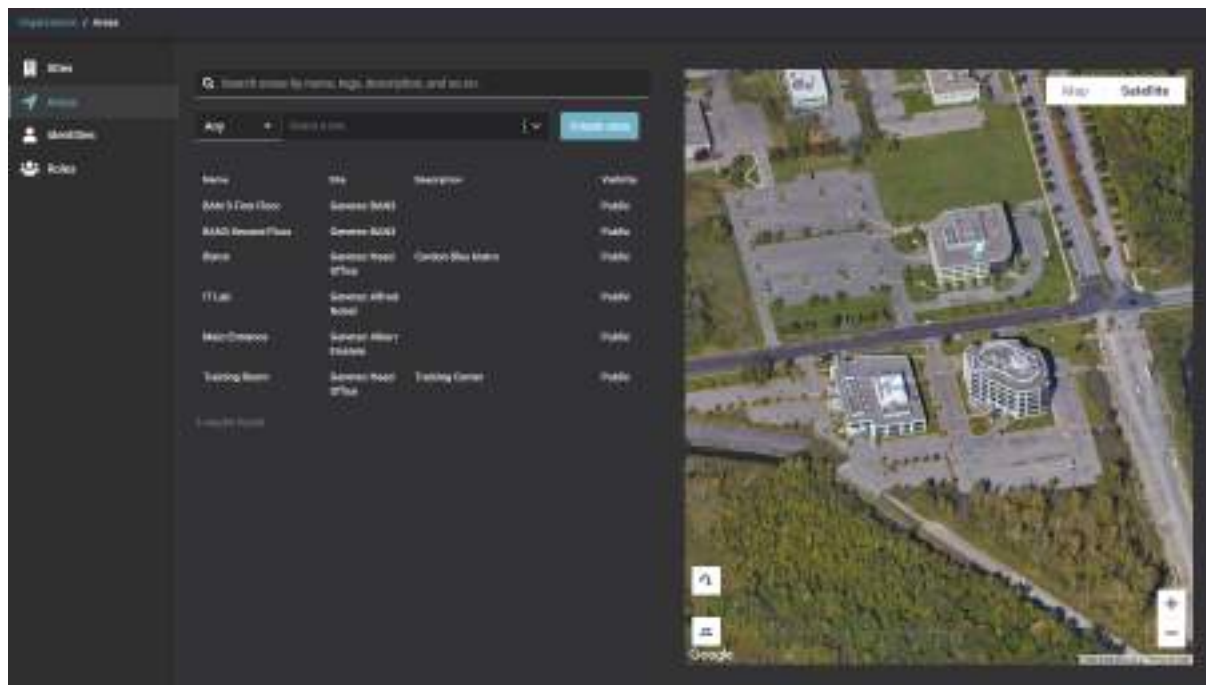
Advanced settings

Request approval workflow*
Supervisor and area approvers

Visibility*
Public

Cancel Save

Your area has now been created in ClearID.



Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



Adding doors to areas

Before you can submit access requests or invite visitors, you must add the doors to the associated areas that Genetec ClearID™ automatically created in Security Center SaaS.

Before you begin

[Create your areas.](#)

What you should know

Only Genetec™ Configuration desktop users with the *View door properties* privilege can add doors to areas in Security Center SaaS that are associated with areas in ClearID.

- When an area is created in ClearID, areas are automatically created in Security Center SaaS.
- Doors must then be added to the associated areas that are automatically created in Security Center SaaS.

Doors that are members of an area can be configured as *Captive* or *Perimeter* doors:

- Perimeter doors are used to enter and exit an area, and help to control access.
- Captive doors are used within an area.

Set the *door sides* correctly to ensure that and are properly tracked. A door's *Entrance* and *Exit* sides are relative to the area being configured.

Procedure

- 1 In Genetec Configuration desktop, open the *Area view* task.
- 2 Select an area and then click the **Properties** tab.
- 3 In the *Doors* section, click **Add an item** (+) and select the doors that you want to link to your area.
- 4 For all doors in the *Doors* section, configure the door type:
 - If the door is used to enter or exit the area, set the slider to **Perimeter**.
 - If the door is located inside the area, set the slider to **Captive**.

NOTE: If a smaller area is nested inside a larger area, you don't need to add the perimeter doors of the smaller area as captive doors of the larger area. The system automatically organizes nested areas when calculating people counts and applying antipassback rules.

 - To swap the door sides, select the door and click **Swap door side**.
- 5 Click **Apply**.

Your doors are now added to the areas in Security Center SaaS that are associated with ClearID areas.

After you finish

In ClearID, you can now [submit access requests](#) or [invite visitors](#).

Related Topics

[About areas](#) on page 70

Enabling visitor management for areas

Before visitors can request an area visit, you must configure the visitor management settings for your area.

Before you begin

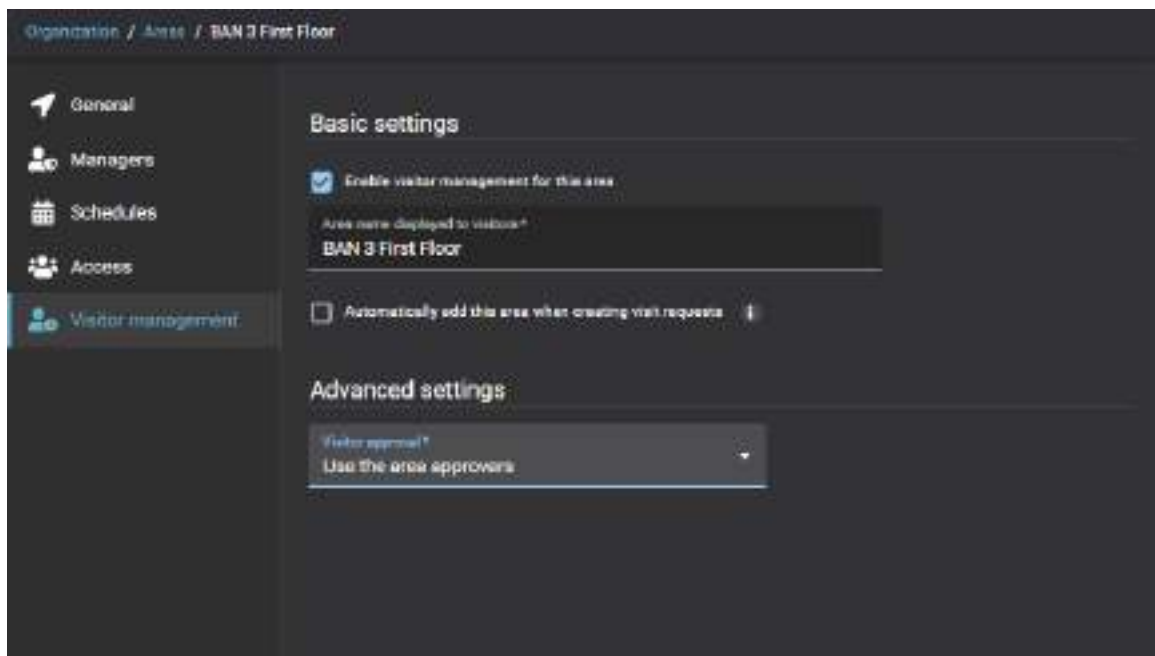
[Create your areas.](#)

What you should know

- Visitor management for areas is off by default.
- Only area owners or a site owners can enable visitor management for areas in Genetec ClearID™.
- The options displayed when a visit request is created vary depending on the users requesting access and also the settings that you configure here.

Procedure

- 1 Click **Organization > Areas**.
- 2 From the **Areas** list, select an area.
- 3 Under the **Visitor management** tab, configure the following options:



- **Basic settings:** Select the **Enable visitor management for this area** option to enable visitor management for this area.
- **Area name displayed to visitors:** Enter the area name that you want displayed in email notifications sent to visitors.
- **Automatically add this area when creating visit requests:** If you select this option, all guests in your visit request are automatically granted access to the requested area.
- **Advanced settings:** If you didn't select the **Automatically add this area when creating visit requests** option, then specify the required approvers:
- **Visitor approval:** Choose the approvers for visitor access from the following options:

- **Automatically approve visitors:** Automatically approve access requests for this area.
- **Use the area approvers:** Only allow area approvers to approve or deny access requests for this area.
- **Define visit approvers:** Only allow people in the **Visit approvers** list to approve or deny access requests for this area.

4 Click **Save**.

Visitor management is enabled for the area.

Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



After you finish

Access requests or visit requests can now be submitted for this area.

Related Topics

[About workflows](#) on page 5

About nested areas

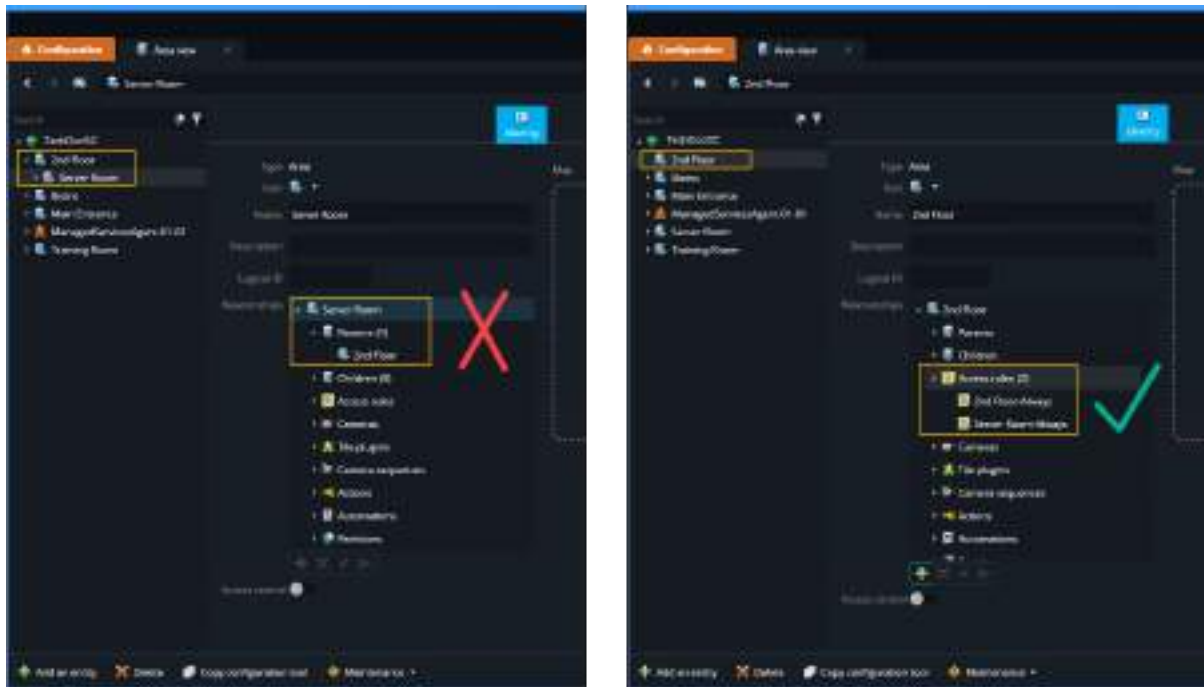
In Security Center SaaS, nested areas can be used to logically group areas so that access is automatically granted to people for associated nested areas when access is requested in Genetec ClearID™ for one of the nested areas.

Nested areas are useful for organizations with lots of restricted areas, lots of logical grouping, or area dependencies. For example, when secure areas require access to other areas to get to the secure area:

- **Example 1:** Requesting access to a server room might automatically grant access to the floor that the server room is on.
- **Example 2:** Requesting access to a restricted area might automatically grant access to the floor the restricted area is on, and also grant access to the building that the floor and restricted area are in.

NOTE: In Genetec™ Configuration desktop, nesting areas using **Parents** or **Children** options in the *Relationships* section of the **Area** view does not inherit access.

BEST PRACTICE: Nest areas using **Access rules** options in the *Relationships* section of the **Area** view to inherit the required access. You can create nested areas to add access rules relationships for up to three logically associated areas. Nesting more than three areas together isn't recommended.



Adding multiple access rules to an area creates the logical group association for nested areas. This relationship association ensures that the areas automatically grant access to the other associated areas when access is requested for one of the nested areas. By default ClearID automatically creates access rules for each schedule that is added to an area.

IMPORTANT: If the schedules for any of the nested areas change, the area relationships (access rules) must be configured again.

Related Topics

[Granting access to areas automatically](#) on page 77

Granting access to areas automatically

To automatically grant access for people to logically grouped areas, you can create nested areas for Genetec ClearID™ in Security Center SaaS.

Before you begin

- [Create the areas that you require.](#)
- [Learn about nested areas.](#)
- Plan the logical grouping of your areas before configuring your nested areas to automatically grant or inherit access.

What you should know

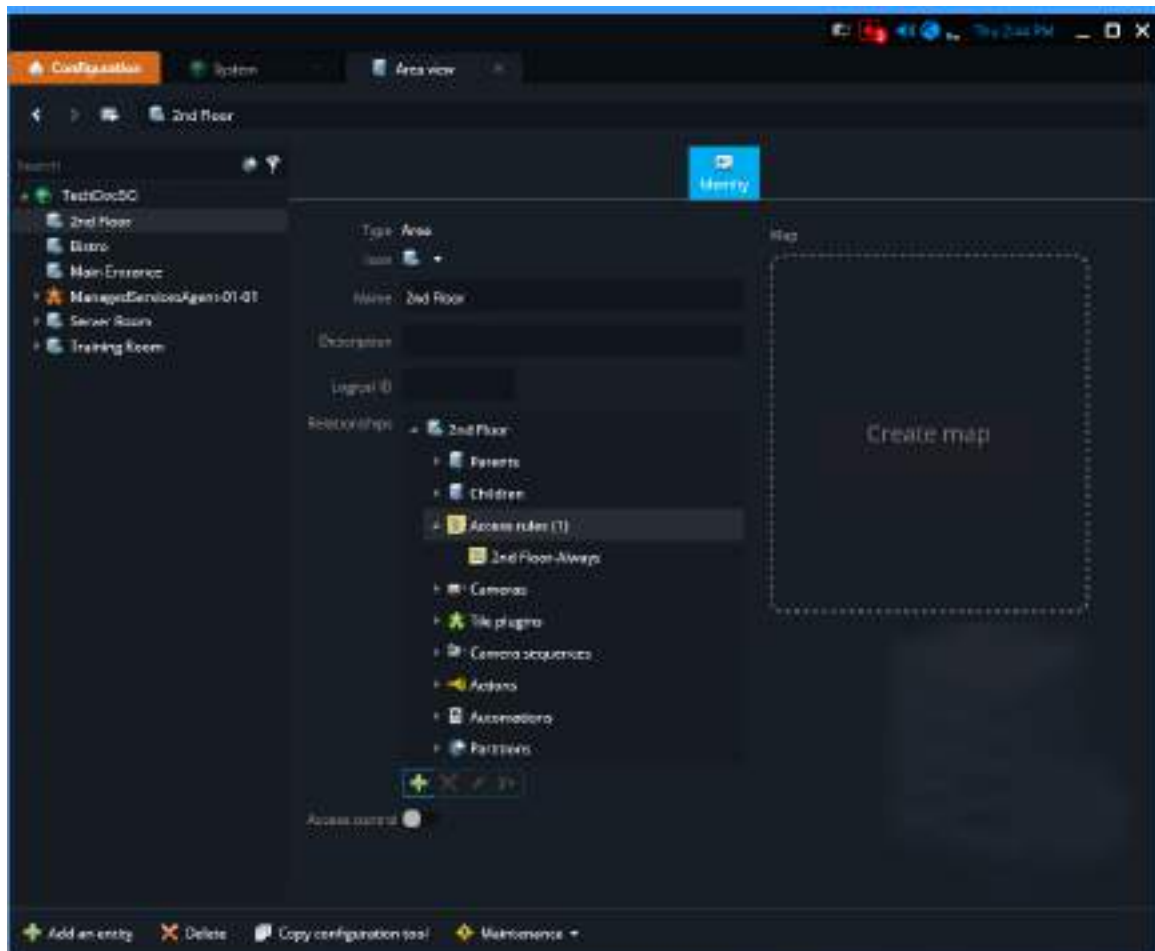
Only a Security Center SaaS administrator or system integrator can configure or map the nested areas.

If the schedules for any of the nested areas change, the area relationships (access rules) must be configured again.

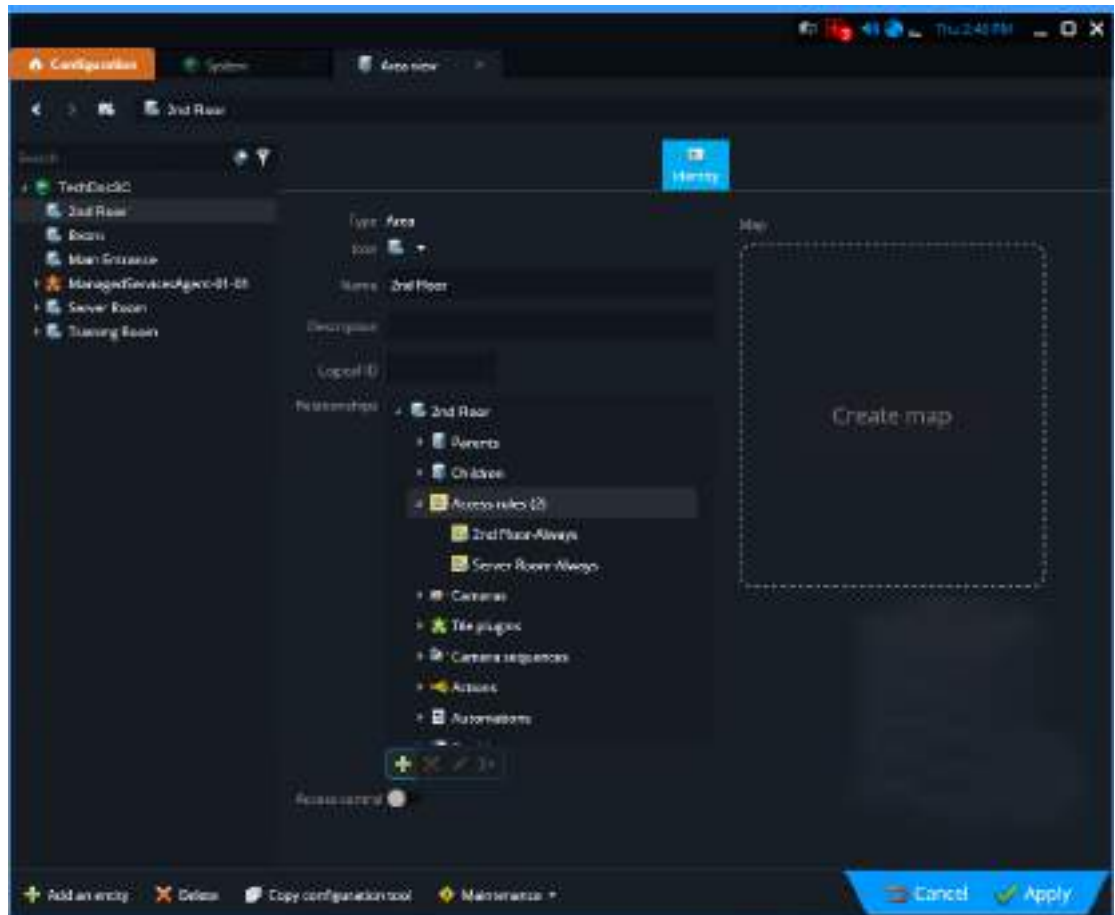
BEST PRACTICE: Nest areas using **Access rules** options in the *Relationships* section of the **Area** view to inherit the required access. You can create nested areas to add access rules relationships for up to three logically associated areas. Nesting more than three areas together isn't recommended.

Procedure

- 1 In Genetec™ Configuration desktop, open the *Area view* task.
- 2 In the **Area view**, click an area in the left navigation pane.



- 3 In the **Identity** tab **Relationships** section, double-click **Access rules**.
 - a) Click **Insert an item** (+) then search for and select the *access rules* that contain the required schedules for the *areas* that you want to associate with the area selected earlier in step 2 on page 78.



TIP: You can also click **Entity type** and select the **Access rule** checkbox, then click **Search** to only display access rules in the entity list.

- b) (Optional) Repeat for other areas.
- 4 Click **Apply**.
 When an access request is received for an area that is part of a group of areas, access is automatically granted based on the relationships defined for the areas. In the previous example, anyone who has access to the Server Room is also automatically granted access to the 2nd floor.

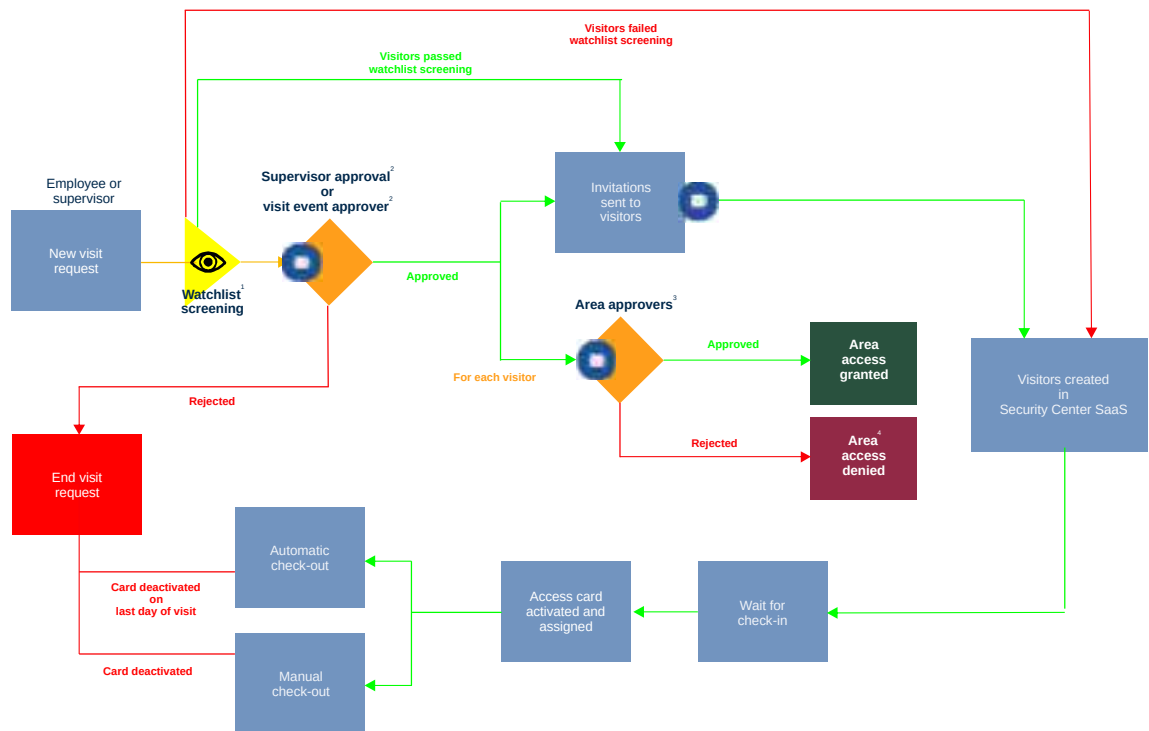
Managing visitors

About visit request workflow

A visit request workflow is a series of activities performed by the system or authorized people during the life cycle of a visit request. The activities can change the state and properties of visit requests, affect other entities in the system, or wait for conditions to be met.

The workflow helps automate tasks like approving or rejecting access requests freeing up time to focus on other tasks.

The following diagram illustrates the visit request workflow that occurs in Genetec ClearID™ and Synergis™.



¹ (Optional) For more information, see Visit request watchlist workflow.

² (Optional) Approval can be enabled or disabled for each site.

³ (Optional) Approval can be enabled or disabled for each area.

⁴ Visit event has been created and visitor has been created in Security Center SaaS but area access has been denied. Visitor might be able to access denied areas if escorted by a host, this access exception is at the discretion of the organization.

Related Topics

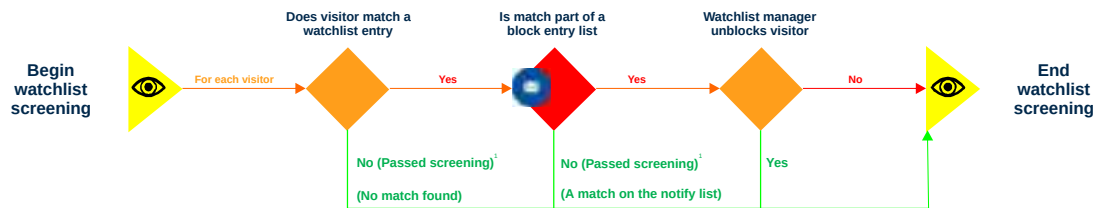
[About workflows](#) on page 5

About visit request watchlist workflow

A watchlist workflow is a series of activities performed by the system or authorized people during the life cycle of a visit request if watchlists are enabled. The activities can change the state and properties of watchlists, affect other entities in the system, or wait for conditions to be met.

The workflow helps automate tasks like screening visitors for persons or companies of interest during a self-service check-in or a self-registration freeing up time to focus on other tasks.

The following diagram illustrates the *watchlist workflow* that occurs (if the watchlist function is enabled for your account) in Genetec ClearID™ and Synergis™ in parallel with the visit request workflow.



¹ Visitor registration is only confirmed after screened visitors aren't found in any block entry watchlists. Any visitors that are blocked do not receive a visit notification email.

Related Topics

[About workflows](#) on page 5

Inviting visitors

To invite one or more guests for a site visit or event, use the self-service portal. Using a self-service portal with area approvers specified simplifies the approval process, and avoids interrupting a chain of people who might or might not be the correct approvers.

Before you begin

1. [Familiarize yourself with workflows.](#)
2. [Enable visitor management for your site.](#)
3. [Ensure that you have the required permissions to invite visitors to the site.](#)

What you should know

You can add visitors individually or import a large list of visitors using a CSV file.

- If you have fewer than five visitors to invite, add your visitors individually.
- If you have more than five visitors to invite, prepare a CSV file to import your visitor list.
- If your identity home site is configured, you're automatically granted access to invite visitors to that site. This option is only available if the visitor management options for the site have been configured to allow people to invite visitors.
- The options displayed when creating a visitor invite can vary depending on the site settings and settings configured for visitor management.

NOTE: Mandatory fields are highlighted in the user interface with an asterisk (*).

Procedure

1. [Log on to the self-service portal.](#)
2. Do one of the following:
 - Click **Dashboard > My requests > New request > Invite visitors.**
 - Click **Dashboard > Visits > New visit event.**
3. In the *New visit event* wizard, follow the prompts to complete the wizard for one of the following situations:
 - [Invite visitors manually](#)
 - [Invite visitors using a CSV import](#)
4. Click **Finish.**

Your visit request has been submitted and is waiting for the required approvals.

Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



After you finish

Confirm whether the request was approved or rejected:

- Check your email for a *Visit approved* email.
- Check **My requests** in Genetec ClearID™.

Related Topics

[Enabling visitor management for sites](#) on page 50

[Visitor Management Feature Note \(2 pages\)](#)

Inviting visitors manually

If you have fewer than five visitors to invite to your event, you can add your visitors manually.

Before you begin

1. [Familiarize yourself with workflows.](#)
2. [Enable visitor management for your site.](#)
3. [Ensure that you have the required permissions to invite visitors to the site.](#)

What you should know

- If your identity home site is configured, you're automatically granted access to invite visitors to that site. Access is only automatically granted if the options for site visitor management have been configured to allow people to invite visitors.
- The options displayed when inviting visitors can vary depending on the site settings and settings configured for visitor management.

NOTE: Mandatory fields are highlighted in the user interface with an asterisk (*).

Procedure

- 1 [Log on to the self-service portal.](#)
- 2 Do one of the following:
 - Click **Dashboard > My requests > New request > Invite visitors.**
 - Click **Dashboard > Visits > New visit event.**

- 3 In the *New visit event* wizard, enter or select details about *where* the event will take place.

The screenshot shows a wizard titled "Channel Partner event at Genetec Alfred-Nobel". At the top, there are four steps: 1. Where (active), 2. When, 3. Who, and 4. Details. The main heading is "What is the name of the event?". Below it is a text input field labeled "Name *" containing "Channel Partner event" with a character count "21 / 100". The next section is "Where will this event take place?". It contains three dropdown menus: "Site *" with "Genetec Alfred-Nobel", "Host meeting location" with "Main Entrance", and "Parking location" with "Alfred-Nobel". Below these is a section "Visitors are automatically assigned default access" with a dropdown menu labeled "Access *" showing "IT Lab". At the bottom left is a "Cancel" button and at the bottom right is a "Next" button.

- 4 Enter or select details about *when* the event takes place and the purpose of the event.

Channel Partner event at Genetec Alfred-Nobel

Where When Who Details

When does the visitor require access?
Remember to include any time before and after the meeting when the visitor might also require access.

The dates and times shown here are in the UTC time zone.

Start date *	Start time *
01/01/2024	10:00 AM
End date *	End time *
01/01/2024	04:00 PM

Duration: 6 hr

What is the purpose of this event?

Visit reason *

Meeting

Cancel Back Next

TIP: Remember to include time before and after the visitor event or meeting when the visitor might also require access.

- 5 Enter or select details about *who* to invite to the event.

The screenshot shows a dark-themed interface for managing an event. At the top, the title is "Channel Partner event at Genetec Alfred-Nobel". Below the title is a progress bar with four steps: "Where" (checked), "When" (checked), "Who" (active, highlighted in blue), and "Details" (disabled). Below the progress bar, the text "Who are the visitors?" is displayed. Underneath, it says "2 visitors added:". To the right of this text are two buttons: "Import visitors" and "Add visitor" (highlighted in blue). Below this is a table listing the added visitors:

John Doe	✉ john.doe@test.com	🏢 Genetec	✎
Jane Doe	✉ jdoe@test.com	🏢 N/A	✎

At the bottom left is a "Cancel" button. At the bottom right are "Back" and "Next" (highlighted in blue) buttons.

- Click **Add visitor** and complete the fields.
- Click **Save**.
- Repeat for each additional visitor.

6 Complete *details* about the event.

Channel Partner event at Genetec Alfred-Nobel

Where When Who Details

Who will escort the visitors?

Name	Email	SMS alerts
John Doe	johndoe@test.com	☒ +1 5141234567

Type to search...

Notes for security

Notes

Cancel Back Finish

- **Name:** The name of the visitor event host.
- **Email:** The email address for the visitor event host.
- **SMS:** Enter a mobile phone number to send SMS alert notifications to visitor hosts when the visitor checks in.
NOTE: Use the search field to add more visitor hosts. You can add up to 10 visitor hosts.
- **(Optional) Notes for security:** Add notes about the visitor, the visit invite, or the visit event.

7 Click **Finish**.

Your visit request has been submitted and is waiting for the required approvals.

Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



After you finish

Confirm whether the request was approved or rejected:

- Check your email for a *Visit approved* email.

- Check **My requests** in Genetec ClearID™.

Related Topics

[SMS alerts](#) on page 95

[Visitor Management Feature Note \(2 pages\)](#)

Inviting visitors using an imported visitor list

If you have more than five visitors to invite to your event, you can use a CSV file import to populate your visitor list.

Before you begin

1. [Familiarize yourself with workflows.](#)
2. [Enable visitor management for your site.](#)
3. [Ensure that you have the required permissions to invite visitors to the site.](#)

What you should know

- If your identity home site is configured, you're automatically granted access to invite visitors to that site. Access is only automatically granted if the options for site visitor management have been configured to allow people to invite visitors.
- The options displayed when inviting visitors can vary depending on the site settings and settings configured for visitor management.

TIP: When you **Import visitors**, a sample CSV file provided by the system can be used. The columns in the sample CSV file match the settings in the site configuration. You can then complete the visitor details values in the CSV file and import all visitors in one click. For example, importing 500 people to a site visit or customer event.

NOTE: Mandatory fields are highlighted in the user interface with an asterisk (*).

Procedure

1. [Log on to the self-service portal.](#)
2. Do one of the following:
 - Click **Dashboard > My requests > New request > Invite visitors.**
 - Click **Dashboard > Visits > New visit event.**

- 3 In the *New visit event* wizard, enter or select details about *where* the event will take place.

The screenshot shows a wizard titled "Channel Partner event at Genetec Alfred-Nobel". At the top, there are four steps: 1. Where (active), 2. When, 3. Who, and 4. Details. The main heading is "What is the name of the event?". Below it is a text input field labeled "Name *" containing "Channel Partner event" with a character count "21 / 100". The next section is "Where will this event take place?". It contains three dropdown menus: "Site *" with "Genetec Alfred-Nobel", "Host meeting location" with "Main Entrance", and "Parking location" with "Alfred-Nobel". Below these is a section "Visitors are automatically assigned default access" with a help icon. It contains a dropdown menu labeled "Access *" with "IT Lab" selected. At the bottom left is a "Cancel" button and at the bottom right is a "Next" button.

Channel Partner event at Genetec Alfred-Nobel

1 Where 2 When 3 Who 4 Details

What is the name of the event?

Name *
Channel Partner event
21 / 100

Where will this event take place?

Site *
Genetec Alfred-Nobel

Host meeting location
Main Entrance

Parking location
Alfred-Nobel

Visitors are automatically assigned default access ⓘ

Access *
IT Lab

Cancel Next

- 4 Enter or select details about *when* the event will take place and the purpose of the event.

Channel Partner event at Genetec Alfred-Nobel

Where When Who Details

When does the visitor require access?
Remember to include any time before and after the meeting when the visitor might also require access.

The dates and times shown here are in the UTC time zone.

Start date *	01/01/2024	Start time *	10:00 AM
End date *	01/01/2024	End time *	04:00 PM

Duration: 6 hr

What is the purpose of this event?

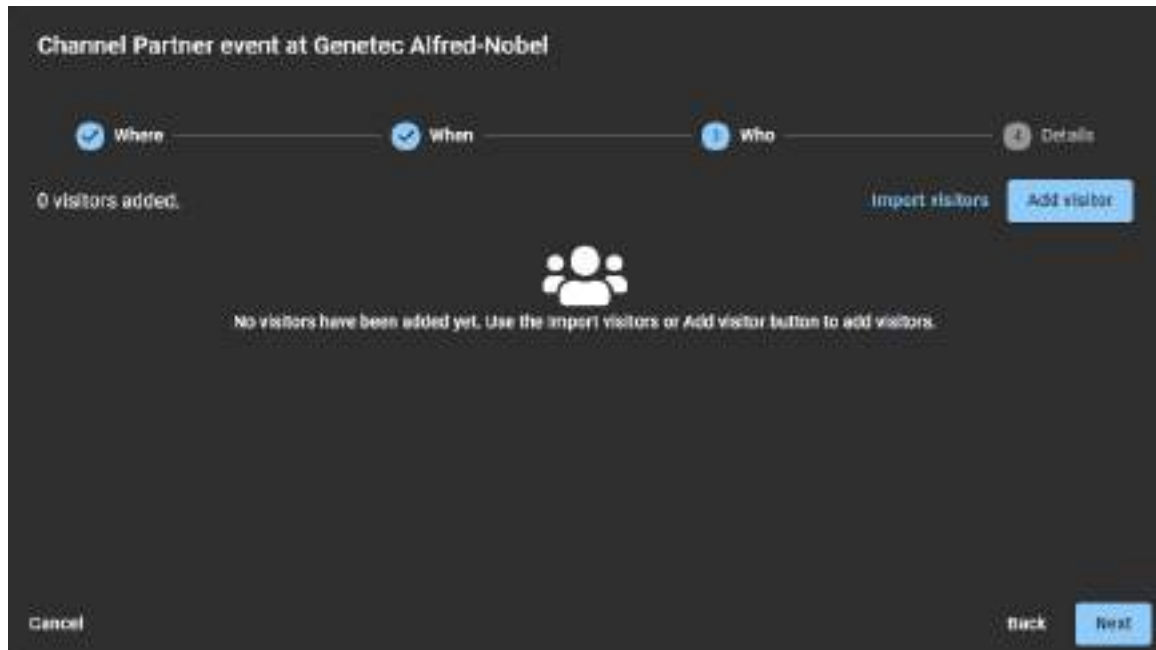
Visit reason *

Meeting

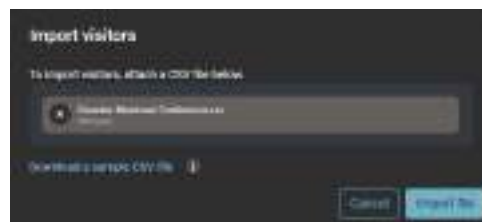
Cancel Back Next

TIP: Remember to include time before and after the visitor event or meeting when the visitor might also require access.

- 5 Prepare to import *who* you want to invite to the event.



- a) In the *Who will attend this event?* section, click **Import visitors** and then choose one of the following:
- Use an existing CSV file.
 - Download a sample CSV file.
- 6 If you chose to use an existing CSV file, do the following:
- a) Drag and drop an existing CSV file containing the customers you want to invite or click **Browse** to select the file you require.



- b) Click **Import file** to import the visitor list.
- c) Click **Confirm** to complete the import.
- d) (Optional) Click **Edit** (✎) to modify any visitor details and click **Save** to confirm the update.

7 If you chose **Download a sample CSV file**, do the following:

a) Click **Download a sample CSV file**.



b) Select and open the downloaded CSV file.

c) For each visitor, complete a row of visitor information in the CSV template file.

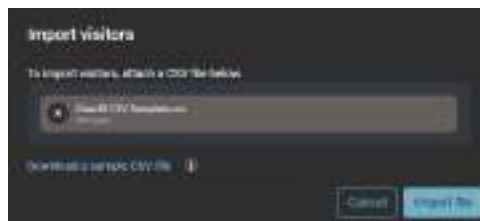
	A	B	C	D	E	F	G
1	FirstName	LastName	Email	CompanyName	IsDisabilityConstantlyRequired	IsScreeningCompleted	HasDisclosureAgreement
2	Rubette	Hegarty	rhagarty@test.com	Hegarty inc.	TRUE	DoNotApply	NOW Completed
3	Rand	Blanning	rblanning@test.com	Blanning inc.	FALSE	ScreeningCompleted	DoNotApply
4							
5							
6							
7							
8							
9							
10							
11							

NOTE: The columns in the CSV template can vary depending on the settings in your site configuration.

d) Save the visitor list as a CSV file.

e) Return to the *Import visitors* dialog, to drag and drop or click **Browse** to select the file you created.

f) Click **Import File** to import the visitor list.



g) Click **Confirm** to complete the import.

8 Complete *details* about the event.

Channel Partner event at Genetec Alfred-Nobel

Where When Who **Details**

Who will escort the visitors?

Name	Email	SMS alerts ⓘ
John Doe	johndoe@test.com	☒ +1 5141234567 ✕

Type to search...

Notes for security ⓘ

Notes

Cancel Back Finish

- **Name:** The name of the visitor event host.
- **Email:** The email address for the visitor event host.
- **SMS:** Enter a mobile phone number to send SMS alert notifications to visitor hosts when the visitor checks in.
NOTE: Use the search field to add more visitor hosts. You can add up to 10 visitor hosts.
- **(Optional) Notes for security:** Add notes about the visitor, the visit invite, or the visit event.

9 Click **Finish**.

Your visit request has been submitted and is waiting for the required approvals.

Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



After you finish

Confirm whether the request was approved or rejected:

- Check your email for a *Visit approved* email.

- Check **My requests** in Genetec ClearID™.

Related Topics

[SMS alerts](#) on page 95

[Visitor Management Feature Note \(2 pages\)](#)

SMS alerts

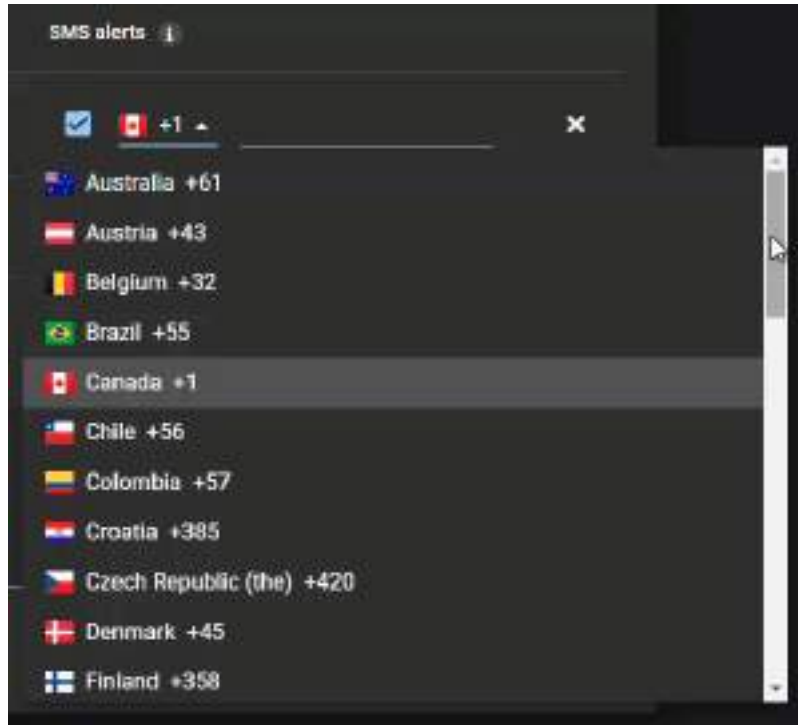
In Genetec ClearID™, SMS alerts are used in the visit event wizard to automatically send notifications to visitor hosts to inform them when visitors check-in.

SMS alerts for visitor check-in are supported for the following countries:

Country	Country code
 Austria	+43
Australia	+61
 Belgium	+32
 Brazil	+55
 Canada	+1
 Chile	+56
 Columbia	+57
 Croatia	+385
 Czech republic (the)	+420
 Denmark	+45
 Finland	+358
 France	+33
 Germany	+49
 Greece	+30
 Iceland	+354
 India	+91
 Ireland	+353
 Italy	+39
 Japan	+81
 Luxembourg	+352

Country	Country code
 Malaysia	+60
 Mexico	+52
 Monaco	+377
 Netherlands	+31
 Norway	+47
 Peru	+51
 Philippines (the)	+63
 Portugal	+351
 Romania	+40
 Singapore	+65
 Spain	+34
 Sweden	+46
 Switzerland	+41
 Taiwan (Province of China)	+886
 Thailand	+66
 United Kingdom of Great Britain and Northern Ireland (the)	+44
 United States of America (the)	+1
 Vietnam	+84

Example



Related Topics

[Inviting visitors manually](#) on page 84

[Inviting visitors using an imported visitor list](#) on page 89

Reviewing visit events

Area owners, security, and reception can review current or upcoming visits or events for their areas. Visits can be requested for hosting other site employees, maintenance contractors, appointments, meetings, interviews, customer visits, business partner conferences, and so on.

What you should know

Only area owners, security, or reception can review visits.

Procedure

- 1 Click **Dashboard > Visits**.
- 2 (Optional) Enter your search criteria.
Only search results for visits that contain the entered word in the visit name are displayed. For example, if you enter *training*, only visits whose name includes the word *training* are displayed in the search results.
- 3 Select the options that you require.
 - **Current and upcoming visits:** Displays current and upcoming visits. By default, 10 visits are displayed and you can click **Load more** to display the next 10 visits.
 - **Past visits:** Displays past visits. By default, 10 past visits are displayed and you can click **Load more** to display the next 10 past visits. You can find past visits that occurred in the last year.
 - **All visits:** Displays all visits. By default, 10 visits are displayed and you can click **Load more** to display the next 10 visits.
- 4 (Optional) Select a filter from the **filter** list to filter results for the visit request state:
 - No filter
 - Approved
 - Canceled
 - Denied
 - Submitted
 - Waiting for approvals

The visits matching your selections are displayed.

Visit	Status	Site	Start	End
Customer visit Business	Approved	Genetec BANK	July 30, 2019, 12...	July 31, 2019, 12...
customer visit Training course	Approved	Genetec Head Office	July 30, 2019, 12...	August 9, 2019, ...
Customer visit Customer visit	Approved	Genetec Head Office	August 2, 2019, ...	September 26, 2...

After you finish

[Copy a visit event.](#)

Copying a visit event

You can copy a visit event to take advantage of reusable information in a recurring visit or visit events that include many participants.

Before you begin

[Review visit events.](#)

What you should know

- Any user can copy their visits to create a similar visit.
- Use the **Copy event** function when you have recurring visits or a visit that includes many participants. For example, one of the following situations:
 - Repeat visitors
 - A meeting that has the same or similar attendees as a previous meeting
 - Monthly customer visits
 - A yearly business partner conference

Procedure

- 1 Click **Dashboard > Visits**.
- 2 Click the visit event that you want to copy.
- 3 Click **Copy event**.
A copy of the visit event is created.
- 4 Modify the visit event as required and click **Save**.
For example: changing the event details, changing dates, adding or removing visitors, adding or removing hosts, or amending notifications.

The new visit event is created and a *Visit created* email notification is sent to all visitors and hosts.

Modifying visit events

From time to time, you might want to modify a visit event to change the event details, or to add or remove visitors or hosts. Updating the visit event details ensures that your visitors are always kept up to date following any changes to an upcoming event.

Before you begin

Create your visit events in Genetec ClearID™ by doing one or more of the following:

- [Inviting visitors manually](#) on page 84
- [Inviting visitors using an imported visitor list](#) on page 89

What you should know

- Visit events can only be modified before the start of the visit event.
- Any modifications to a visit event are highlighted in the updated email notifications sent to relevant recipients.
- If visit event approval is enabled, any visit event modifications that aren't **Reason** field modifications cause the approval process to restart.
- Changing an existing visitor or host email triggers a cancellation notification for the original email and a visit event notification for the newly updated email.
- If visit event approval is enabled, changing a visitor or host name doesn't trigger email notifications for visitors, but does restart the approval process.

Procedure

- 1 Click **Dashboard > Visits**.
- 2 (Optional) If the list is long, use the drop-down menus and column filters to refine the results.
 - **Name:** Enter a search criteria to search for the visit event by name.
 - **Status:** Select one or more status filters to search for the visit event using the event status.
 - **Site:** Start typing to find a site or select a site from the **Site** list.
 - **Date:** In the **Date** column, use the ascending (⬆️) or descending (⬇️) controls to adjust the order of the results.
- 3 Click a visit event and review the event details to verify it's the event that you want to modify.

4 Click **Edit event**.

Channel Partner Event

Requested by: Jane Doe

Approved

Site and areas
Genetec Albert Einstein America/Toronto

Event date and time
Start: 01/01/2024 09:00 AM
End: 01/01/2024 05:00 PM

Event information
Parking location:
Host/Setup location:
Visit reason:
Notes:

Visitors - 2 visitors
John Doe - john.doe@test.com
Jane Doe - jane@test.com

Hosts - 2 hosts (10 hosts max)
Jane Doe
John Q. Grey

History
Genetec ClearID™ system edited the request.
Genetec ClearID™ system approved the request.

Buttons: Edit event, Cancel event, Close, Cancel request

5 Modify one or more of the following as required:

- In the **Name** field, modify the name.¹
- In the *Event date and time* section, modify the start or end date and time.¹
- In the *Event information* section, modify the parking location, host meetup location, or notes.¹

Visit event **Visit reason** modifications don't trigger any approval notifications because the reason has no impact on visitors attending the event.

- In the *Visitors* section, add, modify, or remove visitors.

Any changes to visitors are assessed again to verify any watchlist screening criteria.

- In the *Hosts* section, add, modify, or remove hosts.

NOTE: ¹Modifying the **Name**, **Event date and time**, or **Event information** doesn't trigger re-approval (if approvals are applicable).

6 Click **Save** to confirm your changes.**After you finish**

[Review your visit event details](#) to verify that the changes are correct.

QR codes as a credential for visitors

Genetec ClearID™ can use QR codes as a credential for visitors to simplify access to parking entrance barriers, turnstiles, or gated facilities.



The following third-party vendor QR code solutions are currently supported:

- Qscan barcode readers
- STid QR code readers

Visitors can use a QR code as a credential to open parking entrance barriers, turnstiles, or gated facilities:

- The QR code contained in a visitor confirmation email can be presented using a mobile device.
- The visitor confirmation email can also be printed and used for check-in.
- SMS messages notify hosts when their visitors arrive (if the check-in notification function is enabled).

Related Topics

[Supported devices](#) on page 12

Importing a custom card format (QR code credential) in Synergis

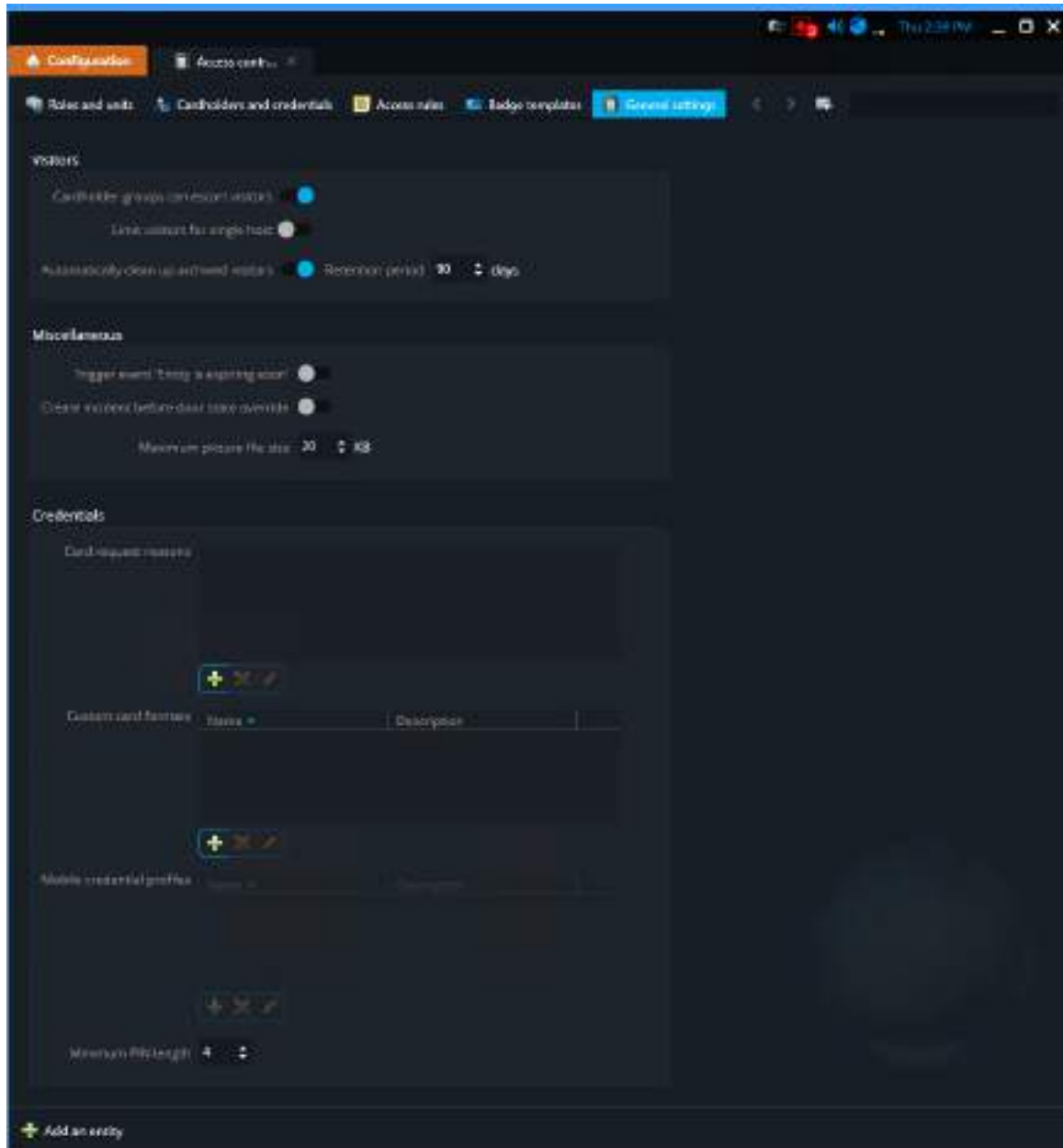
Before you can use QR codes as a credential in Genetec ClearID™, you must configure Synergis™ to support the ClearID QR code custom card format. A QR code can then be used as a credential to access parking entrances, turnstiles, or gated facilities.

What you should know

- Only Security Center SaaS administrators or users with the *modify credential properties* privilege can import the custom card format.

Procedure

- 1 In Genetec™ Configuration desktop, open the *Access control* task and select the **General settings** view.



- 2 In the *Custom card formats* section of *Credentials*, click **Add an item** (+).

 - a) Download this [QRcode.xml](#) file.
 - b) In the *Custom card format editor* dialog, click **Import**.

Custom card format editor

General

Name:

Description:

Code format string:

Card format type: ☒ Wiegand ☐ ABA

Format length: 32 bits

Wiegand fields

Sequence generator:

Parity checks:

Bit position	Mask	Type

Buttons: Export, Import, Validate with a credential, Cancel, OK

IMPORTANT: The card format type that is used during import is **Wiegand** format.

- c) Navigate to and select the *QRcode.xml* file you downloaded.
- d) Click **Open** and click **OK**.

Custom card format editor

General

Name: QR Code (Hex)

Description: ClearID Registration Code

Code format string:

Card format type: ☒ Wiegand ☐ ABA

Format length: 40 bits

Wiegand fields

QR Code
Mask: 0-39

Sequence generator:

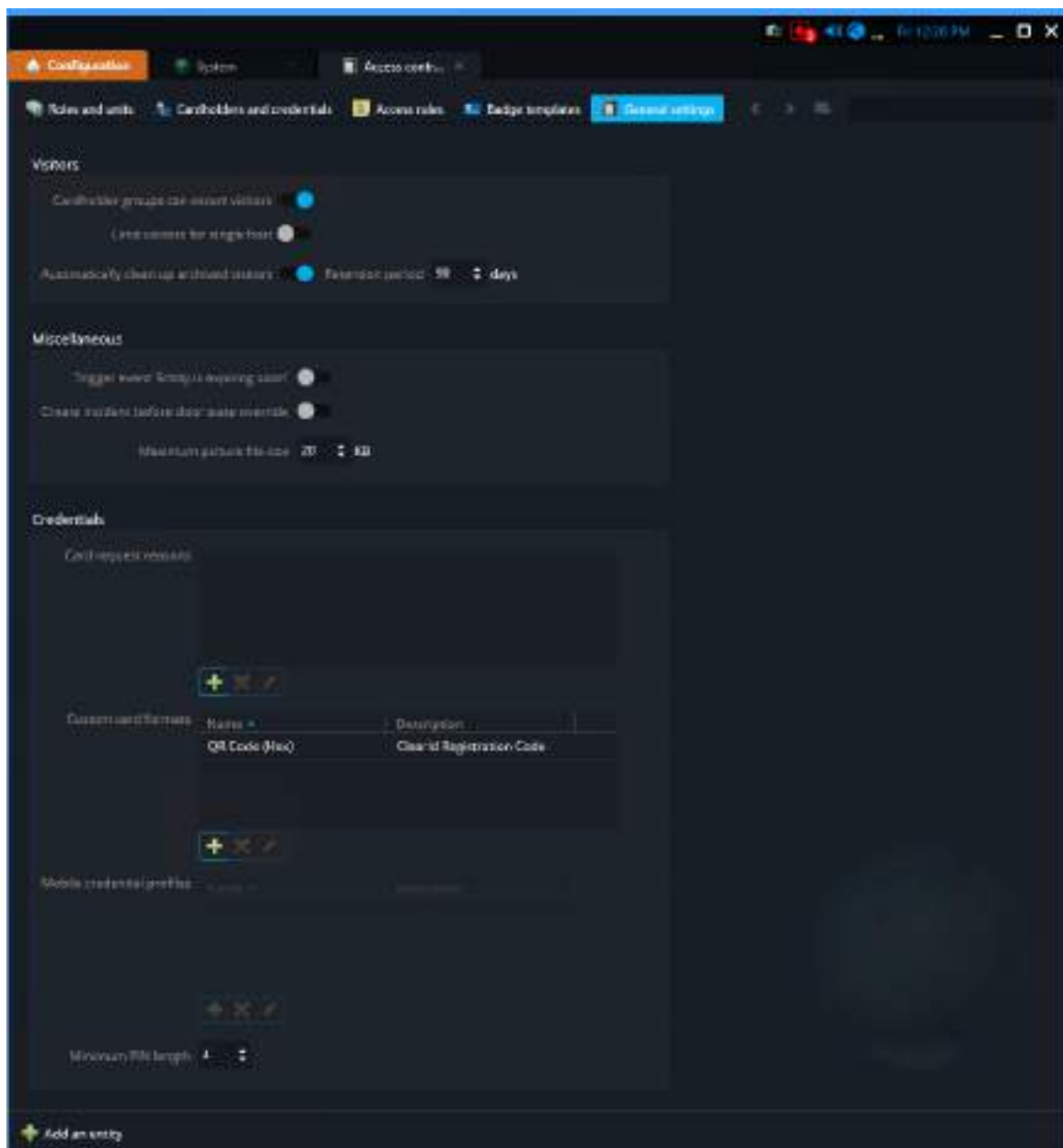
Parity checks:

Bit position	Mask	Type

Buttons: Export, Import, Validate with a credential, Cancel, OK

IMPORTANT: You must use this specific *QRcode.xml* file, because there's a GUID in the file that the ClearID requires.

After you import the *QRcode.xml* file, you can check your settings.



In the *Access control* task **General settings** view, the *Custom card format* for QR code (Hex) is now selected and available.

After you finish

[Enable QR code credentials for visitors.](#)

Enabling QR code credentials for visitors

To automatically create a QR code credential for visitors when a visit request is created, you must enable QR code credentials for visitors.

Before you begin

- [Enable visitor management for sites in Genetec ClearID™](#)
- [Import a custom card format \(QR code credential\) in Synergis™](#)

IMPORTANT: Make sure that the custom card format (QR code) is imported and available in the Security Center SaaS that your site is connected to.

What you should know

Only site owners or account administrators can enable the QR code credentials for visitors.

- When a QR code is automatically created for a visitor, the visitor is created in an inactive state, and the visitor credential contains an automatically generated QR code. The QR code in the credential matches exactly the QR code in the visitor confirmation email.
- The visitor credential is active at this point, but the QR code isn't usable, because the visitor isn't checked in yet. When the visitor check-in occurs, the QR code is valid until the visitor checks out, or the end of the day for the scheduled visit.

For example, QR code credentials for visitors could be used to automatically grant access to a turnstile after check-in.

Procedure

- 1 Click **Organization > Sites**.
- 2 Search for and select a site.
- 3 Click **Visitor management** to configure the visitor management options for a site.
- 4 In the *Advanced* section, select **Automatically create QR code credentials for visitors**.



- 5 Click **Save**.

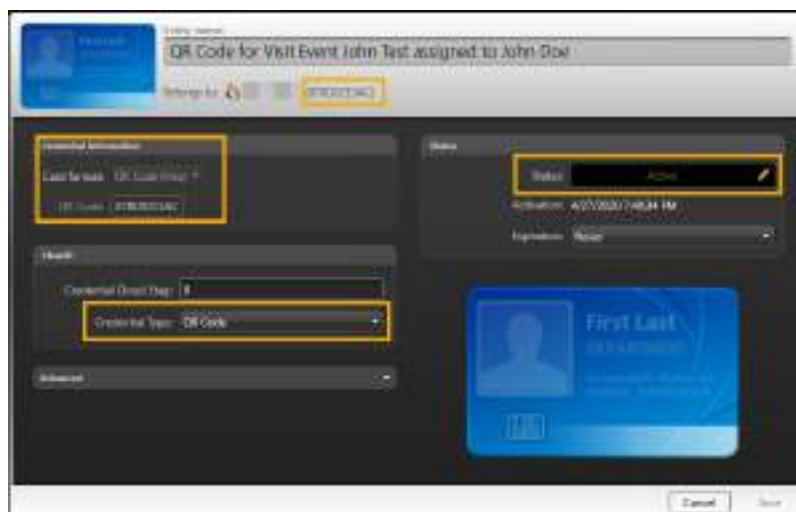
The next time a visitor is invited to the site, ClearID automatically creates a QR code credential for the visitor. The QR code is included in the visitor confirmation email.



After you finish

Perform a visitor invite and check-in test, to validate that QR code credentials are automatically created for visitors.

TIP: You can perform a visitor search in the *Visitor management* task in Genetec™ Operation desktop, then edit the credential to check the visitors' **Credential information**, **Credential type**, and **Status**.



Related Topics

[Enabling visitor management for sites](#) on page 50

Configuring Qscan devices for ClearID

Before you can use QR codes as a credential in Genetec ClearID™, you must configure your Qscan devices to support the custom card format (QR code credential) used in ClearID. A QR code can then be used as a credential to access parking entrances, turnstiles, or gated facilities.

Before you begin

Familiarize yourself with the Qscan documentation:

- [Qscan User Guide \(PDF\)](#)
- [Qscan \(for parking lots\) brochure \(PDF\)](#)
- [QscanT \(for turnstiles\) brochure \(PDF\)](#)
- [QscanI \(indoor version\) brochure \(PDF\)](#)

WARNING: Qscan barcode readers contain a Class 2 laser. Do not look directly into the laser.

What you should know

This procedure is for system integrators or account administrators who install and configure barcode scanners.

The following Qscan devices can be used with ClearID to scan QR codes as a credential for visitors:

- [Qscan \(for parking lots\)](#)
- [QscanT \(for turnstiles\)](#)
- [QscanI \(indoor version\)](#)

Procedure

- 1 [Connect a Qscan barcode reader to a Mercury Controller.](#)
- 2 [Configure Qscan barcode reader to support 40-bit hexadecimal QR codes.](#)

Related Topics

[Supported devices](#) on page 12

Connecting a Qscan barcode reader to a Mercury controller

In situations where you need to use a Qscan barcode reader to access parking entrances, turnstiles, or gated facilities, you must connect a Qscan barcode reader to a Mercury controller. The Mercury controller ensures that the barcode reader can communicate with Security Center Synergis™ to manage access.

Before you begin

WARNING: Qscan barcode readers contain a Class 2 laser. Do not look directly into the laser.

What you should know

This procedure is for system integrators or account administrators who install and configure barcode scanners.

In this scenario, we describe how to connect a Qscan barcode reader to a Mercury EP 1502 controller.

Procedure

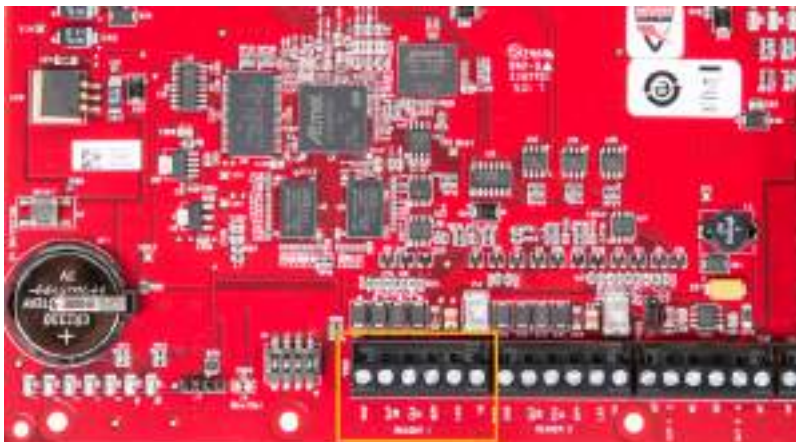
- Connect your Qscan barcode reader device to the Reader 1 connection block in the Mercury EP 1502 controller.



Figure 1: Figure 1: Qscan barcode reader



Figure 2: Figure 2: Mercury EP1502 controller boards



NOTE: The Mercury controller boards can vary in color depending on when they were manufactured and purchased.



Figure 3: Mercury EP1502 controller board wiring loom connections

Use the following table to understand how to connect the Qscan barcode reader wires to the terminals on the Mercury controller *Reader 1* connector block.

Mercury controller and Qscan reader wiring connections

Mercury EP1502: Reader 1 connections	Qscan barcode reader: wire colors
GND (Ground)	BLUE
DAT D0 (Data/Data 0/TR-)	GREEN
CLK D1 (Clock/Data 1/TR+)	WHITE
BZR (Reader Buzzer)	Not applicable
LED (Reader LED)	ORANGE
V0 (Reader Power)	RED

After you finish

[Configure Qscan barcode reader to support 40-bit hexadecimal QR codes](#)

Configuring a Qscan barcode reader to support 40-bit hexadecimal QR codes

Before the QR codes automatically generated by Genetec ClearID™ for visitor confirmation email notifications can be understood and processed by Synergis™ Cloud Link during check-in, you must configure your Qscan barcode reader to support 40-bit hexadecimal QR codes.

Before you begin

[Connect Qscan barcode reader to Mercury controller](#)

WARNING: Qscan barcode readers contain a Class 2 laser. Do not look directly into the laser.

What you should know

This procedure is for system integrators or account administrators who install and configure barcode scanners.

In this scenario, we describe how to program Qscan devices to support 40-bit hexadecimal QR codes used in ClearID and output to Synergis Cloud Link.

For example, a QR code when scanned by Qscan is typically read as alphanumerics `ABC1234567`.

Synergis Cloud Link requires the QR code in HEX format `0xAB 0xC1 0x23 0x45 0x67` to manage access requests.

CAUTION: The steps described in the following process remove alphanumeric QR code support from the Qscan barcode reader. The Qscan barcode reader can't be used in alphanumeric mode while the 40-bit hexadecimal mode is active.

Procedure

- 1 To reset to factory default settings, scan the [qscan resetbarcode1.pdf](#) barcode.



NOTE: The Qscan reader beeps twice if the factory reset is successful.

- 2 To ignore alphanumeric characters, scan the [qscan no alpha delete.pdf](#) barcode.



- 3 To turn HEX conversion on, scan the [qscan hex conversion.pdf](#) barcode.



- 4 To output 40-bits, scan the [qscan 40-bit.pdf](#) barcodes.

NOTE: This file has three barcodes so scan one at a time.



Configuring STid devices for ClearID

Before you can use QR codes as a credential in Genetec ClearID™, you must configure your STid devices to support the custom card format for QR codes used in ClearID. A QR code can then be used as a credential to access parking entrances, turnstiles, or gated facilities.

Before you begin

Familiarize yourself with the STid documentation:

- [Architect® Blue QR code readers](#)
 - [ARCS-AQ/BT - 13.56 MHz + Bluetooth® + QR Code multi-technology reader](#)
- [SECard - High security programming kits](#)
- [SECard User Manual](#)

What you should know

This procedure is for system integrators or account administrators who install and configure QR code readers.

In this scenario, we describe how to program STid devices to support 40-bit hexadecimal QR codes used in ClearID and output to Synergis™ Cloud Link.

Procedure

- 1 [Learn about STid QR code readers.](#)
- 2 [Import custom card format.](#)

- 3 Set up and connect your QR code reader to your access control panel.

NOTE: The steps you must perform vary depending on your access control panel.

- To connect your OSDP reader to Synergis Cloud Link, see [OSDP readers connected to the Synergis Cloud Link RS-485 ports](#).
- To connect your OSDP reader to Mercury, see [Adding OSDP \(Secure Channel\) readers to a Mercury controller](#).

- 4 [Creating an STid QR code reader configuration](#) on page 118.

- 5 [Transferring your reader configuration to your STid QR code reader](#) on page 132.

After you finish

[Add doors to areas.](#)

About STid QR code readers

In Genetec ClearID™, STid QR code readers can be used to read QR code credentials.



NOTE: The image shown here illustrates STid readers that you might have in your organization. For a list of the Open Supervised Device Protocol (OSDP) readers that ClearID supports, see [Supported devices for ClearID](#).

Why choose the OSDP protocol over the Wiegand protocol?

WIEGAND Protocol

In Wiegand the reader always sends a fixed-length wiegand format, regardless of the credential length. The *custom card format* called by Genetec™ Operation desktop is always the same. The manufacturer has confirmed this Wiegand readers (SY-ARCS-R31-AQBT1-XX1) limitation.

Consequence: An *Unknown credential* message is displayed in Genetec Operation desktop when the credential doesn't match the length required by the protocol. The message is displayed even if the QR code credential is already enrolled in the Security Center Synergis™ database.

Workaround: To make sure that all types of credentials work simultaneously with Wiegand protocol readers and Synergis, all other credentials (RFID or QR code from another source such as Axis) should match the ClearID QR code credential length (40 bits). This approach ensures that Synergis always receives the same *custom card format* from ClearID and correctly interprets all types of payloads that the reader sends.

OSDP Protocol

In Open Supervised Device Protocol (OSDP) the reader dynamically adapts the format length regarding the credential length.

BEST PRACTICE: Use OSDP with STid QR code readers to ensure that the QR code credential is accepted and understood.

The following table shows example reads from the same reader.

Credential code	Card format	
4AE6CD6464E	QR code (HEX)	ClearID QR code
E01EC72022429729	64 bits	DESFire 64 bits private ID credentials

The examples show that the *custom card format* called by Genetec Operation desktop is different for each read.

Consequence: The OSDP reader is more flexible and correctly interprets the credential.

Planning your QR code reader deployment

Depending on your needs, you can use the latest STid Architect® Blue QR code readers. Alternatively, you can add interchangeable QR code modules if you want to reuse existing STid readers.



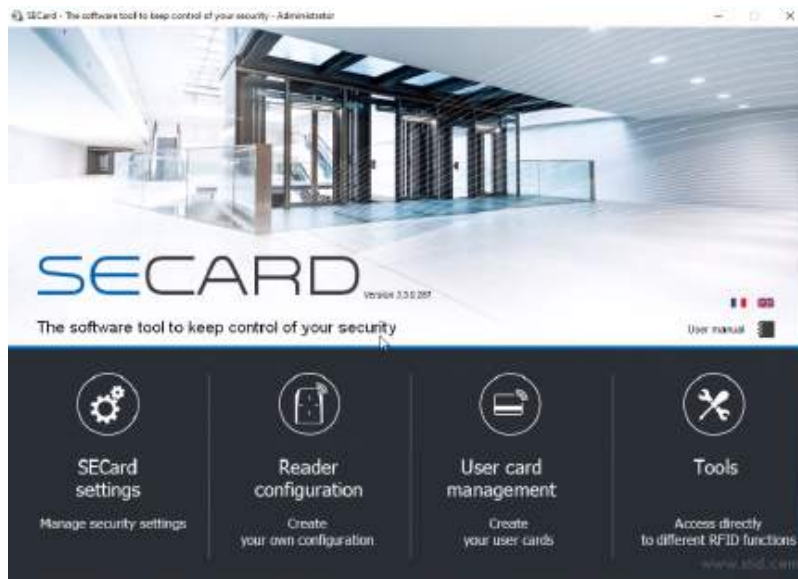
Consider the following when planning your STid QR code reader implementation:

- **BEST PRACTICE:** If you're planning a new STid QR code reader implementation, consider using the latest QR code readers with the latest firmware. For example, model: ARCS-AQ/BT. Only use STid readers that support the OSDP protocol and have upgraded to **firmware version 10**.
- If you already have numerous STid readers deployed in your organization, consider adding the interchangeable QR code reader module and updating your firmware.
TIP: Using the interchangeable module upgrades can result in significant savings on a large project.
- If you're re-using existing readers, refer to *STid documentation* about how to upgrade your reader to **firmware version 10** or later.

Programming your STid QR code readers

The STid QR code readers can be programmed using the *STid SECard - High security programming kit*.

BEST PRACTICE: Use STid **SECard software version 3.5** or later to configure your STid QR code readers.



The KIT-SECARD-BT-V3.X includes the following:

- STid Architect® ARC-G desktop reader, enroller, encoder



- USB key containing the STid SECard software



IMPORTANT: Genetec Inc. doesn't provide support for the STid SECard solution. Customers must use the stand-alone STid SECard software to configure the OSDP readers to work with the ClearID ACS panel solution.

Related Topics

[Supported devices](#) on page 12

Creating an STid QR code reader configuration

Before you can use QR codes as a credential in Genetec ClearID™, you must create your STid QR code reader configuration. A QR code can only be used as a credential for an STid QR code reader after the QR code reader configuration has been uploaded to an STid OCB smart card and then transferred to the reader.

Before you begin

Familiarize yourself with the STid documentation:

- [SECard - High security programming kits](#)
- [SECard User Manual](#)
- Install the STid SECard - High security programming kit software.

What you should know

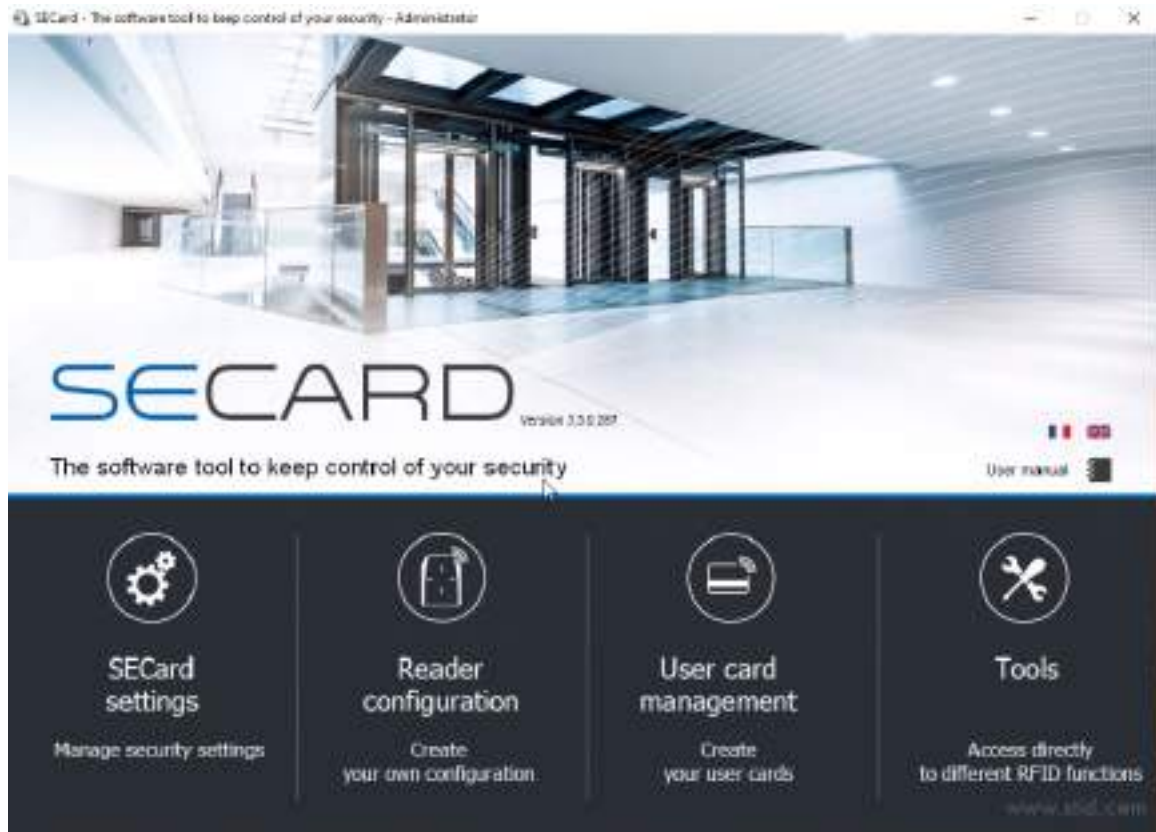
This procedure is for system integrators or account administrators who install and configure QR code readers.

NOTE: The STid SECard software requires a license. The number is typically found on the USB reader that is used to encode a smart card.

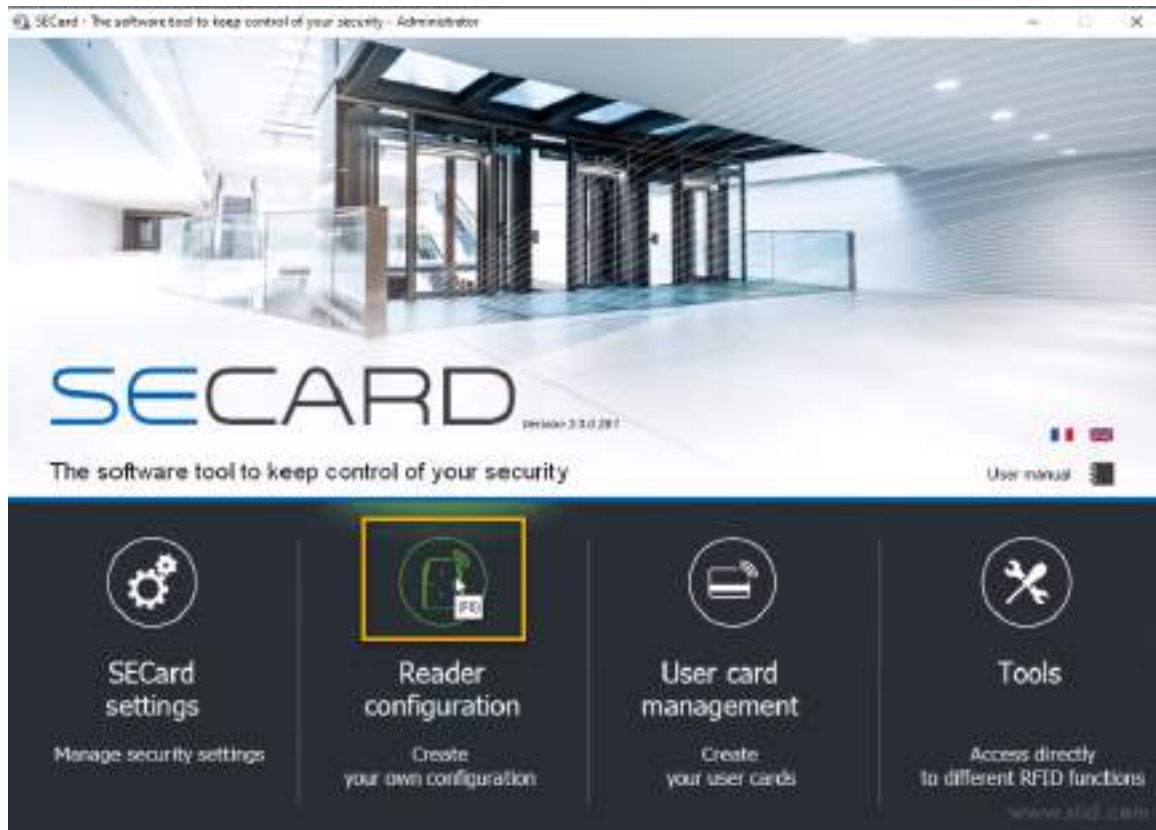


Procedure

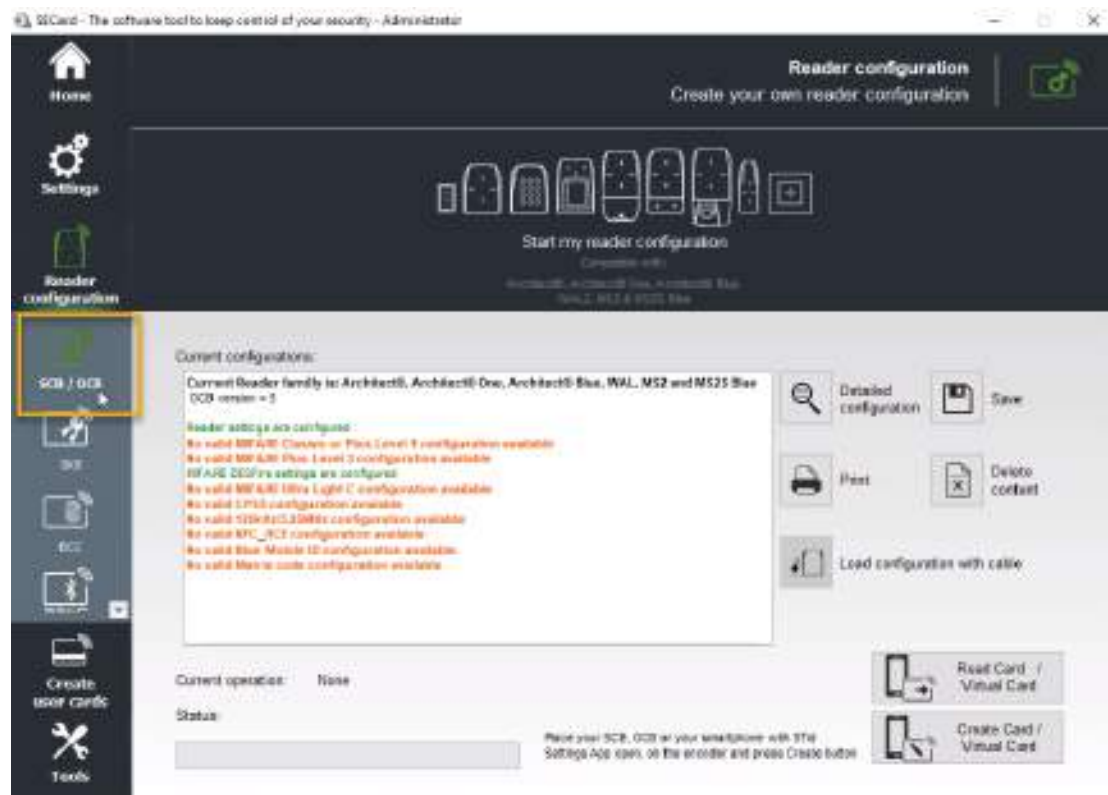
- 1 Open the STid SECard - High security programming kit software to configure your STid QR code reader.



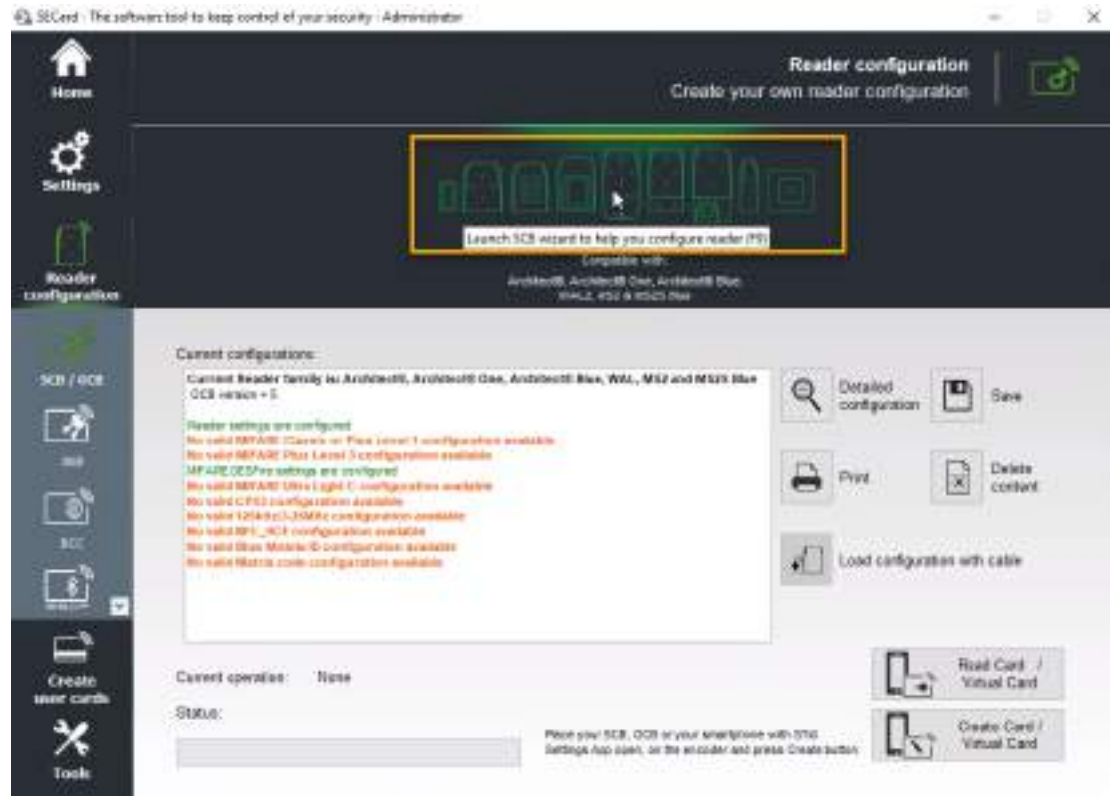
- 2 Click **Reader configuration**.



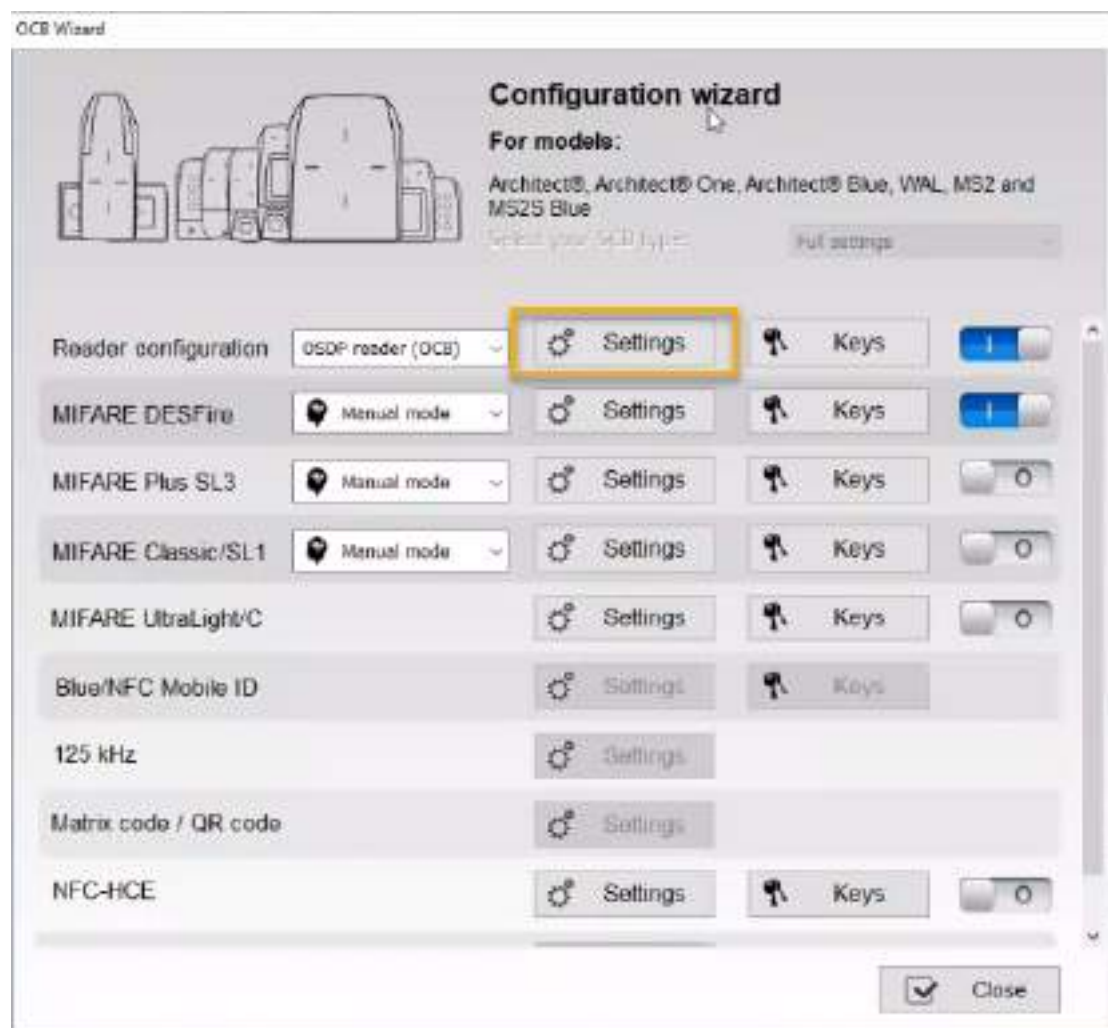
- a) In the navigation sidebar, click **SCB / OCB**.



- b) Click the readers image at the top of the screen to launch the SCB wizard.



- c) In the *Reader configuration* row, next to OSDP reader (OCB), click **Settings** to open the Configuration wizard.



- 3 In the *Configuration wizard* dialog, select **SECard V3.5 x OCBv5** and click **Next**.

OCB Wizard

Configuration wizard

Create your OCB reader configuration card

Wizard configuration steps for ODSP reader:

- Reader selection and security options
- Reader communication protocol
- LED and Buzzer
- Keypad and biometrics
- Touchscreen options
- Bluetooth® / NFC options
- Matrix code / QR Code options and settings

The functions available with the configuration card (OCB) depend on the generation of the reader's firmware.
You must choose the version corresponding to your reader generation.

[Click to view firmware compatibilities array](#)

Choose SECard version to use

SECard V3.5.x OCBv5
SECard V3.3.x OCBv3
SECard V3.4.x OCBv4
SECard V3.5.x OCBv5

 Get configuration from SCB wizard

[Click to view compatibilities ARC/ARCS, ARC1/ARC1S and WAL2](#)

Back Next Cancel

- a) In the *Reader reference selection* dialog, select the **Matrix / QR Code** checkbox and click **Next**.

OC8 Wizard

Reader reference selection

Choose reader type and options to configure

1 2 3 4 5 6 7 8

Features activation

☐ Keypad

☐ Touchscreen

☐ Blue/NFC Mobile ID

☐ Biometric

☐ Prox 125 kHz

☒ Matrix code / QR code

Reader protection options

☒ Save user keys in non volatile memory

☒ Tamper switch signal

☒ Erase keys on tamper switch activation

Accelerometer sensitivity

☐ On tamper activation keeps LED red as default

Low

Back Next Cancel

b) In the *Reader parameters* dialog *Protocols* section, select the Type **RAW** and click **Next**.

OCB Wizard

Reader parameters

Protocol and options

1 2 3 4 5 6 7 8

Private ID security

☐ Data authenticated encryption

Protocols

Type

☒ RAW ☐ Wiegand

☐ Use protocol size Byte(s)

☒ Backward compatibility

☒ Justify data to left ☐ Justify data to right

Protocol options

☐ Forced site code on UID

☐ 2 bytes Value

☐ Enable Plain mode after secure channel authentication

☒ Use ACK instead of Busy command

Offset bit(s)

☐ Change RS485 address

Baudrate

☒ No wrap text

ISO14443-3B PUPi / IClass

☐ Enable

Card ID range filter (LSB)

UID/ID range to

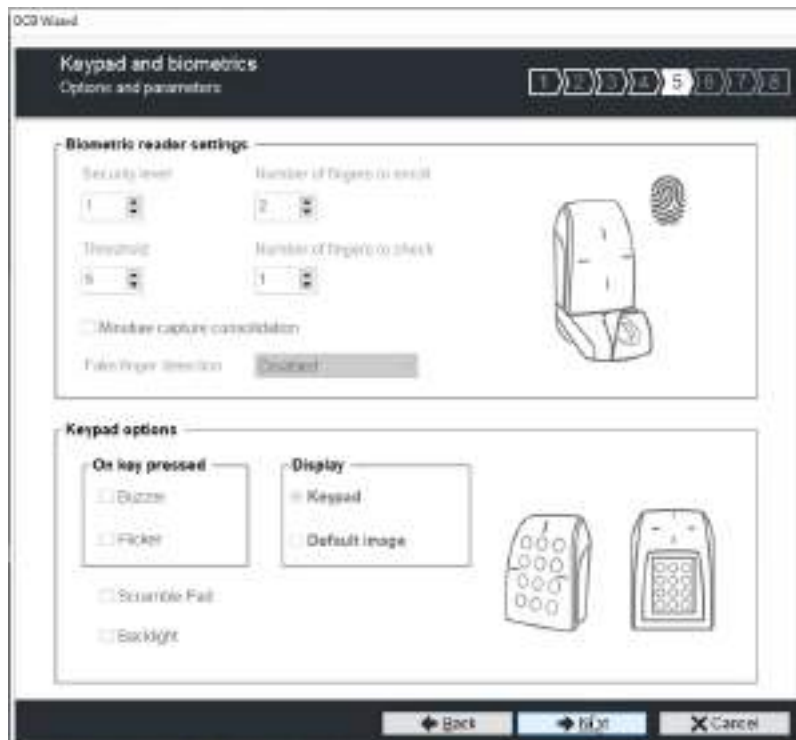
Back Next Cancel

NOTE: When the **Use protocol size** checkbox isn't selected, the **Byte(s)** setting is ignored. Not selecting a protocol size ensures that the reader can adapt the length according to the length of the credential.

- 4 The following steps (4.a on page 126 - 4.d on page 127) aren't essential for QR code use, but might still be relevant to your installation.
- a) Click **Next** to skip the *LED and Buzzer* dialog.



- b) Click **Next** to skip the *Keypad and biometrics* dialog.



- c) Click **Next** to skip the *Touchscreen options* dialog.



d) Click **Next** to skip the *Blue/NFC Mobile ID options* dialog.



- 5 In the *Matrix code types to be read* section of the *Matrix code / QR code* dialog, select the **QR code** checkbox only. Then in the *Matrix code format* section, select the **Hexadecimal** checkbox. These settings specify that a 2D QR code can be read and sent in hexadecimal format.

OCB Wizard

Matrix code / QR code

Settings and Reading options

1 2 3 4 5 6 7 8

Matrix code types to be read

Code 2D

☐ Data Matrix

☒ QR code

☐ Aztec code

Code 1D

☐ Code 128

Matrix code format

☒ Hexadecimal

☐ Decimal

☐ ASCII

☐ RAW

Ambient lighting

☐ Eco mode ⓘ

☒ Standard mode / Night & day ⓘ

☐ Intense lighting mode ⓘ

Advanced settings

Lighting beam brightness

Intense

Lighting beam target

High

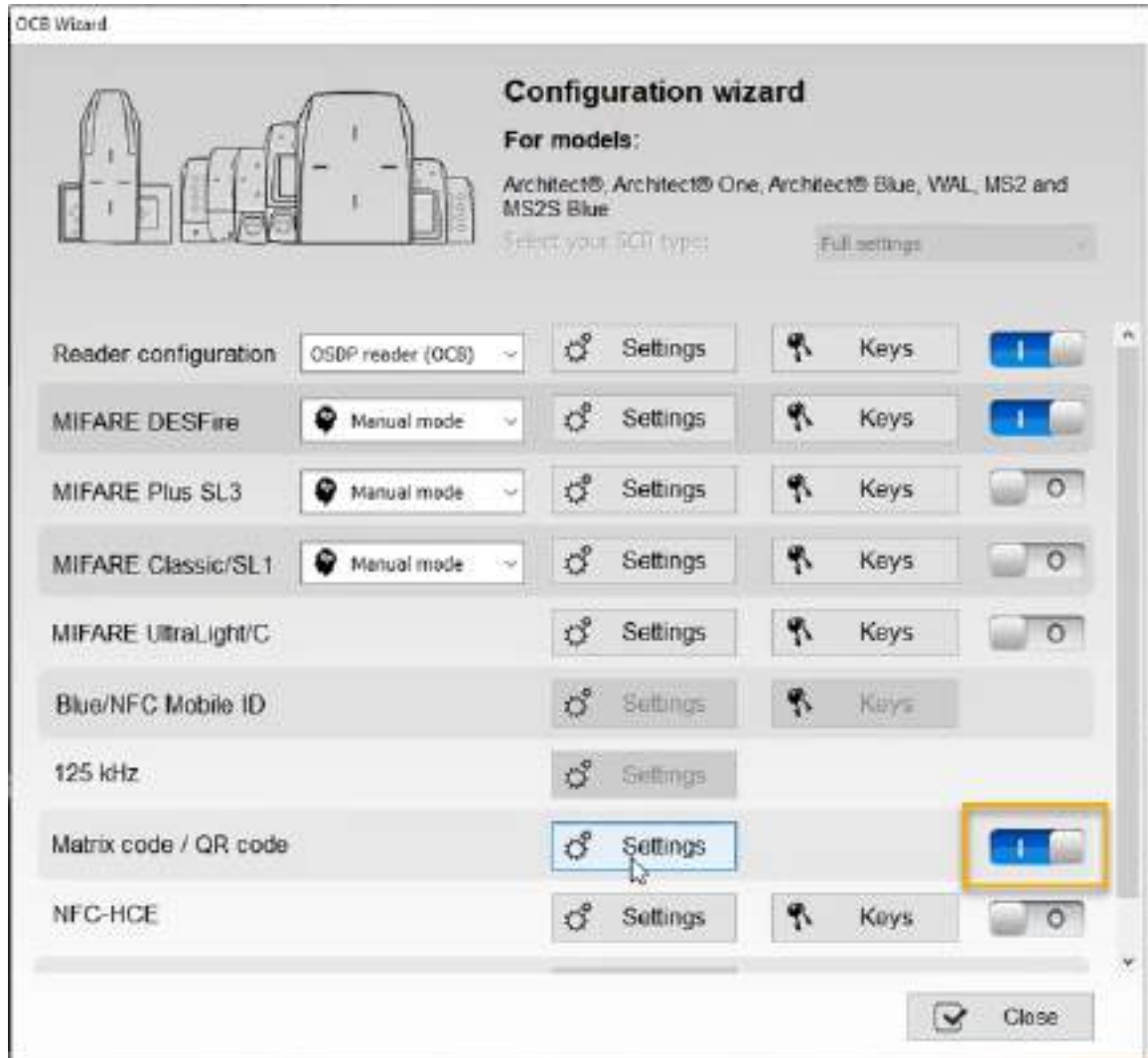
Detection sensitivity

Normal

Back Validate Cancel

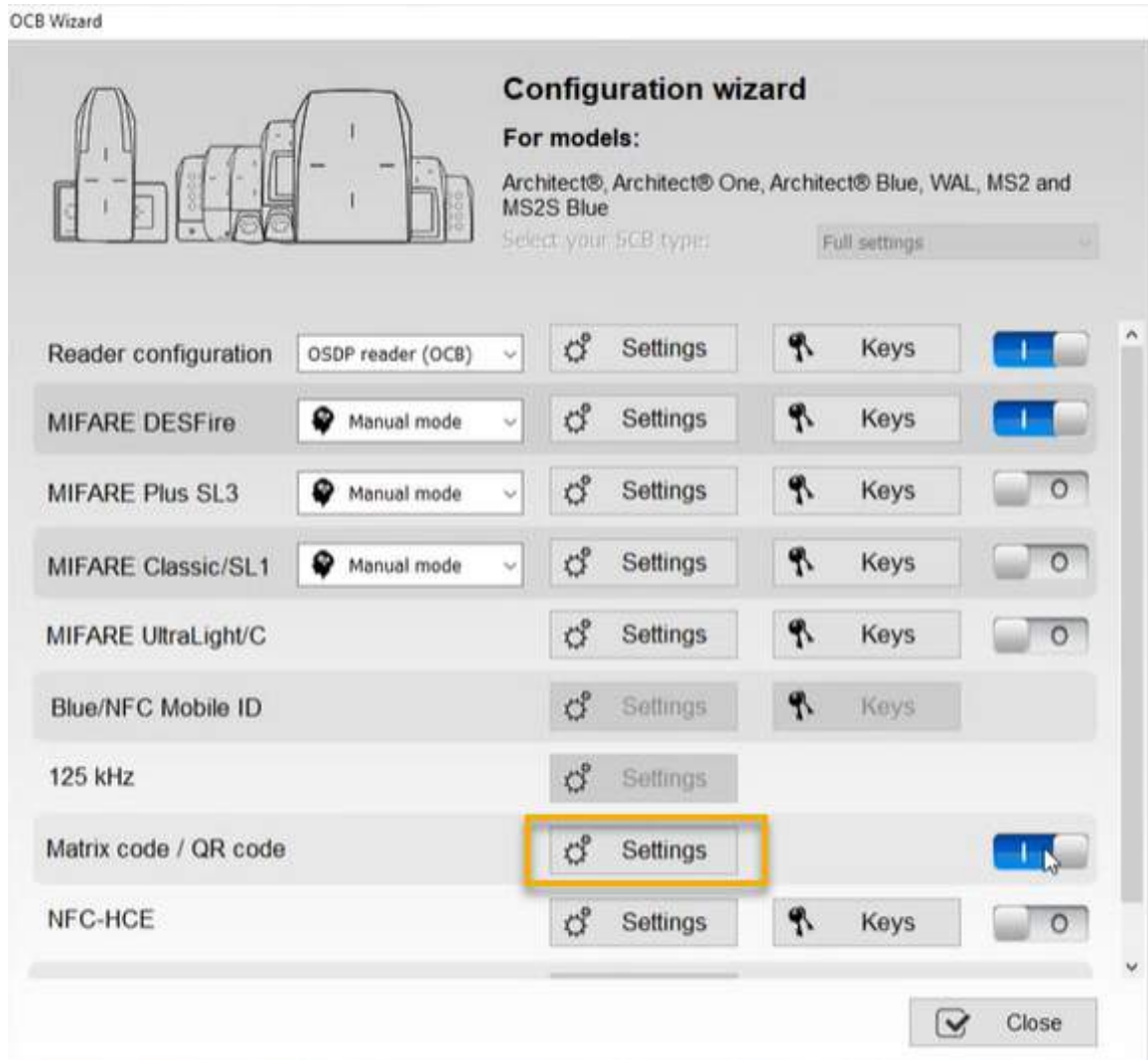
- a) (Optional) In the *Ambient lighting* section, modify the settings if required.
- b) Click **Validate**.

- 6 In the *Matrix code / QR code* row, drag the slider to the enabled position.



TIP: If the *Matrix code / QR code* section isn't available for selection in the Configuration wizard, make sure that you've validated your Reader configuration as detailed earlier.

- 7 In the *Matrix code / QR code* row, click **Settings**.



- a) In the *Matrix code / QR code settings* dialog, use the default settings and click **Validate**.

OCB Wizard

Matrix code / QR code settings



Current configured matrix code format: Hexadecimal

Data read

☒ All
Maximum 192 chars

☐ Selection

Settings

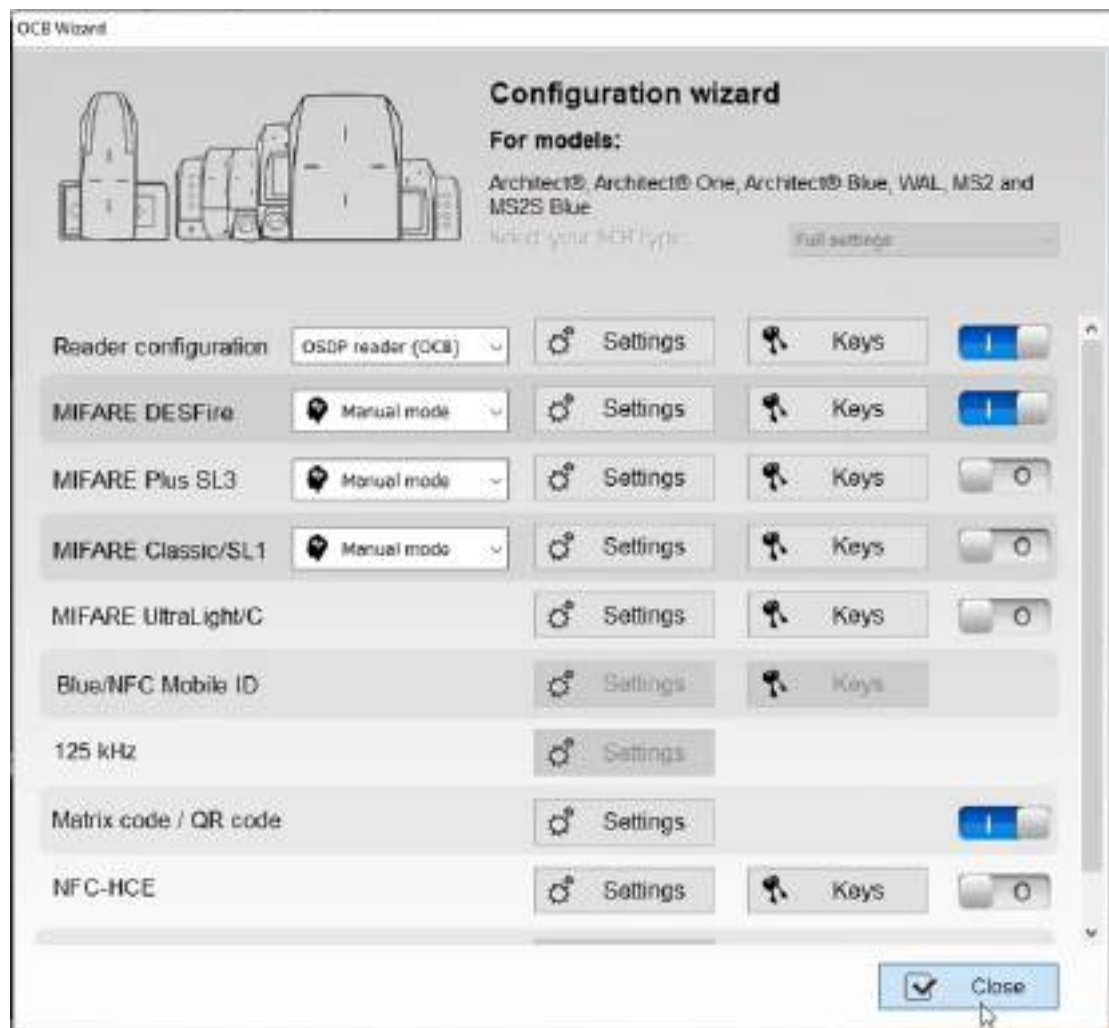
Size: char

Offset: char

Reverse: ☐

☒ Validate ☐ Cancel

b) Click **Close**.



Your STid QR code reader configuration has now been created.

After you finish

[Transfer your reader configuration to your STid QR code reader.](#)

Transferring your reader configuration to your STid QR code reader

Before you can use QR codes as a credential in Genetec ClearID™, you must complete your STid QR code reader configuration by configuring an STid OCB smart card so that you can transfer the reader configuration to the STid QR code reader.

Before you begin

Familiarize yourself with the STid SECard documentation:

- [SECard - High security programming kits](#)
- [SECard User Manual](#)
- Install the software for the STid SECard - High security programming kit.
- [Create your STid QR code reader configuration.](#)

What you should know

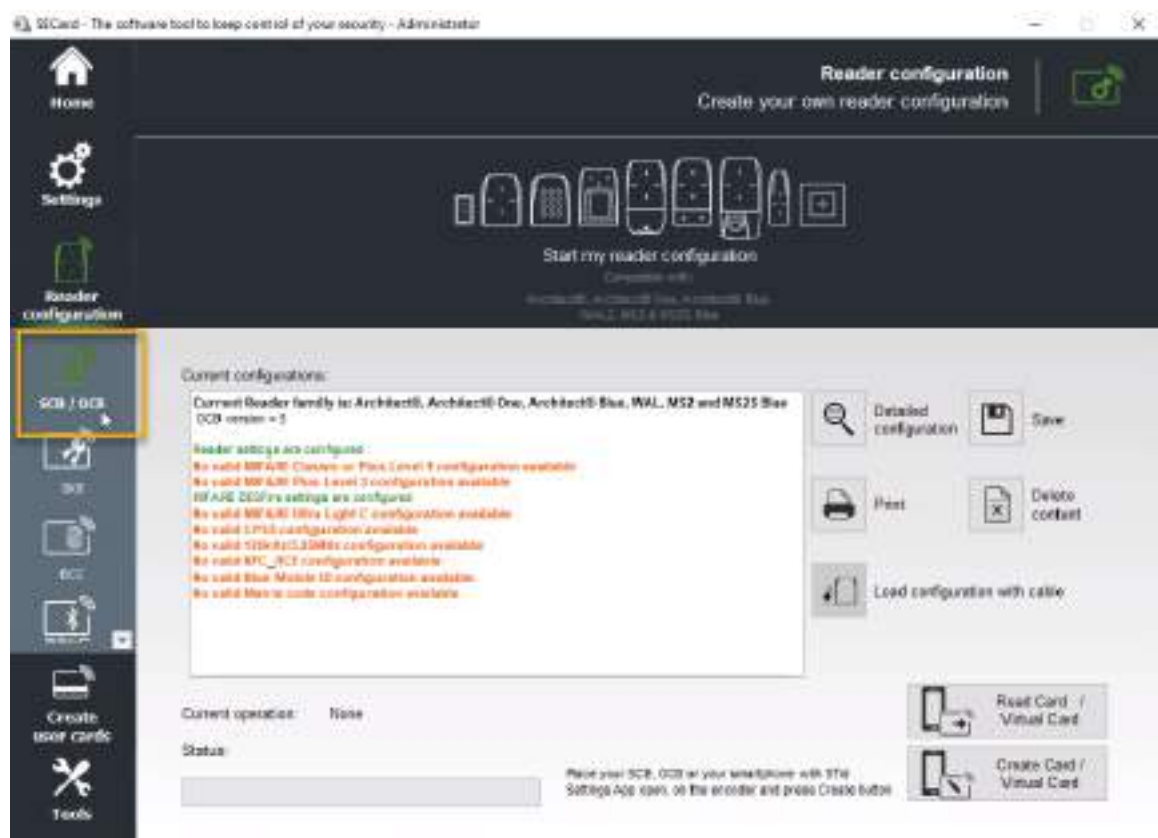
This procedure is for system integrators or account administrators who install and configure QR code readers.

NOTE: Ensure that you have a USB encoder installed and ready to configure your OCB card. For example, the STid Architect® ARC-G desktop reader, enroller, encoder.



Procedure

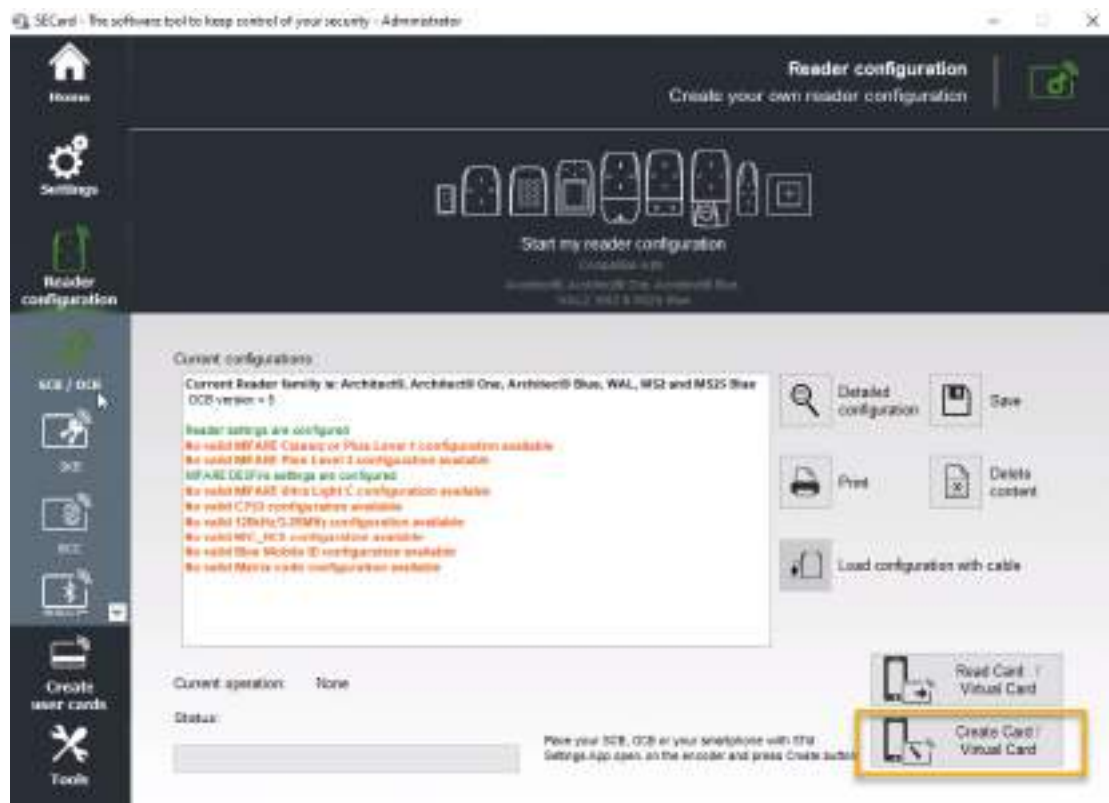
- 1 Launch the STid SECard software to configure your card.
- 2 In the navigation sidebar, click **SCB / OCB**.



- 3 Create your STid OCB card.
 - a) Place the OCB card on your USB encoder (reader).



- b) Click **Create Card / Virtual Card** to create your configuration card.



- 4 Take the OCB smart card containing your reader configuration to the new QR code reader location and pass the card in front of the reader.



NOTE: Your new QR code reader must be online and available to transfer the configuration settings from the smart card to your QR code reader.

- 5 Verify that your QR code reader is still active after the OCB has been swiped on the wall reader.

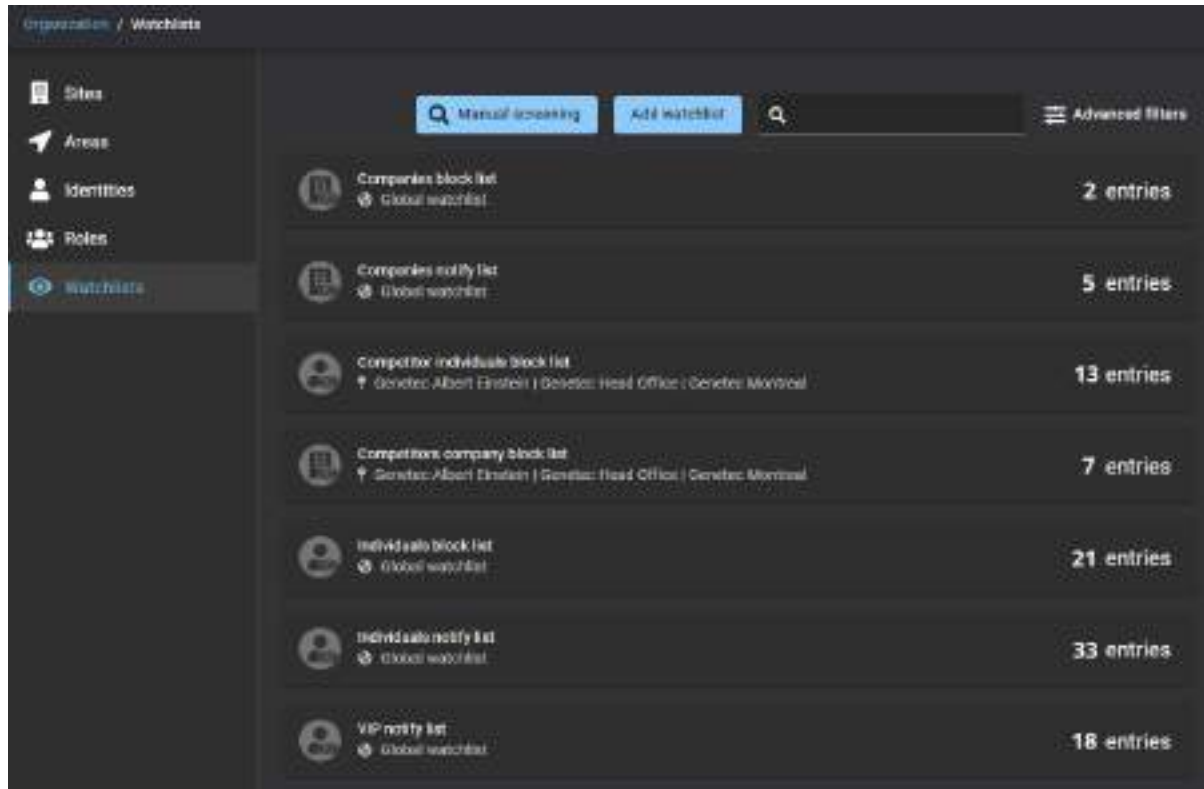
After you finish

[Add doors to areas.](#)

Managing visitor watchlists

About watchlists

In Genetec ClearID™, watchlists are used to screen visitors at an individual or company level. You can configure the watchlist to perform allow, block, or notify actions at a site or global level.



Screening matches only occur when the following applies:

- Individuals: There is a **First name** and **Last name** match, **First name** and **Last name** alias match, or **Email** address match.
- Companies: There is a **Company** name, company domain, or email address domain match.

There are two types of watchlist:

- Individuals watchlist
- Companies watchlist



An **Individuals** watchlist is used to monitor visitor check-ins for *persons of interest* listed in a watchlist and then take action as specified in the watchlist configuration. For example, you might create an individuals watchlist to automatically block visitors listed in a watchlist and notify watchlist managers. For other situations, you might only notify watchlist managers. You might also create an individuals watchlist to notify all watchlist managers when VIPs check-in at your site.



A **Companies** watchlist is used to monitor visitor check-ins for *companies of interest* listed in a watchlist and then take action as specified in the watchlist configuration. For example, you might create a companies watchlist to automatically block access for people with a **Company** name, company domain, or email address domain that matches specific companies of interest listed in this watchlist.

NOTE: The *Individuals* or *Companies* listed in the entries inside a watchlist can be entered individually or imported as a whole using a .CSV file.

Watchlist behavior

The behavior of the watchlists can be configured differently as follows:

- Notify watchlist managers.
- Automatically block visitors listed in a watchlist and notify watchlist managers.

Global watchlists

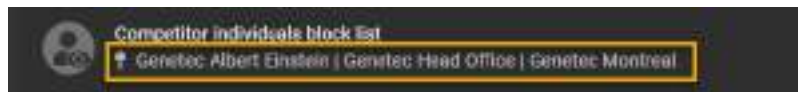
Global watchlists are highlighted using a world globe identifier (🌐) in the watchlist view as follows:



Site watchlists

If a watchlist is not configured as a *global watchlist*, it's considered a site-level watchlist and can be applied to one or more sites.

Site-level watchlists are highlighted using a site identifier (📍), followed by one or more sites, in the watchlist view as follows:



Reasons to block or notify

Reasons to block entry to visitors listed in a watchlist, or notify a watchlist manager might include one or more of the following:

- Serious criminal records by Government agency
- Violent activity or threats
- False Credentials
- Contraband items
- Theft
- Safety violation
- Other reasons

NOTE: Only a *watchlist manager* can view the reasons why visitors are in notify or block watchlists.

Adding watchlist managers

Before you can add or modify watchlists or configure watchlist settings, you must add your watchlist managers.

Before you begin

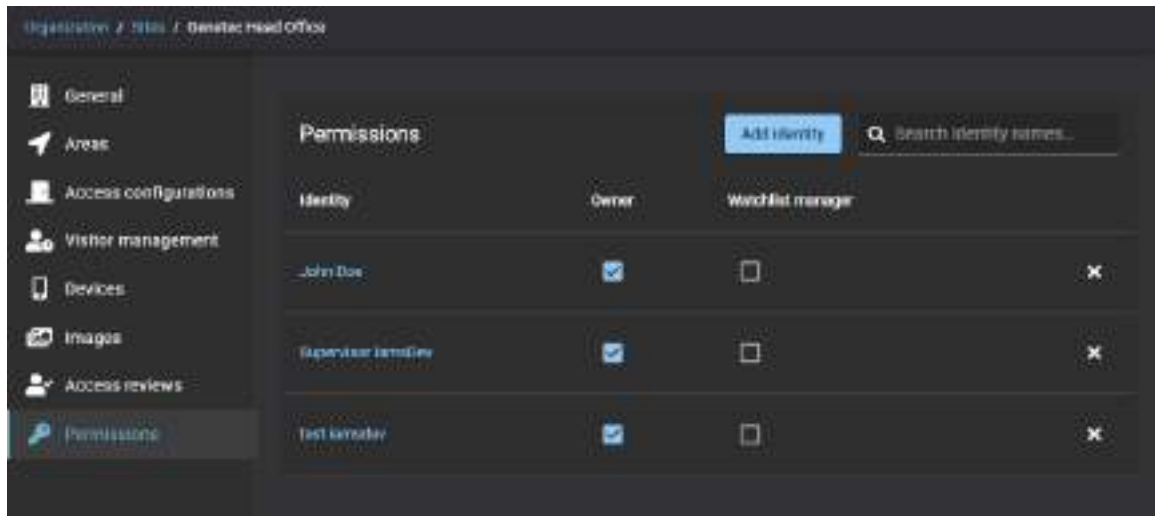
[Create your sites.](#)

What you should know

To add watchlist managers in Genetec ClearID™, you must be an account administrator.

Procedure

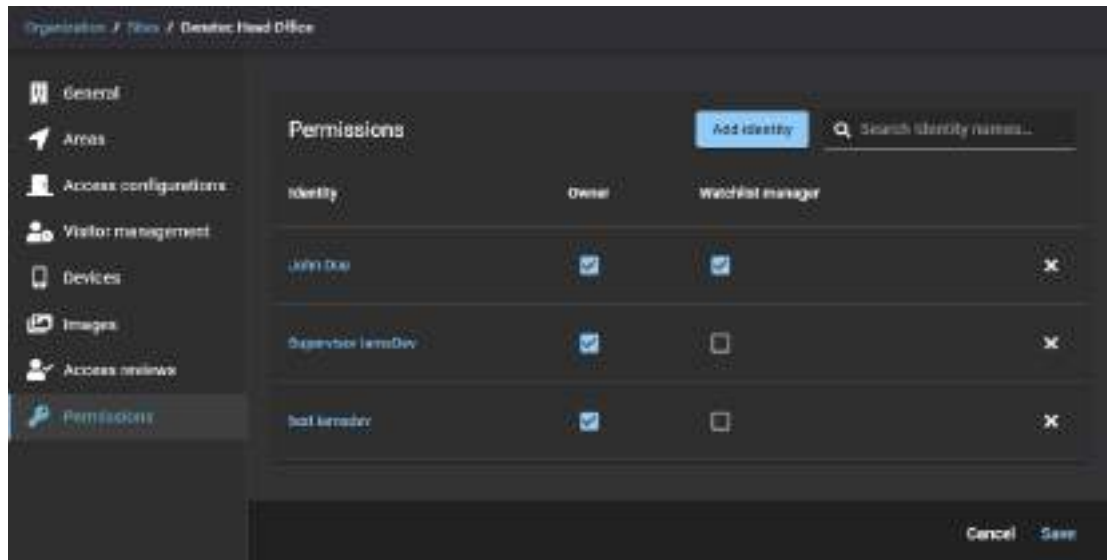
- 1 Click **Organization > Sites**.
- 2 Select your site and click **Permissions**.
- 3 (Optional) Click **Add identity** to add identities to the site **Permissions** list.



- a) Search for or select one or more identities and click **Add**.

TIP: You can click the identity hyperlink in the **Identity** column to review identity details (company, department, home site, supervisor, and email) and to verify that you have the correct identities in the list.

- 4 Select the **Watchlist manager** checkbox to assign watchlist manager permissions to an identity.
 - a) (Optional) Clear a checkbox to remove individual permissions that are no longer required from an identity.
 - b) (Optional) Click  to remove all permissions that are no longer required from an identity.



- 5 Click **Save**.

After you finish

[Add your watchlists.](#)

Adding watchlists

Add an individuals watchlist or companies watchlist so that you can screen individuals or companies and automatically perform block or notify actions at a site or global level as specified in the watchlist configuration.

Before you begin

[Learn about watchlists.](#)

What you should know

- Any *watchlist manager* or account administrator can modify or delete any watchlist that is configured as a *global watchlist*.

Procedure

- Click **Organization > Watchlists**.
- Click **Add watchlist**.

The screenshot shows the 'New watchlist' configuration form. At the top, there is a toggle switch for 'Enabled' which is turned on. Below this, there is a 'Type' dropdown menu currently set to 'Individuals'. Underneath the dropdown are three text input fields labeled 'Name', 'Address', and 'Description'. The form is divided into three sections: 'Watchlist behavior' with two radio button options ('Notify watchlist managers' is selected), 'Watchlist settings' with a checked checkbox for 'Global watchlist that applies to all sites in your system', and 'Watchlist entry permissions' with two radio button options ('Assign a watchlist entry permission for each watchlist entry' is selected). At the bottom left is a 'Cancel' button and at the bottom right is a 'Save' button.

- 3 At the top of the new watchlist, click the **Enabled** slider to enable or disable the watchlist.
- 4 In the **Type** field, select a watchlist type. From the list, select either **Individuals** or **Companies**:
 - **Individuals:**  An **Individuals** watchlist is used to monitor visitor check-ins for *persons of interest* listed in a watchlist and then take action as specified in the watchlist configuration. For example, you might create an individuals watchlist to automatically block visitors listed in a watchlist and notify watchlist managers. For other situations, you might only notify watchlist managers. You might also create an individuals watchlist to notify all watchlist managers when VIPs check-in at your site.
 - **Companies:**  A **Companies** watchlist is used to monitor visitor check-ins for *companies of interest* listed in a watchlist and then take action as specified in the watchlist configuration. For example, you might create a companies watchlist to automatically block access for people with a **Company** name, company domain, or email address domain that matches specific companies of interest listed in this watchlist.
- 5 Enter a **Name** for the watchlist.
The name of a watchlist can be changed at any time to suit your needs.
TIP: Consider using a *discrete name* where applicable. This discrete name avoids divulging sensitive information about why someone might be blocked or on a list when the notification is sent to people.
- 6 Enter a **Description** for the watchlist.
- 7 In the *Watchlist behavior* section, select one of the following:
 - **Notify watchlist managers**
 - **Automatically block visitors listed in a watchlist and notify watchlist managers**
- 8 In the *Watchlist settings* section, choose whether you want a global watchlist or a site-specific watchlist.
 - To apply the watchlist to all sites in your system, select **Global watchlist that applies to all sites in your system**.
 - To apply the watchlist to one or more specific sites, clear the **Global watchlist that applies to all sites in your system** checkbox.
 - a) If you chose to apply your watchlist at a site level, add your sites and press enter.
 - b) Repeat at necessary.

NOTE: The *Watchlist entry permissions* section is disabled if the **Global watchlist that applies to all sites in your system** checkbox is selected.

- 9 If you have **Watchlist entry permissions** activated for your account, in the *Watchlist entry permissions* section, select one of the following:
- **All watchlist managers can modify or delete watchlist entries:** All watchlist managers can modify or delete watchlist entries.
 - **Assign a watchlist entry permission for each watchlist entry:** Watchlist entry permissions are assigned at a more granular site level in each watchlist entry. This means that only watchlist managers for the site can modify or delete entries.

Example:

New watchlist ☒ Enabled

Type*
Individuals

Name*
Individuals BLOCK list

Description
Automatic block GLOBAL watchlist all sites

Watchlist behavior

☐ Notify watchlist managers

☒ Automatically block visitors listed in a watchlist and notify watchlist managers

Watchlist settings

☒ Global watchlist that applies to all sites in your system

Watchlist entry permissions

☐ All watchlist managers can modify or delete watchlist entries

☒ Assign a watchlist entry permission for each watchlist entry

Cancel Save

Figure 4: Example 1: Individuals block watchlist - configured as a global watchlist to automatically block visitors and notify watchlist managers.

Example:

New watchlist ☒ Enabled

Type: Companies

Name: Companies NOTIFY list

Description: Notify when visitors from Competitor company visit specific sites

Watchlist behavior

☒ Notify watchlist managers

☐ Automatically block visitors listed in a watchlist and notify watchlist managers

Watchlist settings

☐ Global watchlist that applies to all sites in your system

Watchlist sites

Genetec Albert Einstein Genetec Head Office Genetec Montreal [Add more](#) To add a site, start typing and press Enter

Watchlist entry permissions

☒ All watchlist managers can modify or delete watchlist entries

☐ Assign a watchlist entry permission for each watchlist entry.

Cancel [Save](#)

Figure 5: Example 2: Companies notify watchlist - configured as a site-specific watchlist to notify watchlist managers when visitors are from a competitors company.

10 Click **Save**.

Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



After you finish

Do one or more of the following:

- [Add your individuals watchlist entries](#)
- [Add your companies watchlist entries](#)

Adding an individuals watchlist entry

Add one or more individuals watchlist entries so that you can screen individual visitors and automatically perform block or notify actions at a site or global level as specified in the watchlist configuration.

Before you begin

[Add your watchlists.](#)

What you should know

Only a *watchlist manager* can:

- Add individuals watchlist entries.
- View reasons why visitors are in notify or block watchlists.

Procedure

- 1 Click **Organization > Watchlists**.
- 2 Select a watchlist from the list.

3 Click **Add entry**.

Individual Enabled

Watchlist entry criteria

First name*

Middle name

Last name*

First name aliases
To add an alias, start typing and press Enter

Last name aliases
To add an alias, start typing and press Enter

Email
To add an email, start typing and press Enter

Emails to always allow

Email
To add an email, start typing and press Enter

Additional information

Physical description

Reason

Date of birth
MM/DD/YYYY

External reference ID

Company name

Permissions

This entry can only be modified or deleted by the watchlist manager for the following sites:

Sites with watchlist entries that can be modified or deleted
To add a site, start typing and press Enter

Cancel Save

4 At the top of the watchlist entry click the **Enabled** slider to enable or disable the watchlist entry.5 In the *Watchlist entry criteria* section, complete the fields:

- **First name:** Enter a first name.
- **Middle name:** Enter a middle name.
- **Last name:** Enter a last name.
- **First name aliases:** Add any known first name aliases and press enter. Repeat as required.

NOTE: Aliases are shown in brackets in the watchlist entries list.

- **Last name aliases:** Add any known last name aliases and press enter. Repeat as required.
- **Emails:** Add any known emails and press enter. Repeat as required.

- 6 In the *Emails to always allow* section, add any emails that you want to exclude from the watchlist screening process.

This section is used to add any similar emails or false positive email matches that you might want to always allow. For example, a possible match that has the same name details, but is a different person with a different email address that should be allowed.

- 7 In the *Additional information* section, complete any additional fields that you require:

- **Physical description:** Enter a physical description.
- **Reason:** Enter a reason for the block or notify.

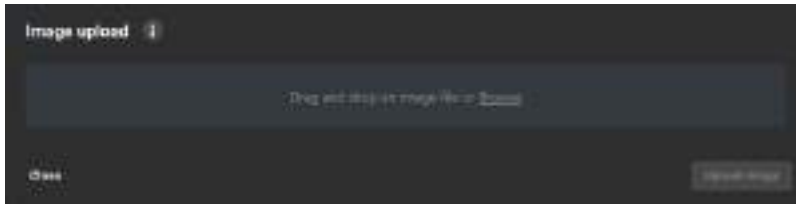
NOTE: The **Reason** field can contain sensitive private information, and can only be viewed by the watchlist manager for the site.

- **Date of birth:** Use the calendar picker to enter a date of birth.

The date of birth information is useful additional information when a visitor check-in matches multiple people with the same name. It can be used to validate an identity and also eliminate duplicates or false positive matches.

- **External reference ID:** Enter an external reference ID.
- **Company name:** Enter a company name.

- 8 In the *Additional information* section, Click **Add image** to add one or more images if required.



- Drag and drop an image or click **Browse** to select the image file that you require and click **Upload image**.
- Repeat for each additional image you want to upload.
- (Optional) Click **Delete image** for any images you no longer require.

TIP: Click **Open in new tab** to view the full-size image.

- 9 If you have **Watchlist entry permissions** activated for your account, in the *Permissions* section, add the sites that you require.

- 10 Click **Save**.

Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



After you finish

[Test your watchlist entries.](#)

Adding a companies watchlist entry

Add one or more companies watchlist entries so that you can screen visitors at a company level and automatically perform block or notify actions at a site or global level as specified in the watchlist configuration.

Before you begin

[Add your watchlists.](#)

What you should know

Only a *watchlist manager* can:

- Add companies watchlist entries.
- View reasons why visitors are in notify or block watchlists.

Procedure

- 1 Click **Organization > Watchlists**.
- 2 Select a watchlist from the list.
- 3 Click **Add entry**.

Company ☒ Enabled

Watchlist entry criteria

Company name *

Company aliases
To add an alias, start typing and press Enter

Company domain
To add a domain, start typing and press Enter
www.example.com

Additional information

Reason

External reference ID

Permissions

This entry can only be modified or deleted by the watchlist manager for the following sites

Sites with watchlist entries that can be modified or deleted
To add a site, start typing and press Enter

Cancel Save

- 4 At the top of the watchlist entry click the **Enabled** slider to enable or disable the watchlist entry.

- 5 In the *Watchlist entry criteria* section, complete the fields:
 - **Company name:** Enter a company name.
 - **Company aliases:** Add any known company aliases and press enter. Repeat as required.
NOTE: Aliases are shown in brackets in the watchlist entries list.
 - **Company domains:** Add any known company domains and press enter. Repeat as required.
- 6 In the *Additional information* section, complete any additional fields that you require:
 - **Reason:** Enter a reason for the block or notify.
NOTE: The **Reason** field can contain sensitive private information, and can only be viewed by the watchlist manager for the site.
 - **External reference ID:** Enter an external reference ID.
- 7 If you have **Watchlist entry permissions** activated for your account, in the *Permissions* section, add the sites that you require.
- 8 Click **Save**.

Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



After you finish

[Test your watchlist entries.](#)

Importing watchlist entries from a file

To accelerate your watchlist configuration and setup, you can import your watchlist entries from a .CSV file. You can also download a sample .CSV file to help you prepare your watchlist entries file in the correct format.

Before you begin

Prepare your watchlist entries in a .CSV file, so that they are ready for import.

What you should know

Only a *watchlist manager* can import watchlist entries.

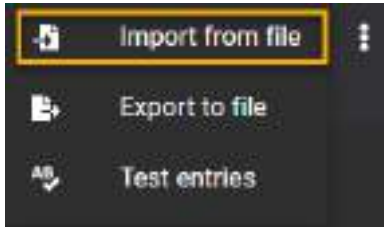
You can import pre-existing watchlist entry data using a .CSV file from one or more of the following sources:

- Sharepoint
- Excel
- Be on (the) look-out (BOLO) list - a watchlist term typically used in the field of policing
- No entry list
- Deny entry list (DEL)

Procedure

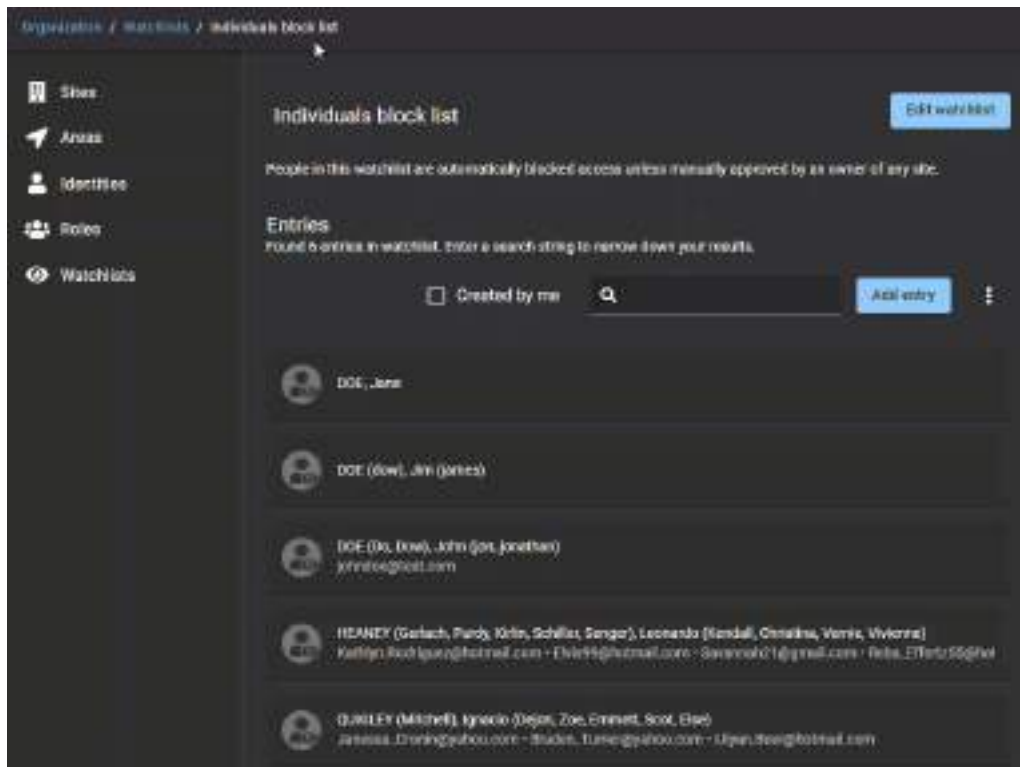
- 1 Click **Organization > Watchlists**.
- 2 Select a watchlist.

- 3 Click  and click **Import from file**.



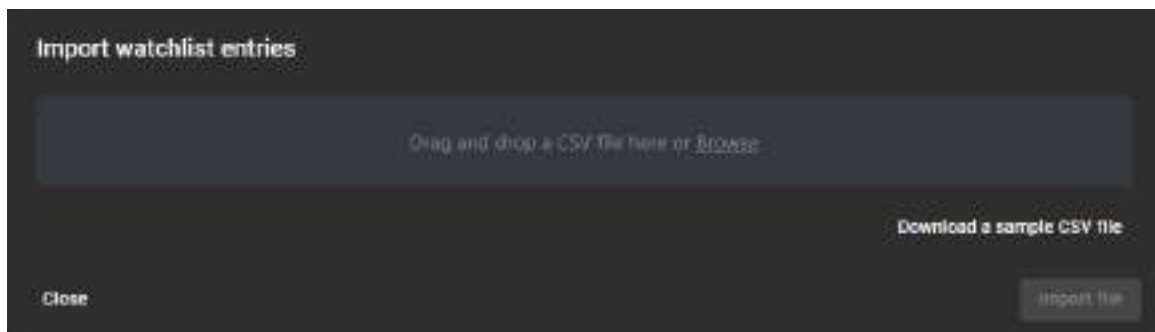
- 4 (Optional) Click **Download a sample CSV file** to help you prepare a watchlist entries file in the correct format.

NOTE: The columns and entries in the sample CSV file (*watchlist-sample.csv*) can vary depending on the watchlist type (**Individuals** or **Companies**) you select when you download the sample.

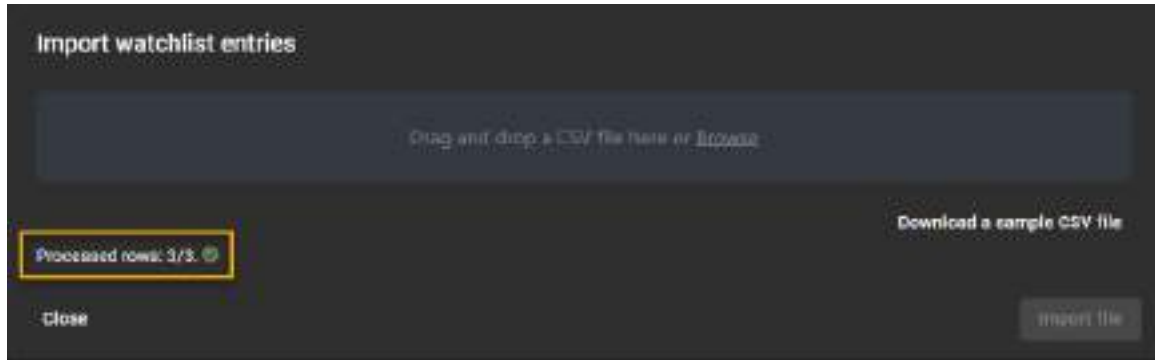


TIP: Click the animation to view full size.

- 5 In the **Import watchlist entries** dialog, drag and drop a CSV file or click **Browse** to select a file.



- Click **Import file**.



NOTE: The **Processed rows** field in the *Import watchlist entries* dialog indicates how many watchlist entries have been processed.

After you finish

[Test your watchlist entries.](#)

Exporting watchlist entries to a file

You can export your watchlist entries to a .CSV file for mass editing or backup purposes. For example, you could export your watchlist entries to Microsoft Excel, edit the entries, remove any duplicates, and then merge watchlists or consolidate watchlist entries into a new watchlist.

Before you begin

Do one or more of the following:

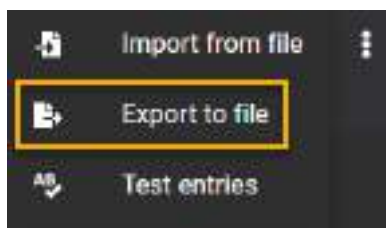
- [Add your individuals watchlist entries.](#)
- [Add your companies watchlist entries.](#)
- [Import your watchlist entries..](#)

What you should know

Only a *watchlist manager* can export watchlist entries.

Procedure

- Click **Organization > Watchlists**.
- Select a watchlist.
- Click **!** and click **Export to file**.



The file is exported as a .CSV file to the default download location for your browser. By default the exported file is created using the name of your watchlist. For example, *Individuals block list.csv*.

- 4 Follow your browser prompts to complete downloading the exported file.

After you finish

(Optional) Manipulate the watchlist entry data as required.

Testing watchlist entries

To test new watchlist entries, you can enter the details of a person of interest or a company of interest to verify if there's a screening match.

Before you begin

Do one or more of the following:

- [Add individuals watchlist entries](#)
- [Add companies watchlist entries](#)

What you should know

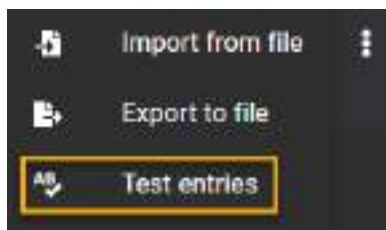
Only a *watchlist manager* can test watchlist entries.

Screening matches only occur when the following applies:

- Individuals: There is a **First name** and **Last name** match, **First name** and **Last name** alias match, or **Email** address match.
- Companies: There is a **Company** name, company domain, or email address domain match.

Procedure

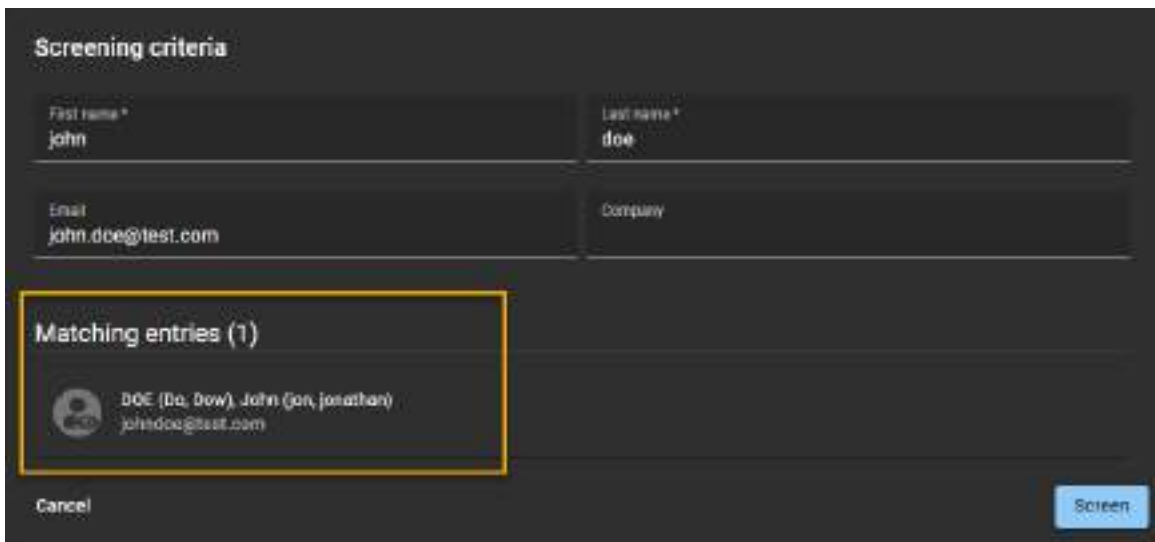
- 1 Click **Organization > Watchlists**.
- 2 Select a watchlist.
- 3 Click  and click **Test entries**.



- 4 In the *Screening criteria* dialog, enter the details of the entry that you want to test
NOTE: Mandatory fields are highlighted using an asterisk (*).

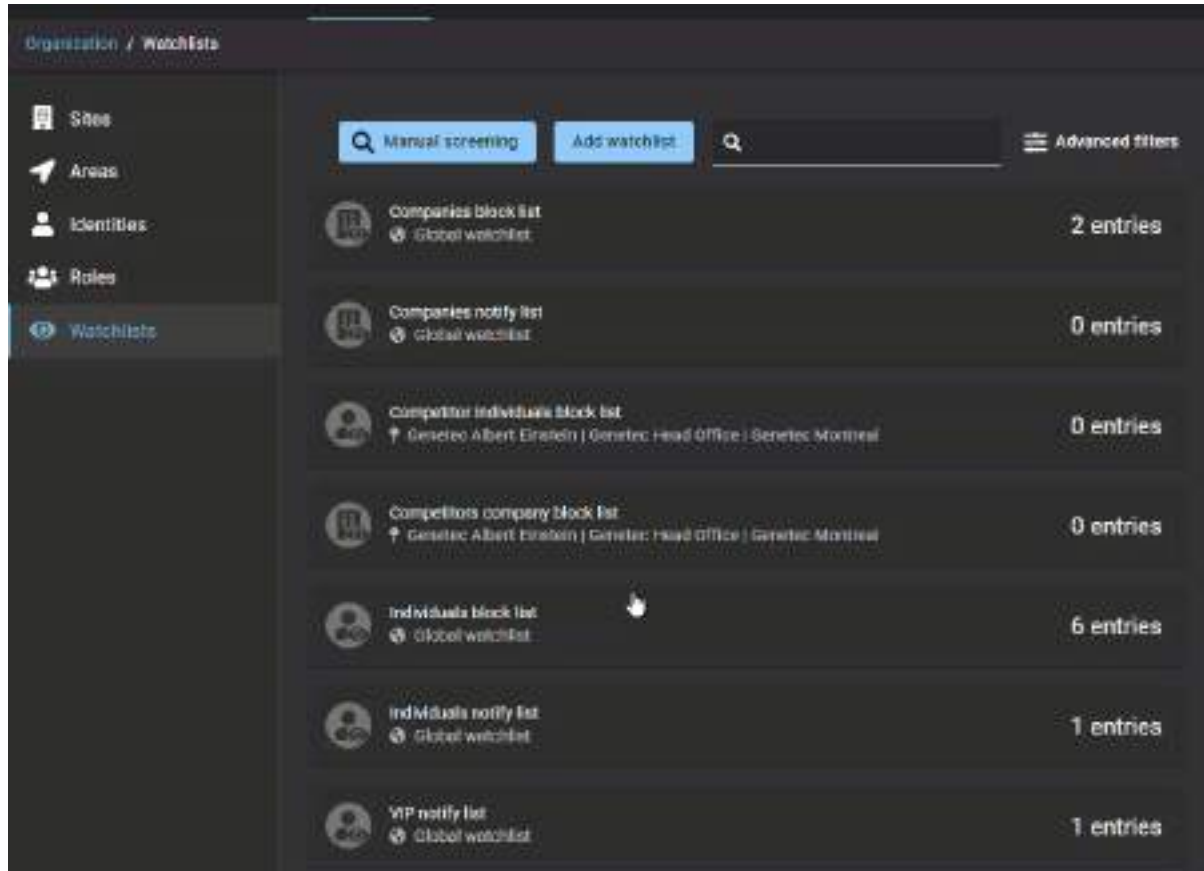


- 5 Click **Screen**.
Matching entries are shown in the *Matching entries* list in the *Screening Criteria dialog*.



- 6 (Optional) Click a matching entry in the list to view the complete details of the watchlist entry.
7 Click **Cancel** to exit the *Screening Criteria dialog*.

Example



Deleting watchlist entries

A watchlist manager can delete individuals watchlist entries or companies watchlist entries that have become obsolete or are no longer required.

Before you begin

Do one or more of the following:

- [Add individuals watchlist entries](#)
- [Add companies watchlist entries](#)

What you should know

A watchlist entry can only be deleted by the *watchlist manager* who created it.

Procedure

- 1 Click **Organization > Watchlists**.
- 2 Select a watchlist from the list.
- 3 (Optional) If the watchlist entries list is long, select **Created by me** to reduce the displayed results.

- 4 Do one of the following:
 - Click to select a watchlist entry in the list
 - Search for the entry that you want to delete.
- 5 Scroll to the bottom of the watchlist entry and click **Delete entry**.

Individual Enabled Delete entry

Watchlist entry criteria

First name * Middle name Last name *

First name aliases Last name aliases

Email

Emails to always allow

Email

Additional information

Physical description

Reason

Date of birth

External reference ID

Company name

Cancel 1 / 3 Save

- 6 In the *Delete entry* dialog, click **Remove** to confirm your deletion.

Delete entry

Are you sure you want to delete the entry "DOE, Jim"?

Cancel Remove

Modifying watchlists

After you add your watchlists, you can modify some of the watchlist settings. A watchlist manager can disable a watchlist, change the Name or Description, and change watchlist behavior.

Before you begin

[Add your watchlists.](#)

What you should know

When modifying a watchlist, the following applies:

- You can't change a *global watchlist* to become a *site watchlist*.
- You can't change a *site watchlist* to become a *global watchlist*.
- You can't modify **Watchlist entry permissions** after a watchlist is created.

Any *watchlist manager* or account administrator can modify any watchlist that is configured as a *global watchlist*.

Procedure

- 1 Click **Organization > Watchlists**.
- 2 (Optional) Use the search box to find a specific watchlist.
- 3 (Optional) Click **Advanced filters** to filter the list results by **Site** or **Watchlist type**.
Select the filter options that you require:
 - a) From the **Site** list, select a site.
 - b) From the **Watchlist types** list, select a watchlist type.
 - c) Click **Close**.
- 4 Select a watchlist from the list.

- 5 Click **Edit watchlist**.

Individuals notify list ☒ Enabled Delete watchlist

Name *
Individuals notify list

Description

Watchlist behavior

☒ Notify watchlist managers

☐ Automatically block visitors listed in a watchlist and notify watchlist managers

Watchlist settings

☐ Global watchlist that applies to all sites in your system

Cancel Save

- 6 Modify the watchlist as required by doing one or more of the following:
- At the top of the watchlist dialog, click the **Enabled** slider to enable or disable the watchlist.
For example, you might want to disable a large watchlist and refer to it while restructuring entries into other watchlists.
 - In the **Name** field, change the watchlist **Name**.
 - In the **Description** field, change the watchlist **Description**.
 - In the *Watchlist behavior* section, modify the **Watchlist behavior**. Select either **Notify watchlist managers** or **Automatically block visitors listed in a watchlist and notify watchlist managers**.
- 7 Click **Save**.

Deleting watchlists

A watchlist manager can delete watchlists that have become obsolete or are no longer required. Or a watchlist might need to be deleted in situations where you need to change a *site watchlist* to a *global watchlist* or vice versa.

Before you begin

[Add your watchlists.](#)

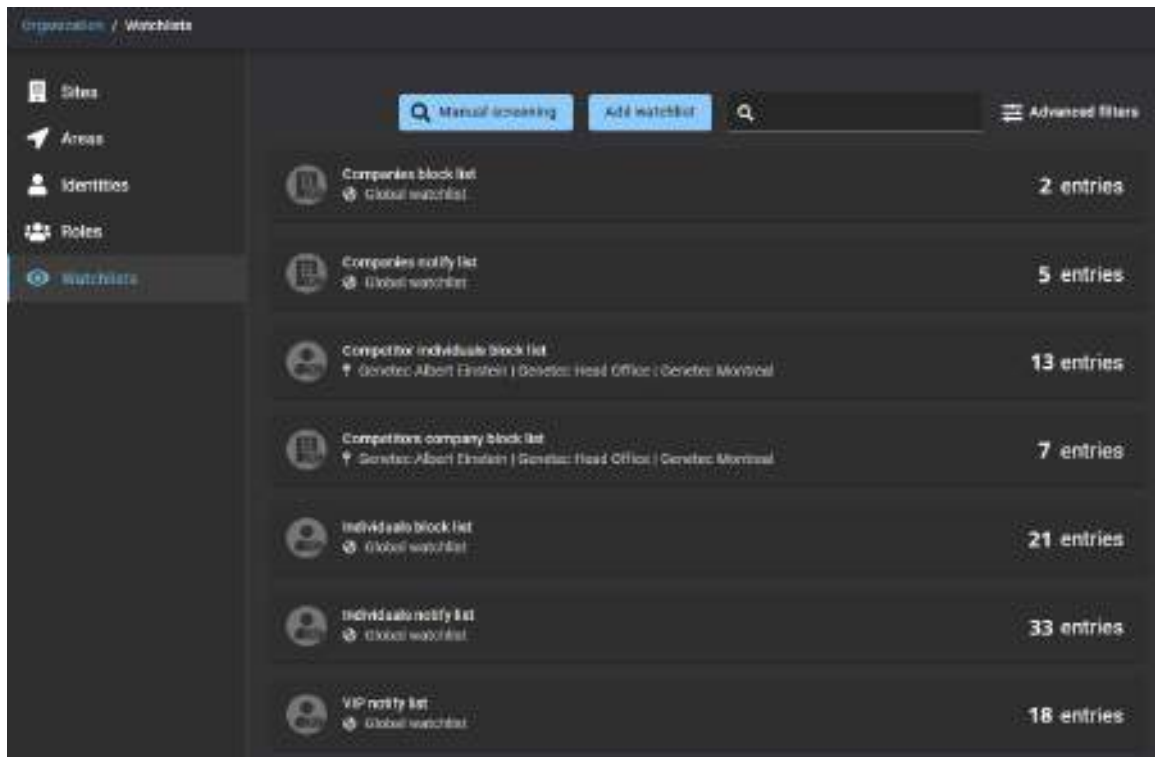
What you should know

A watchlist can only be deleted by the *watchlist manager* who created it.

NOTE: Any watchlist manager or account administrator can delete any watchlist that is configured as a global watchlist.

Procedure

- 1 Click **Organization > Watchlists**.



- 2 (Optional) Use the search box to find a specific watchlist.
- 3 (Optional) Click **Advanced filters** to filter the list results by **Site** or **Watchlist type**.
Select the filter options that you require:
 - a) From the **Site** list, select a site.
 - b) From the **Watchlist types** list, select a watchlist type.
- 4 Select a watchlist from the list.
- 5 Click **Edit watchlist**.

- 6 Verify you have the required watchlist and click **Delete watchlist**.

Individuals block list Enabled Delete watchlist

Name*
Individuals block list

Description

Watchlist behavior

☐ Notify watchlist managers

☒ Automatically block visitors listed in a watchlist and notify watchlist managers

Watchlist settings

☒ Global watchlist that applies to all sites in your system

Cancel Save

Do one of the following:

- a) In the *Delete watchlist* dialog, click **Delete watchlist** to confirm the deletion.

Delete watchlist

Are you sure you want to delete the watchlist "Individuals block list"?

Cancel Delete watchlist

- b) (Optional) Click **Cancel** to abandon the deletion.

Screening visitors manually

To manually screen a visitor, you can enter the visitor details to check if there's a screening match. For example, testing a new watchlist to find watchlists that contain a person or company of interest, or to validate a new hire against an internal watchlist.

Before you begin

[Add your individual watchlist entries.](#)

What you should know

Only *watchlist managers* or account administrators can manually screen visitors for the following:

- Finding watchlists that contain a person of interest.
- Validating a new hire against an internal **Individuals** watchlist or **Companies** watchlist.

Screening matches only occur when the following applies:

- Individuals: There is a **First name** and **Last name** match, **First name** and **Last name** alias match, or **Email** address match.
- Companies: There is a **Company** name, company domain, or email address domain match.

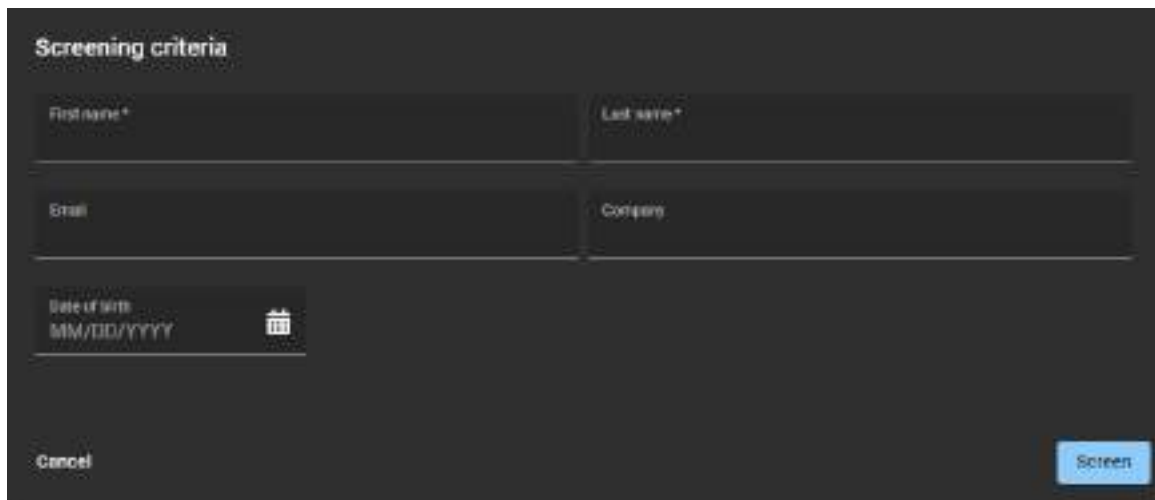
If *security* or *reception* employees need to manually screen visitors, the *Watchlist manager* permission must be added to their identity.

Procedure

- 1 Click **Organization > Watchlists**.
- 2 Click **Manual screening**.

- 3 In the *Screening criteria* dialog, complete the details for the visitor that you want to manually screen.

NOTE: Mandatory fields are highlighted using an asterisk (*).



Screening criteria

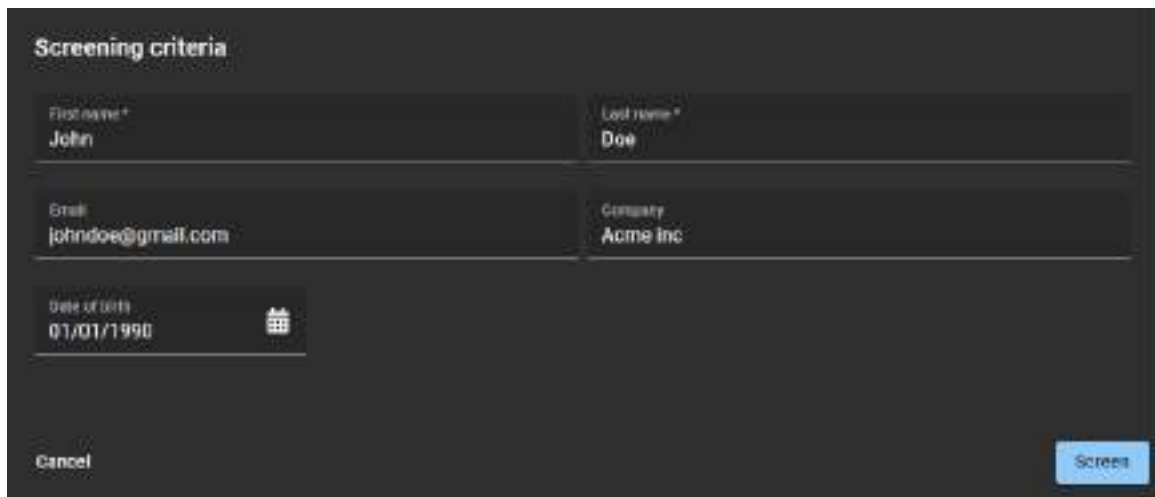
First name * Last name *

Email Company

Date of birth: MM/DD/YYYY

Cancel Screen

- **First name:** Enter a first name.
- **Last name:** Enter a last name.
- **Email:** Enter the visitor's email address.
- **Company:** Enter the visitor's company name.
- **Date of birth:** Use the calendar picker to select the visitor's date of birth. The date of birth information is useful additional information when a visitor check-in matches multiple people with the same name. It can be used to validate an identity and also eliminate duplicates or false positive matches.



Screening criteria

First name * Last name *

John Doe

Email Company

john.doe@gmail.com Acme Inc

Date of birth: 01/01/1990

Cancel Screen

4 Click **Screen**.

Matching entries for individuals or companies are shown in the *Matching entries* list in the *Screening Criteria dialog*.

Screening criteria

First name *
John

Last name *
Doe

Email
johndoe@gmail.com

Company
Acme Inc

Date of birth
01/01/1990

Matching entries (2)

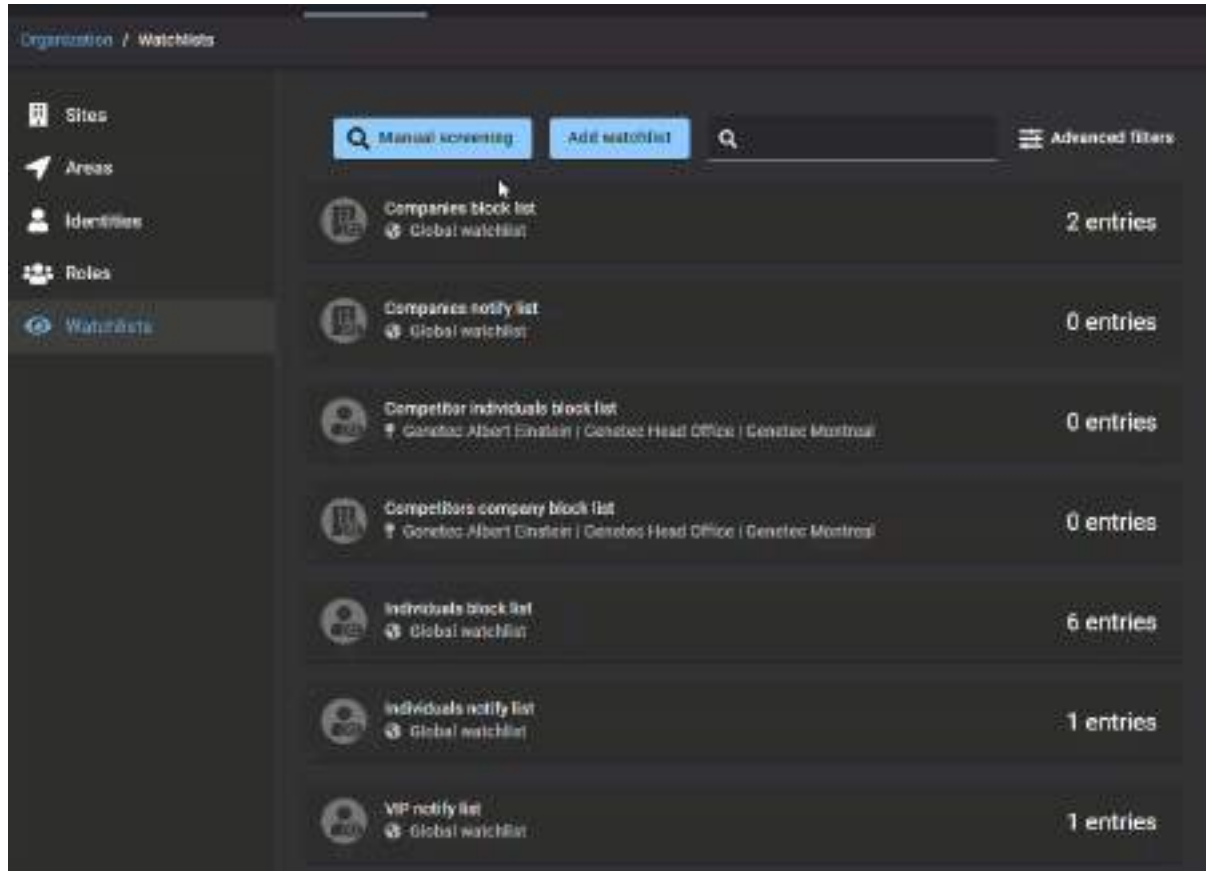
- DOE, John (jon, jonathan, jonathon)
- Acme Inc (acme, acme incorporated, Acme Inc.)
www.acme.com

Cancel

Screen

- 5 (Optional) Click an individual in the **Matching entries** list to view the complete details of the individuals watchlist entry.
- 6 (Optional) Click a company in the **Matching entries** list to view the complete details of the companies watchlist entry.
- 7 Click **Cancel** to exit the *Screening Criteria dialog*.

Example



TIP: Click the animation to view full size.

Related Topics

[Adding watchlist managers](#) on page 139

Unblocking visitors blocked by a watchlist

To unblock visitors incorrectly blocked by a watchlist, you can add the visitors email to an always allow list.

Before you begin

[Add your individuals watchlist entries.](#)

What you should know

Only a *watchlist manager* or account administrator can unblock a blocked visitor.

- Individuals watchlist email match cannot be set to **Always allow**.
- Company watchlist entry matches cannot be set to **Always allow**.
- Notify watchlist entry matches cannot be set to **Always allow**.

Use this procedure to add any similar emails or false positive email matches for visitors that you might want to allow once or always allow. For example, a possible match that has the same name details, but is a different person with a different email address that should be allowed.

Procedure

- 1 In your *Visitor watchlist alert* for <person or company of interest> email, click **SEE BLOCK DETAILS**.



The visitor watchlist alert dialog opens in the Genetec ClearID™ web portal.

Visitor watchlist alert

? Requested by: Jamie Myles

Blocked

Site and areas
Deeeto Albert Enasein (America/Toronto)
Main Entrance

Event date and time
From: May 28, 2021 12:00 PM
To: May 31, 2021 1:00 PM

Visitor
First name: John
Last name: Doe
Email: johndoe@test.com
Company:

Hosts + 1 Hosts
Jamie Myles

Matching watchlist entries Always allow all

	DOE, John (Jon, Jonathan, Jonathon) johndoe@test.com	Individuals notify list	John Doe	☐	+
	DOE (Da, Dew), John (Jon, Jonathan) johndoe@test.com	Individuals block list	John Doe	☐	+

Close Allow entry

- a) In the *Matching watchlist entries* section, hover over the info icon to see the watchlist entry details that matched this visitor.
 - b) (Optional) Click a matching watchlist entry in the list to open and view the watchlist entry details. The watchlist entry opens in a new browser tab.
- 2 Choose whether you want to allow entry one time or always allow entry. Do one of the following:
- If you want to allow entry one time only for this visitor watchlist alert, click **Allow entry**.
 - If you want to always allow specific future matching entries for this visitor, in the **Matching watchlist entries** list, move the **Always allow** slider to the enabled position for each entry you want to always allow, then click **Allow entry**.
 - If you want to always allow all future matching watchlist entries for this visitor, in the **Matching watchlist entries** section, move the **Always allow all** slider to the enabled position, then click **Allow entry**.
- NOTE:** Only the slider controls for the watchlist entries that can be set to **Always allow** will be moved to the enabled position.

- 3 In the **Reason** field, enter a reason why the blocked visitor was unblocked and allowed to visit.

Visitor watchlist alert

? Requested by: Jamie Myles

Blocked

Site and areas
Genetec Albert Einstein (America/Toronto)
Main Entrance

Event date and time
From: May 28, 2021 12:00 PM
To: May 31, 2021 1:00 PM

Visitor

First name	Last name	Email	Company
John	Doe	john.doe@test.com	

Hosts • 1 Hosts
Jamie Myles

Matching watchlist entries Always allow all

Individuals notify list	Individuals block list
DOE, John (Jon, Jonathan, Jonathon) john.doe@test.com	DOE (Dr. Dow), John (Jon, Jonathan) john.doe@test.com

Allow reason ✕

Reason:
john.doe@test.com is not the BLOCKED john.doe@competitor.com and should always be allowed.

88 / 300

Confirm

- 4 (Optional) In the **Allow reason** section, click **✕** to cancel the unblock, then click **Close**.
- 5 Click **Confirm**.

Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



Synchronizing data

Authenticating your connection

Before you can connect with Genetec ClearID™ to synchronize data or issue API commands, you must first authenticate your applications (or API environment) so that your applications or API can communicate with ClearID.

What you should know

Use the API integration key to authenticate your applications when making requests to your ClearID account.

- The OAUTH 2.0 protocol is used to authenticate non-user system communications or connections with ClearID.
- Store your key securely and don't share it.

IMPORTANT: When you regenerate your key, you must update any applications that access this account to use the new key.

You can create an API integration to authenticate communications for the following:

- Genetec ClearID™ API
- Genetec ClearID™ One Identity Synchronization Tool (Azure AD, Database, File)

Procedure

- 1 Add an API integration.
 - a) In ClearID, click **Administration > API integrations**.
 - b) Click **Add API integration**.
 - **Name:** Enter a name for the API integration. For example, API user connection or One Identity synchronization.
 - **Description:** Enter a meaningful description for the API integration.
 - c) Click **Save**.
- 2 Select a user from the API integration list.
 - a) Click **Generate key** and then click **Confirm**, to generate the authentication key for your API integration.

CAUTION: The current API integration key immediately becomes invalid and isn't recoverable.
 - b) Click **Download authentication key**.

TIP: Make a note of the downloaded file location for later use.

By default, the authentication key for your API integration is named *key-systemID-APIintegrationname.json*.

You're now ready to configure your applications to synchronize data or issue API commands.

Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



After you finish

Depending on how attributes are set up in your organization, do one of the following:

- [Synchronize identity attributes using One Identity \(Azure AD, Database, File\)](#).

- [Synchronize identity attributes using REST API commands.](#)

Synchronizing identities using an API

Use the Genetec ClearID™ API to code your own solutions to automate various functions in ClearID. The primary use for the REST API is synchronizing identities. However, many other scenarios are also possible.

About the ClearID API

The Genetec ClearID™ API is an Application Programming Interface that developers can use to help customers and partners integrate additional software or perform custom functions.

Genetec ClearID™ is an API first service and the Web interface is built on top of that REST API. As a result most of the functionality from the Web interface is accessible by using Representational State Transfer (REST) endpoints.

The ClearID API is developed with two main objectives:

- **Platform independence:** Any client should be able to call the API, regardless of how the API is implemented internally. This platform independence requires standard protocols, and a mechanism where the client and the web service can agree on the data format to exchange.
- **Service evolution:** The web API should be able to evolve and add functionality independently from client applications. As the API evolves, existing client applications should continue to function without modification.

The ClearID API follows the best practices for Representational State Transfer (REST) and uses the standard HTTP actions: GET, POST, PUT, PATCH, and DELETE.

Examples

The primary use for the REST API is synchronizing identities. However, many other scenarios are also possible.

Here are some examples of the reports or data that you can obtain from ClearID using the REST API:

- List of all upcoming and past visit events.
- List of all approved visitor hosts.
- List of all upcoming and past visit events for a specific requester, host, or site.
- List of all active or inactive hosts, permissions information for each host, contact details, title, department, and company.

For each visit you can also obtain the following:

- Event
- Event name
- Expected arrival and departure date and time
- Visit requester
- List of guests
- Visit type
- Parking location
- Meetup location
- Site visited
- Areas on that site
- Approval details

For more information about automating functions using the ClearID REST API, see the [Genetec™ Developer documentation](#).

Synchronizing identities using the SCIM integration

To synchronize external system attributes from a supported identity provider into Genetec ClearID™ identity attributes, you can use the System for Cross-domain Identity Management (SCIM) integration. These identity attributes can then be used in ClearID to assign people to roles and automate role-based access control.

What you should know

Only Microsoft Entra ID is currently supported. If you want to integrate another supported identity provider, contact your deployment representative.

Procedure

- 1 [Learn about the SCIM standard.](#)
- 2 [Learn about Microsoft Entra ID attribute fields.](#)
- 3 [Configure the SCIM integration.](#)
- 4 (Optional) [Reset the SCIM integration identity data.](#)
- 5 [Review SCIM integration synchronization status.](#)

About the SCIM standard

The System for Cross-domain Identity Management (SCIM) standard is an open-standard protocol for exchanging identity information between entities. It's widely used to automate the process of managing user identities in IT systems. The SCIM integration ensures that any changes are automatically synchronized to other systems when identity attributes change.

- **System:** SCIM creates a common format for how identity data is exchanged.
- **Cross-domain:** SCIM securely communicates identity data across platforms.
- **Identity management:** SCIM automates the flow of information between an identity provider or [identity and access management \(IAM\) system](#) and cloud-based applications.

Benefits

- Using SCIM reduces the effort that it takes to create, modify, and synchronize identity data.
- Because the SCIM integration uses Microsoft Entra ID in the cloud, there's no machine or infrastructure to manage.
- There are no firewall ports to configure.

NOTE: The SCIM integration only synchronizes the identity attributes that have changed. This approach results in a significant reduction in throughput and processing overheads. Other solutions typically synchronize all identity attributes at a specified time to get all the latest identity data.

About Microsoft Entra ID attribute fields

When you synchronize an external system with Genetec ClearID™ using the System for Cross-domain Identity Management (SCIM) standard, your external system attributes are imported into ClearID identity attributes. The import uses the field mappings in Microsoft Entra ID.

Most of the ClearID identity fields are created as custom attributes.

You must prefix each field with: `urn:ietf:params:scim:schemas:extension:clearid:2.0:User`

Identity attributes

Attribute fields	Notes
Basic fields: active username displayName	- These basic fields are the only fields that we use from the SCIM base schema. - displayName is required in the mapping.
Base identity fields: urn:ietf:params:scim:schemas:extension:clearid:2.0:User:description urn:ietf:params:scim:schemas:extension:clearid:2.0:User:firstName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:lastName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:middleName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:countryCode urn:ietf:params:scim:schemas:extension:clearid:2.0:User:email	- firstName or lastName must be supplied in the mapping (the same as in the portal identity form). - email must be a valid email format to be created in the identity properly. - countryCode must be a 3-letter code. It's best to use a constant value from Microsoft Entra ID for now.
CompanyData fields: urn:ietf:params:scim:schemas:extension:clearid:2.0:User:employeeNumber urn:ietf:params:scim:schemas:extension:clearid:2.0:User:secondaryEmail urn:ietf:params:scim:schemas:extension:clearid:2.0:User:cityOfResidence urn:ietf:params:scim:schemas:extension:clearid:2.0:User:stateOfResidence urn:ietf:params:scim:schemas:extension:clearid:2.0:User:zipCode urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberPrimary urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberSecondary	secondaryEmail must be a valid email format to be created in the identity properly.
PrivateData fields: urn:ietf:params:scim:schemas:extension:clearid:2.0:User:supervisorName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:departmentName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:jobTitle urn:ietf:params:scim:schemas:extension:clearid:2.0:User:companyName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeDescription urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeCode	
SystemData fields: urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasExtendedTime urn:ietf:params:scim:schemas:extension:clearid:2.0:User:externalId	- Boolean fields only work with the SCIM 2.0 feature flag. - externalId is required and needs to be unique. This value is used to manage the creation of identities (same way in OneIdentity). The easiest way to use this value is to map with an email or username.
Other custom fields: (that aren't directly part of the identity model) urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasWebPortalAccess	Boolean fields only work with the SCIM 2.0 feature flag.

Attribute fields	Notes
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:isAdmin	

Attribute fields that are not supported

Date fields:

- birthday
- activationDateUtc
- expirationDateUtc
- externalSyncTimeUtc

Fields with ids (reference to identityIds):

- creationOnBehalf
- approvers
- siteId
- provisioningAttributes
- customFields

Configuring the SCIM integration

Before you can synchronize an external system with Genetec ClearID™, you must first configure the System for Cross-domain Identity Management (SCIM) integration in ClearID and Microsoft Azure.

Before you begin

- [Learn about the SCIM standard.](#)
- [Learn about Microsoft Entra ID attribute fields.](#)

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

Only Microsoft Entra ID is currently supported. If you want to integrate another supported identity provider, contact your deployment representative.

IMPORTANT: Do not skip the disable groups step. ClearID does not support the synchronization of groups.

Procedure

- 1 [Generate your SCIM key.](#)
- 2 [Create your Microsoft Azure enterprise application.](#)
- 3 [Connect your ClearID SCIM integration to Microsoft Azure.](#)
- 4 Configure your attribute mappings.
 - a) [Disable the Microsoft Entra ID groups setting.](#)
 - b) [Configure the Microsoft Entra ID user settings.](#)
- 5 [Configure the ClearID SCIM integration synchronization settings.](#)

After you finish

[Review the SCIM integration synchronization status.](#)

Generating a SCIM key

For your Genetec ClearID™ SCIM integration to communicate with Microsoft Entra ID, you must generate a System for Cross-domain Identity Management (SCIM) key.

What you should know

Only a ClearID portal *administrator* can perform this task.

Procedure

- 1 In the ClearID portal, click **Administration > SCIM Integration**.

- 2 In the *Generate key* section, enter a key name and click **Generate Key**.
For example, the key name could be GenetecSCIMIntegrationKey.

Endpoint URL

Use the endpoint URL to connect ClearID to your SCIM identity provider.

Microsoft Entra ID identity provider. ⓘ

<https://scim.demo.clearid.io/sync/techdoc/scim?aadOptscim062020> 

Other identity providers. ⓘ

<https://scim.demo.clearid.io/sync/techdoc/scim> 

Generate key

Use the security token to authenticate your SCIM application with your identity provider.

Generate key

✔ **IMPORTANT:** Store your key securely and do not share it. When you regenerate your key, you must update any applications that access this account to use the new key.

```
HDfKQzSYNEH2UfHdRKhTUjhcQFzWMLVTT1a60DFaZjUBMjHcOTBjHSB82DIwLMJhZjct2wM1N2wZTNkY
```

```
#Qy
```



Active keys

Name	Created on	Created by	
GenetecSCIMIntegrationKey	November 6, 2024 at 9:12 AM	jmyles@genetec.com	

Showing 1 to 1 of 1 total active keys. < >

After you finish

Create your Microsoft Azure enterprise application.

Creating a Microsoft Azure enterprise application

Your organization can automate identity attribute provisioning using the Genetec ClearID™ SCIM integration with Microsoft Entra ID as the identity provider. To use the integration, you must first create an enterprise application in Microsoft Azure.

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

Procedure

- 1 In the Microsoft Azure portal, search for and click **Enterprise applications**.
- 2 In the *Enterprise applications* section, click **New application**.
- 3 Click **Create your own application**.
- 4 Select **Integrate any other application you don't find in the gallery (Non-gallery)**.

- 5 Enter your application name and click **Create**.
For example, the application name could be ClearID SCIM Integration.

Create your own application



 Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

ClearID SCIM Integration



What are you looking to do with your application?

- ☐ Configure Application Proxy for secure remote access to an on-premises application
- ☐ Register an application to integrate with Microsoft Entra ID (App you're developing)
- ☒ Integrate any other application you don't find in the gallery (Non-gallery)

Create

NOTE: Watch for a successfully added notification in the upper right of the screen.

After you finish

[Connect your ClearID SCIM integration to Microsoft Azure.](#)

Connecting your ClearID SCIM integration to Microsoft Azure

Before you can use the SCIM integration in Genetec ClearID™ to synchronize identity attributes, you must provide your credentials that connect the ClearID SCIM Integration API to Microsoft Azure.

Before you begin

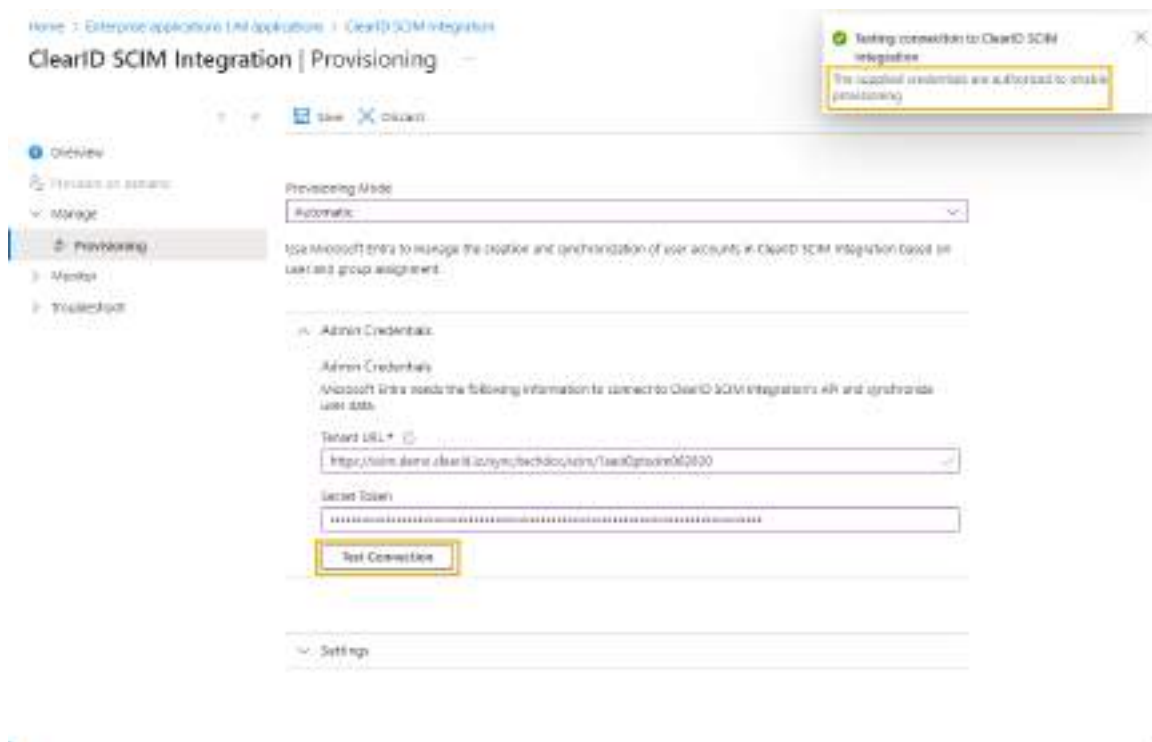
[Create your Microsoft Azure enterprise application.](#)

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

Procedure

- 1 In the Microsoft Azure portal, find and click **Enterprise applications**.
- 2 In the *Enterprise applications* section, search for and select your **ClearID SCIM integration** application.
- 3 In the *Manage* section, click **Provisioning** and then click **Provisioning** again.
- 4 From the **Provisioning Mode** list, select **Automatic**.
- 5 Expand the *Admin Credentials* section.
- 6 In the ClearID portal **SCIM integration** tab, locate the *Endpoint URL* section and click **Copy to clipboard** next to the Microsoft Entra ID identity provider.
The endpoint URL is copied to your clipboard.
- 7 Return to the Microsoft Azure *Provisioning* page and paste into the **Tenant URL**.
The endpoint URL is used to connect ClearID to SCIM authentication systems and Microsoft Entra ID.
- 8 In the ClearID portal **SCIM integration** tab, locate the *Generate key* section and click **Copy to clipboard**.
- 9 Return to the Azure AD *Provisioning* page and paste into the **Secret Token** field.
The SCIM key is used to authenticate your application with Microsoft Entra ID.
- 10 Click **Test Connection**.



- 11 Click **Save**.

TIP: Watch for a successful update notification in the upper right of the screen.

After you finish

Disable your Microsoft Entra ID group settings.

Disabling Microsoft Entra ID groups setting

Genetec ClearID™ doesn't support the synchronization of groups. To prevent group settings or attributes from being synchronized, disable the Microsoft Entra ID Groups setting in your Microsoft Azure enterprise application.

Before you begin

[Connect your ClearID SCIM integration to Microsoft Azure.](#)

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

IMPORTANT: ClearID doesn't support group synchronization. This setting must be disabled.

Procedure

- 1 In the Microsoft Azure portal, search for and click **Enterprise applications**.
- 2 In the *Enterprise applications* section, search for and select your **ClearID SCIM integration** application.
- 3 In the *Manage* section, click **Provisioning** and then click **Provisioning** again.
- 4 Expand the *Mappings* section of the *Provisioning* page.
- 5 Click **Provision Microsoft Entra ID Groups**.

- 6 Move the **Enabled** slider to **No**.

Home > Enterprise applications > All applications > ClearID TCM Integration > Provisioning >

Attribute Mapping

Save X Discard

Name: Provision Microsoft Entra ID Group

Enabled: **No**

Source Object: Group

Source Object Scope: All records

Target Object: Provision Microsoft Entra ID Group

Target object actions:

- ☒ Create
- ☒ Update
- ☒ Delete

Attribute Mappings

Attribute mappings define how attributes are synchronized between Microsoft Entra ID and custom apps:

customapp's Attribute	Microsoft Entra ID Attribute	Matching precedence	Add	Remove
displayName	displayName	1	edit	Delete
externalid	objectid		edit	Delete
password	password		edit	Delete

[add new mapping](#)

☐ Show advanced options

- 7 Click **Save** and then click **Yes** to confirm your changes.
- 8 Close the window and return to the *Provisioning* page.
It might take a moment to refresh the page.

After you finish

[Configure your Microsoft Entra ID user settings.](#)

Configuring Microsoft Entra ID user settings

To define how identity data flows between Microsoft Entra ID and Genetec ClearID™, you must configure your user settings and map attributes for automatic synchronization.

Before you begin

[Disable your Microsoft Entra ID groups setting.](#)

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

Procedure

- 1 In the Microsoft Azure portal, search for and click **Enterprise applications**.
- 2 In the *Enterprise applications* section, search for and select your ClearID SCIM integration application.
- 3 In the *Manage* section, click **Provisioning** and then click **Provisioning** again.
- 4 Expand the *Mappings* section and click **Provision Microsoft Entra ID Users**.

5 Modify the default attribute mappings.

a) On the *Attribute Mapping* page, click **Delete** to remove unused default attributes.

Only keep the following:

- userName
- active
- displayName

Home > Enterprise applications | All applications > ClearID SCIM Integration | Provisioning >

Attribute Mapping

 Save  Discard

Name

Provision Microsoft Entra ID Users

Enabled

☒ Yes ☐ No

Source Object

User

Source Object Scope

All records

Target Object

urn:ietf:params:scim:schema:extension:enterprise:2.0:User

Target Object Actions

☒ Create☒ Update☒ Delete

Attribute Mappings

Attribute mappings define how attributes are synchronized between Microsoft Entra ID and customappsso

customappsso Attribute	Microsoft Entra ID Attribute	Matching precedence
userName	userPrincipalName	1
active	Switch([IsSoftDeleted], "False", "True", "True", "False")	
displayName	displayName	

[Add New Mapping](#)☐ Show advanced optionsb) Click **Save** and then click **Yes** to confirm your changes.

6 Modify the customappsso user attributes.

- a) On the *Attribute Mapping* page, click **Show advanced options**.
- b) Click **Edit attribute list for customappsso**, and then click **Delete** to remove all the unused default attributes.

Only keep the following:

- id
- active
- displayName
- title
- userName

Home > Integrate applications > All applications > ClearID SCM Integration > Provisioning > Attribute Mapping >

Edit Attribute List

Save Delete

customappsso User Attributes

Name	Type	Primary Key?	Required?	Multi-valued?	Existence?	API Expression	Reference Object
id	String	☒	☒	☐	☐		
active	Boolean	☐	☐	☐	☐		
displayName	String	☐	☐	☐	☐		
title	String	☐	☐	☐	☐		
userName	String	☐	☒	☐	☐		
	String	☐	☐	☐	☐		

Tip

- Editing the attribute list informs the provisioning service what attributes exist in your systems. Editing this list does not modify the schema of these systems.
- Leave "Metadata" blank for new attributes unless instructed by documentation. Requires a JSON metadata object.
- Leave "Reference Object" blank unless the "Type" is set to "Reference". Only reference attributes in the form of objectName.attributeName or just objectName.
- See the online documentation on attribute editing.

- c) Click **Save** and then click **Yes** to confirm your changes.

7 Add the ClearID schema attributes.

Only include the list of attributes available to ClearID:

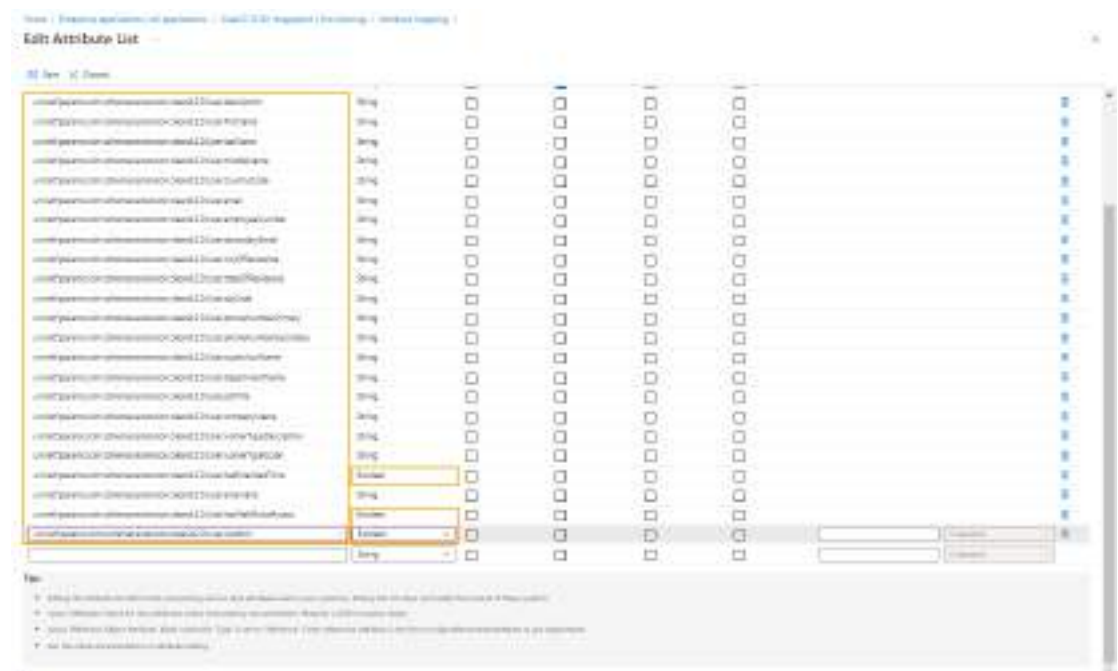
```
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:description
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:firstName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:lastName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:middleName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:countryCode
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:email
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:employeeNumber
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:secondaryEmail
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:cityOfResidence
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:stateOfResidence
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:zipCode
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberPrimary
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberSecondary
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:supervisorName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:departmentName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:jobTitle
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:companyName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeDescription
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeCode
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasExtendedTime
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:externalId
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasWebPortalAccess,
Boolean
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:isAdmin, Boolean
```

- a) On the *Edit Attribute List* page, copy and paste an attribute name from the preceding ClearID schema attributes code example into the **Name** field and select the attribute **Type**.

Almost every attribute has the type **String**, except for three attributes that have the **Boolean** type: *hasExtendedTime*, *hasWebPortalAccess*, and *UserisAdmin*.

IMPORTANT: The ClearID *externalId* attribute is the unique identifier that ClearID uses for synchronization. It's mapped to the unique *objectId* attribute in Microsoft Entra ID.

- b) Repeat for each attribute listed in the preceding ClearID schema attributes code example.



- c) Click **Save** and then click **Yes** to confirm your changes.

- 8 Add the ClearID attribute mappings.
 - a) On the *Attribute Mapping* page, click **Add New Mapping**.
 - b) On the *Edit Attribute* page, add the attributes that you require from the attributes added earlier in step 7 on page 185.

Include the following:

 - Mapping type: **Direct**
 - Source attribute: **objectid**
 - Target attribute: *<your attribute value>*
 - c) Click **OK**.
 - d) Repeat for each attribute added earlier and replace the target attribute value with the next attribute you want to add.

For a successful first synchronization, you need the following attributes. You can add more attributes later.

Attribute Mapping

Source: Personnel (Microsoft Entra ID) [Dropdown]

Target: User [Dropdown]

Source Object Details

Target Object Details

Attribute Mapping

Source Attribute	Target Attribute
id	id
name	name
email	email
phone	phone
address	address
password	password
created_at	created_at
updated_at	updated_at

Buttons: Save, Cancel, Add, Delete, Copy, Paste

NOTE: The `objectid` is the GUID in azure. There's no way to manipulate the `objectid` of a user in Azure. It's a hard-coded field that can't be modified.

- e) Click **Save** and then click **Yes** to confirm your changes.
You can now close the window and return to the *Provisioning* page.

After you finish

Configure the ClearID SCIM integration synchronization settings.

Configuring the ClearID SCIM integration synchronization settings

To determine what identity data is synchronized to Genetec ClearID™, you must select the required synchronization settings and activate provisioning in Microsoft Azure.

Before you begin

[Configure your Microsoft Entra ID user settings.](#)

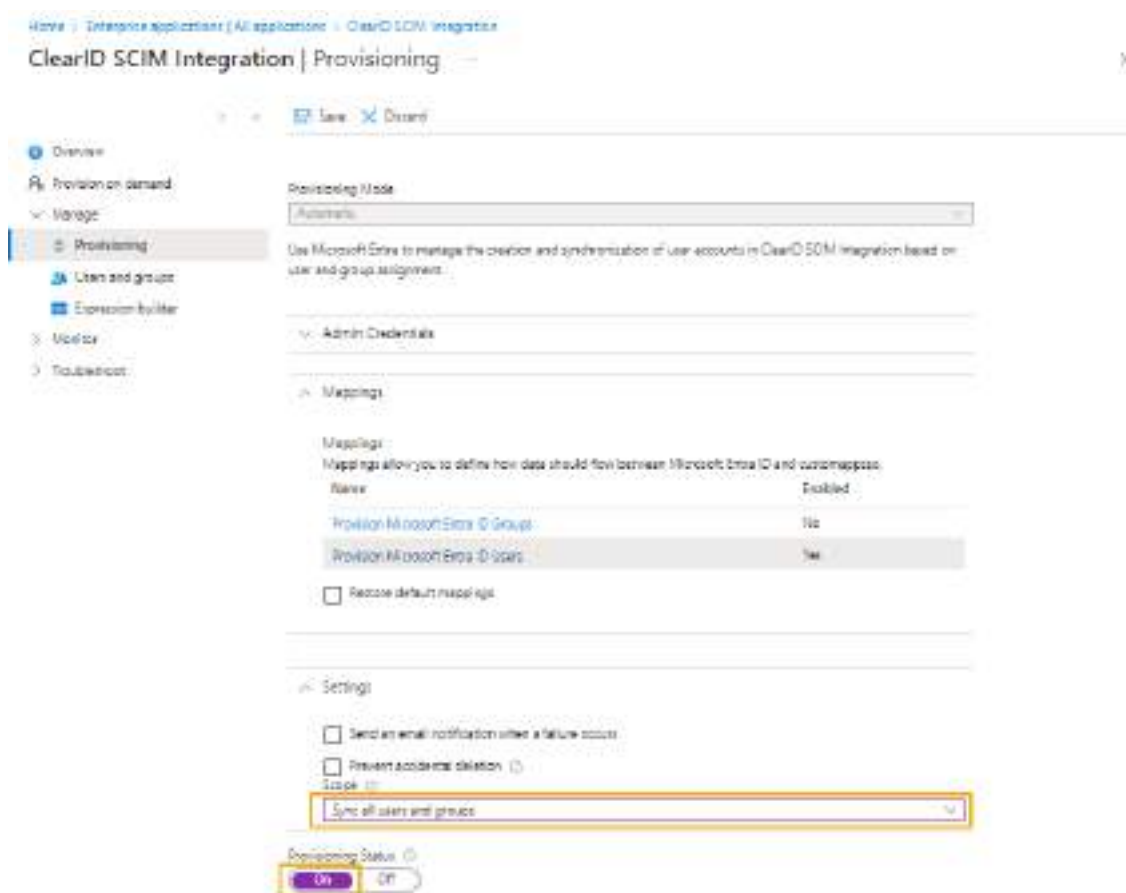
What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

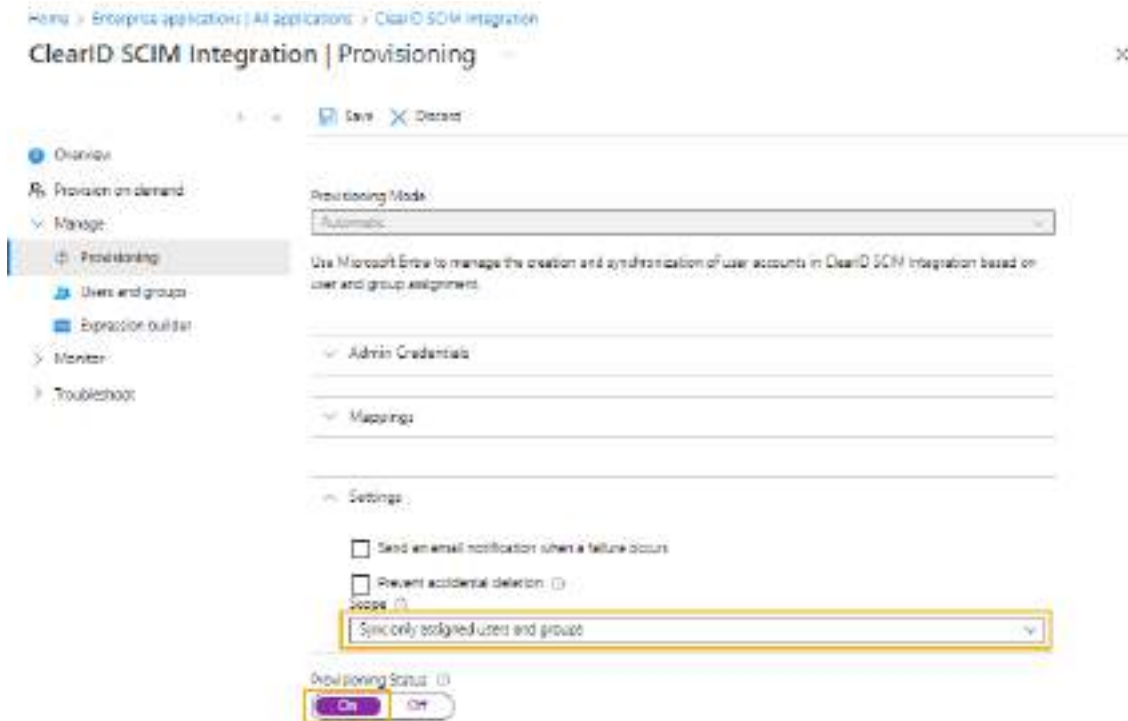
Procedure

- On the *Provisioning* page, click **Settings** and choose which users to synchronize to ClearID:
 - Sync all users and groups:** Synchronizes everything in Microsoft Entra ID.
 - Sync only assigned users and groups:** Only selected users and groups are synchronized.

IMPORTANT: ClearID doesn't support group synchronization. Depending on the provisioning settings that you select, either all users identity data or only selected users identity data is synchronized.
- If you chose **Sync all users and groups**, in the *Provisioning status* section, move the slider to **On** and click **Save**.



- 3 If you chose **Sync only assigned users and groups**, complete the provisioning settings.
 - a) Click **Users and groups** in the left navigation bar.
 - b) Click **Add group**.
 - c) Click **None selected**, search for and select the group you want to add, and click **Select**.
 - d) Click **Assign** and repeat for each group that you want to add.
 - e) Return to the *Provisioning* page and click **Settings**.
 - f) In the *Provisioning status* section, move the slider to **On** and click **Save**.



After you finish

[Review the ClearID SCIM integration synchronization status.](#)

Resetting SCIM integration identity data

To resolve issues with identity data, you can reset and replace all System for Cross-domain Identity Management (SCIM) integration identity data in Genetec ClearID™. This reset process uses the latest values from Microsoft Entra ID.

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

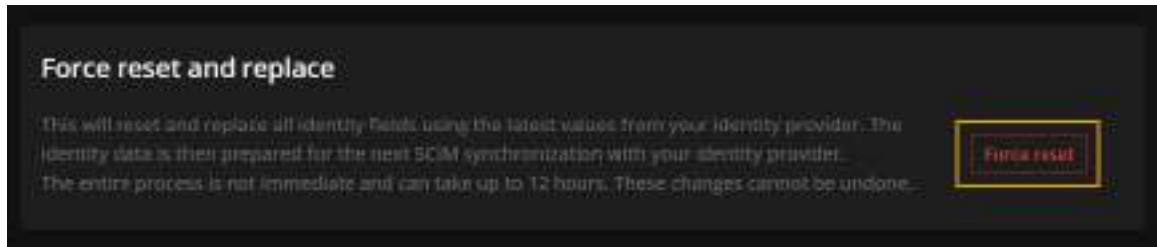
Only use this reset to resolve an identity data issue. For example, after your identity data has been manually manipulated, when there's a discrepancy, or when identity data has been deleted in ClearID.

The reset will prepare identity data for the next SCIM synchronization between ClearID and Microsoft Entra ID. This process only pushes identity data changes in one direction, to Entra ID.

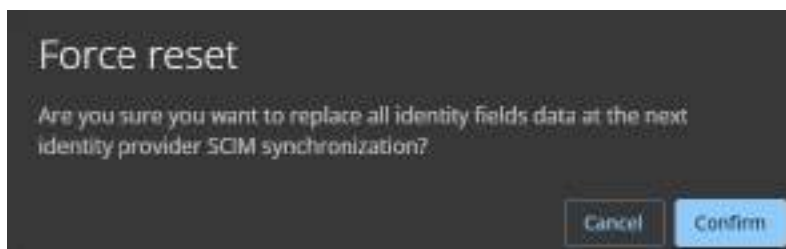
IMPORTANT: The entire process can take up to 12 hours. These changes can't be undone.

Procedure

- 1 In the ClearID portal, click **Administration > SCIM Integration**.
- 2 In the *Force reset and replace* section, click **Force reset**.



- 3 Click **Confirm** to reset and replace your identity data.



After you finish

Check the SCIM integration synchronization status to confirm that your identity data has been reset.

Reviewing the SCIM integration synchronization status

You can check the overall status of the System for Cross-domain Identity Management (SCIM) integration identity synchronization. You can also review the provisioning logs in Microsoft Azure to see more granular details about Genetec ClearID™ SCIM integration synchronization activities related to a specific person or identity.

What you should know

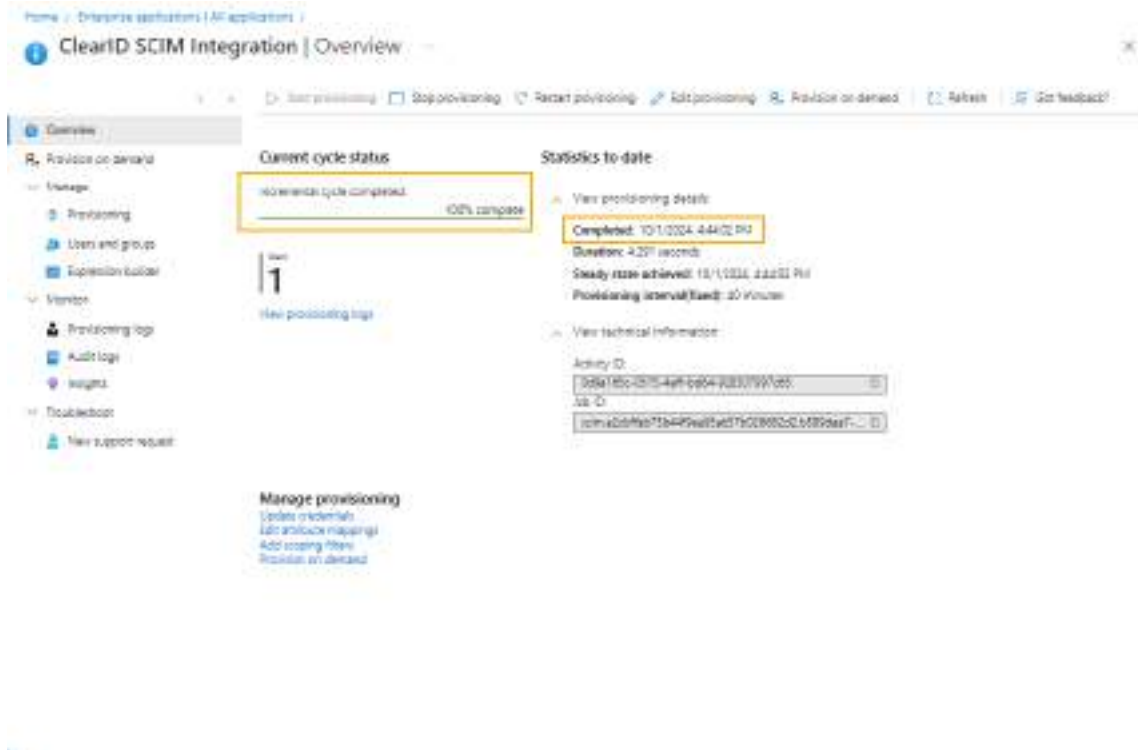
This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

The provisioning logs can be used to verify whether the ClearID SCIM integration is correctly configured and operational. If there are any issues with the configuration, error messages are generated and recorded in the provisioning logs.

Procedure

- 1 In the Microsoft Azure portal, find and click **Enterprise applications**.
- 2 In *Enterprise applications*, select your SCIM integration application.

- 3 On the *Overview* page, check whether the last synchronization completed successfully and when the last synchronization occurred.



- 4 (Optional) Click **View provisioning logs** to see more granular information about identity synchronization.



NOTE: If the log details are long, the *Provisioning Logs* page includes useful filters to manipulate the data for your needs.

Synchronizing identities using One Identity

Use the Genetec ClearID™ One Identity Synchronization Tool to synchronize external system attributes into Genetec ClearID™ identity attributes. These identity attributes in ClearID can then be used to assign people to roles and automate role-based access control.

What you should know

Using the One Identity Synchronization Tool you can synchronize external system attributes from the following data sources:

- Azure AD (Microsoft Entra ID)
- Database (Microsoft SQL Server, Oracle Database, ODBC)
- File (CSV)

Procedure

- 1 [Learn about the One Identity Synchronization Tool.](#)
- 2 [Learn about One Identity attribute fields.](#)
- 3 [Learn about the Azure web app.](#)
- 4 [Install the One Identity Synchronization Tool.](#)
- 5 [Configure the One Identity Synchronization Tool.](#)
- 6 [Review synchronization status.](#)

Related Topics

[Connectivity issues \(One Identity Synchronization Tool\)](#) on page 324

[Data synchronization issues \(One Identity Synchronization Tool\)](#) on page 325

About the One Identity Synchronization Tool

The Genetec ClearID™ One Identity Synchronization Tool is a Windows service that you can use to import identities information from an external system into Genetec ClearID™.



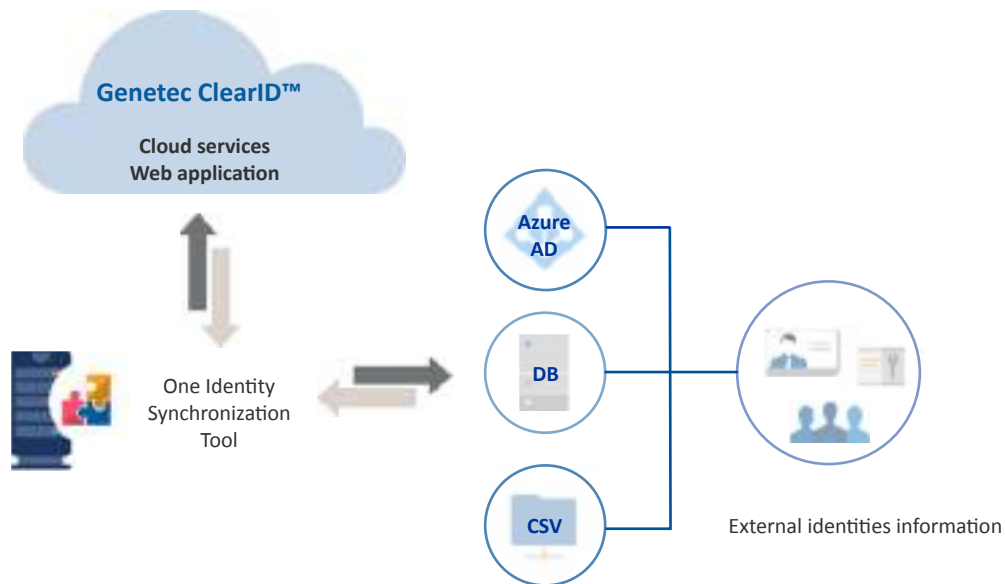
The ClearID One Identity Synchronization Tool includes the following components:

- **Genetec.ClearID.OneIdentity.SynchronizationTool** is the user interface component (*OneIdentityConfigurationTool.exe*) of the windows application that is used to configure the Synchronization Tool.
- **Genetec.ClearID.OneIdentity.SynchronizationService** is the Windows service component (*OneIdentityService.exe*) of the application that performs external system attributes to ClearID identity

attributes synchronization automatically in the background at intervals specified in the Synchronization Tool.

Data sources

You can select one or more data sources to be synchronized from an external system. Using the *Data sources configuration* dialog you configure the **Data sources** and map the One Identity attributes to their associated external system attributes.



- **Azure Active Directory:** The Azure AD (Microsoft Entra ID) data source is an Azure Active Directory that you can import identities information from. For example, importing identities, credentials, and pictures into ClearID.
- **Database:** The database data source can be a Microsoft SQL Server database, an Oracle database, or an ODBC-compliant database that follows the one identity attribute mapping. The database must be accessible from the server where the ClearID One Identity Synchronization Tool is installed. One database can contain one table or view for identities information.
- **File:** The file data source is a delimited text file. For example, a CSV file that follows the one identity attribute mapping, and must be accessible from the server where the ClearID One Identity Synchronization Tool is installed. Each file contains identities information.

Synchronization

Identities in ClearID can come from a variety of data sources (Databases, HR, External Sources) and can be synchronized using various tools (Genetec ClearID™ API or Genetec ClearID™ One Identity Synchronization Tool).

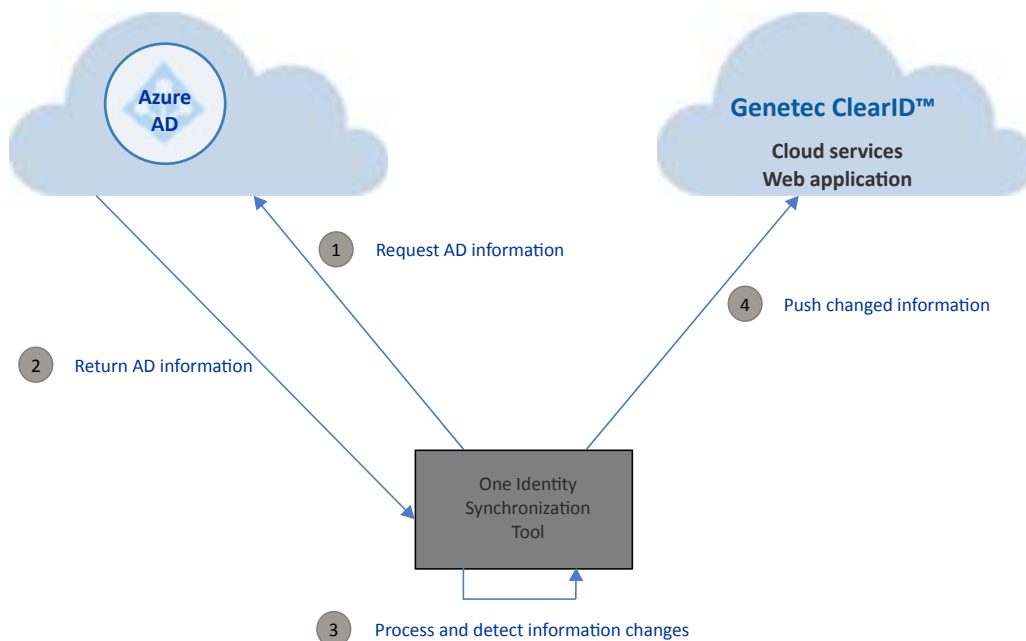
- API is typically used for real-time updates. For example, to remove people quickly. This API synchronization option is the most flexible but it's expensive.
- One Identity is typically used for HR systems. For example, to synchronize all employees every day or every 4hrs. The ClearID One Identity Synchronization Tool is configured to synchronize at the same frequency.

One Identity data synchronization

The following information describes One Identity synchronization:

- Synchronization of external system attributes into ClearID identity attributes is INBOUND only.
CAUTION: Any changes only made to identities in ClearID can be overwritten by the next synchronization from the external system.
- Synchronization can be performed manually using the **Synchronize now** (🔄) option, or automatically at the **Automatic synchronization** intervals specified in the One Identity Synchronization Tool.
 - For each **One Identity field** that is configured, a custom mapping to the **External field** in the external system is created. This mapping ensures that the external system attributes can be synchronized into the One Identity attribute fields.

The following diagram illustrates an Azure AD data synchronization:



The synchronization workflow is essentially the same for all data sources:

1. Data source information is requested.
2. Data source information is returned.
3. Any information changes are processed and detected.
4. Data source information is pushed to the ClearID web application.

Sample SQL files

For the **Database** data source option, sample SQL script files are provided with the tool and can be found here:

C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service

- *Identities_Oracle.sql*
- *Identities_SqlServer.sql*

The sample SQL script files can be used to test the **Database** data source solution, or to help you understand the SQL data format.

Sample CSV files

For the **File** data source option, a sample CSV file is provided with the tool and can be found here:

C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service

- *Identities.csv*

The sample CSV files can be used to test the **File** data source solution, or to help you understand the CSV data format.

About One Identity Synchronization Tool attribute fields

When you synchronize an external system with Genetec ClearID™ using the Genetec ClearID™ One Identity Synchronization Tool, your external system attributes are synchronized (imported) into ClearID identity attributes using the field mappings in the One Identity Synchronization Tool.

NOTE: The data source order is important because the first data source always overrides common fields.

Identity attributes

One Identity field	Data type	Description
Unique ID* * This field is mandatory.	Text field	A unique ID for the identity. The unique ID can be an alphanumeric code or an email address. For example, Employee number xyz12345. IMPORTANT: Azure Active Directory (Microsoft Entra ID) only: If you ever change the mapping of the Unique ID, it can cause duplicate data issues.
Activation date	DateTime	The date that the identity is activated. For example, 1/11/2022. NOTE: All invariant culture DateTime formats are supported.
City	Text field	The city where the identity is located. For example, Paris.
Company	Text field	The company name. For example, Genetec™.
Country code	Text field	The three-letter country code (UPPERCASE). For example, the USA or CAN. NOTE: The three-letter country codes are based on the Alpha-3 codes in the ISO 3166-1 country codes standard.
Date of birth	DateTime	The identity's date of birth. For example, 7/21/2022. NOTE: All invariant culture DateTime formats are supported.
Department	Text field	The department name. For example, IT or Marketing.
Description	Text field	The identity description.

One Identity field	Data type	Description
Email address	Text field	The primary email address (business email) for the identity. For example, johndoe@test.com
Employee number	Text field	The identity's employee number.
Expiration date	DateTime	The date that the identity expires. NOTE: All invariant culture DateTime formats are supported.
First name	Text field	The first name of the identity.
Job title	Text field	The job title of the identity.
Last name	Text field	The last name of the identity.
Middle name	Text field	The middle name of the identity
Mobile phone number	Text field	The secondary phone number (Mobile phone number) For example, 555-555-5555.
Personal email	Text field	The secondary email address (personal email) for the identity. For example, johndoe2@test.com
Phone number	Text field	The primary phone number (Office phone number) For example, 555-555-5555.
Picture	Image	A picture in the format of a blob, a base64 string, or a path to an image. Supported values: - File path - uses a standard windows file path. The path must be accessible from the server. - base64 encoded string - uses a standard base 64 encoding. - Binary - binary data. Supported Image formats: png, jpeg, and bmp.
Preferred name	Text field	The preferred name of the identity.
Provisioning attributes	Text field	The customer defines and configures the provisioning attributes for their environment. The list items are separated by a pipe character " ". For example, A1 A2 A3.
State or province	Text field.	The state or province where the identity is located.
Status	Text field	The Identity activation status. For example, Active or Inactive.
Supervisor name	Text field	The name of the identity's supervisor.
Supervisors	Text field	The list of unique supervisor IDs for the identity. The list items are separated by a pipe character " ". For example, A1 A2 A3.

One Identity field	Data type	Description
Use extended grant time	Boolean value	The value that enables or disables the Use extended grant time option. For example, TRUE or FALSE.
User type	Text field	The type of user. For example, Admin or User .
Username	Text field	The email used by the identity to log on to ClearID.
Web portal access	Text field	The value that enables or disables web portal access . For example, 0 FALSE or 1 TRUE.
Worker type code	Text field	The worker type code.
Worker type description	Text field	The worker type description.
Zip or postal code	Text field.	The Zip or postal code of the identity's location.

About the Azure web app

The Azure web app is a web application that is used to connect Genetec ClearID™ One Identity Synchronization Tool to the Azure AD data so that the Active Directory user information can be accessed and synchronized.

Connection information for Azure web app

To connect the Azure web app to the ClearID One Identity Synchronization Tool, you need the following information:

The screenshot shows a 'Data source configuration' window with a sidebar containing 'Source', 'Configuration' (selected), 'What to sync', and 'Summary'. The main area has three input fields: 'Tenant name', 'Client ID', and 'App key'. A yellow note at the bottom right says '*Field is mandatory'. At the bottom are 'Cancel', 'Back', and 'Next' buttons.

- Tenant name (Directory ID for account)
- Client ID (Application ID)
- App key (Client secret value)

TIP: The Tenant name, Client ID, and App key can be obtained from your Azure Active Directory (Microsoft Entra ID) application registration.

Microsoft Azure | Search resources, services, and docs (5/4)

Home > One Identity

One Identity

Search (Ctrl+V)

Details Endpoints Preview features

Overview

Dashboard

Integration assistant

Manage

Branding & properties

Authentication

Certified & secrets

Token configuration

API permissions

Issues on API

App roles

Groups

Roles and administrators

Monitor

Support & Troubleshooting

Troubleshooting

New support request

Details

Display name

Application ID (Uppercase)

Object ID

User ID

Supported account types

Get started

Documentation

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open source libraries, and application management tools. You can create modern, standards-based authentication solutions, secure and protect APIs, and add sign-in for your users and customers... Learn more

Call APIs

Build more powerful apps with built-in and business data from Microsoft services and your own company's data sources.

View all API permissions

Sign in users in 5 minutes

Take our users to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app.

View all quickstart guides

Microsoft Azure | Search resources, services, and docs (5/4)

Home > One Identity

One Identity | Certificates & secrets

Search (Ctrl+V)

Get feedback

Overview

Dashboard

Integration assistant

Manage

Branding & properties

Authentication

Certified & secrets

Token configuration

API permissions

Issues on API

App roles

Groups

Roles and administrators

Monitor

Support & Troubleshooting

Troubleshooting

New support request

Get feedback

Certificates (0)

Client secrets (5)

Federated credentials (0)

A secret ID that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

Description	Expires	Value	Secret ID
One Identity	1/21/2022	...	...

Azure AD API permissions

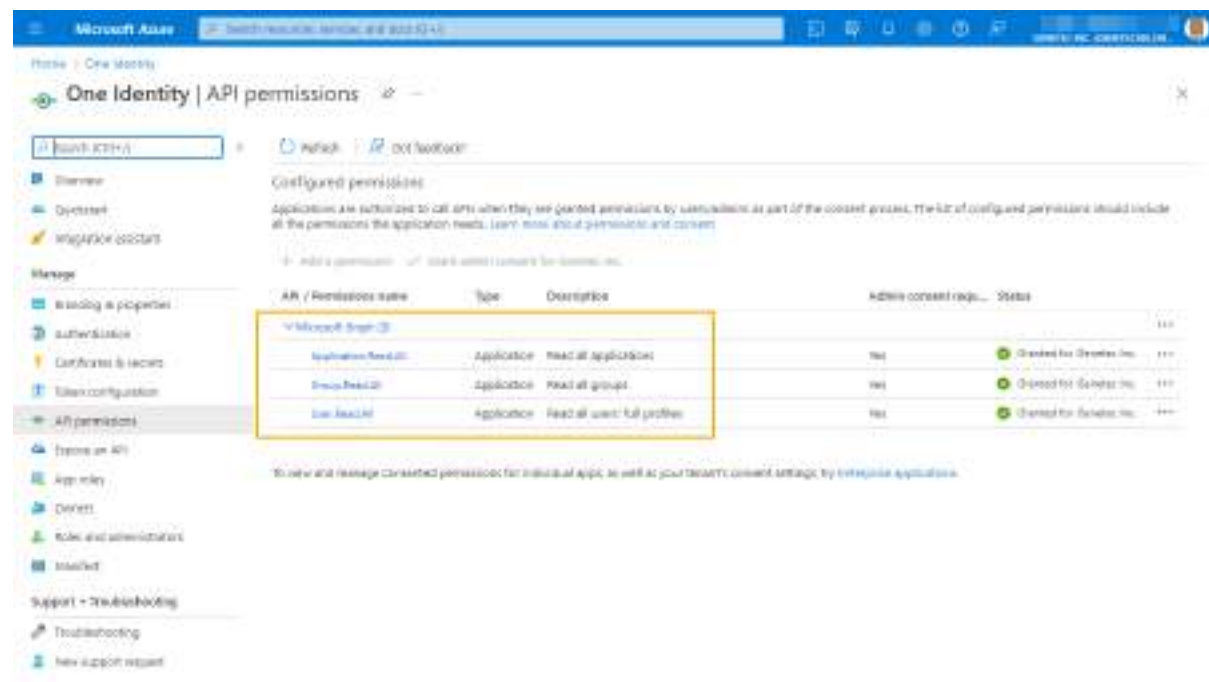
Before you can synchronize data with Genetec ClearID™, an external system attributes administrator (IT or security personnel) must set up and configure the following API read permission privileges in Azure AD.

Microsoft Graph (minimum requirements):

- *Application.Read.All* - Used to get extensions attributes.
 - Allows the app to read applications and service principals without a signed-in user.

For more information, see [List extensionProperties \(directory extensions\)](#)

- *User.Read.All* - Used to get user information.
 - Allows the app to read identity user risk information for all users in your organization without a signed-in user.
- *Group.Read.All* - Used to get group information.
 - Allows the app to read group properties and memberships, and read conversations for all groups, without a signed-in user.



For more information, see [Microsoft Graph permissions reference](#).

Installing the One Identity Synchronization Tool

Before you can import identities information from an external system into Genetec ClearID™, you must first install the Genetec ClearID™ One Identity Synchronization Tool.

Before you begin

Obtain the latest installer package from your deployment contact.

What you should know

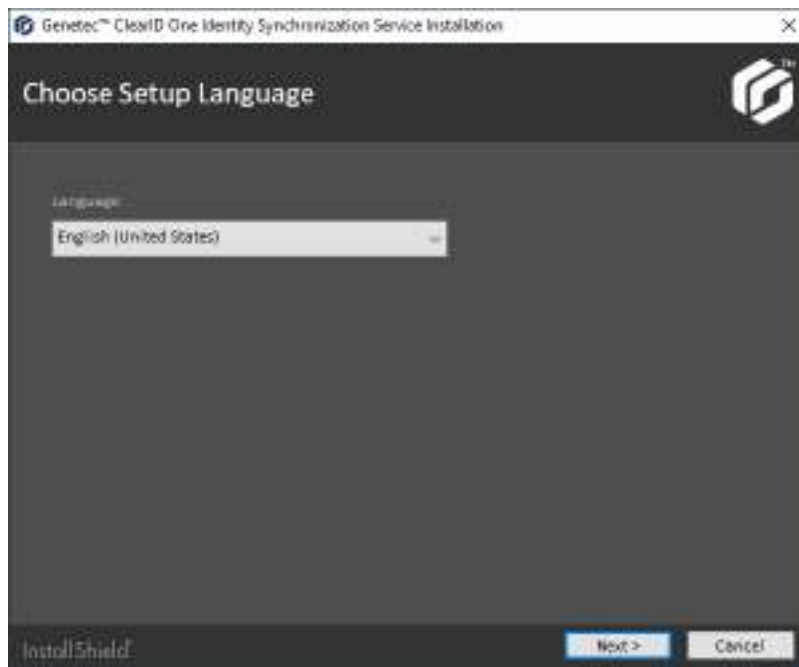
This procedure is for IT or security personnel responsible for external system attributes administration.

Install the One Identity Synchronization Tool on its own dedicated server. It doesn't require a Security Center SaaS server.

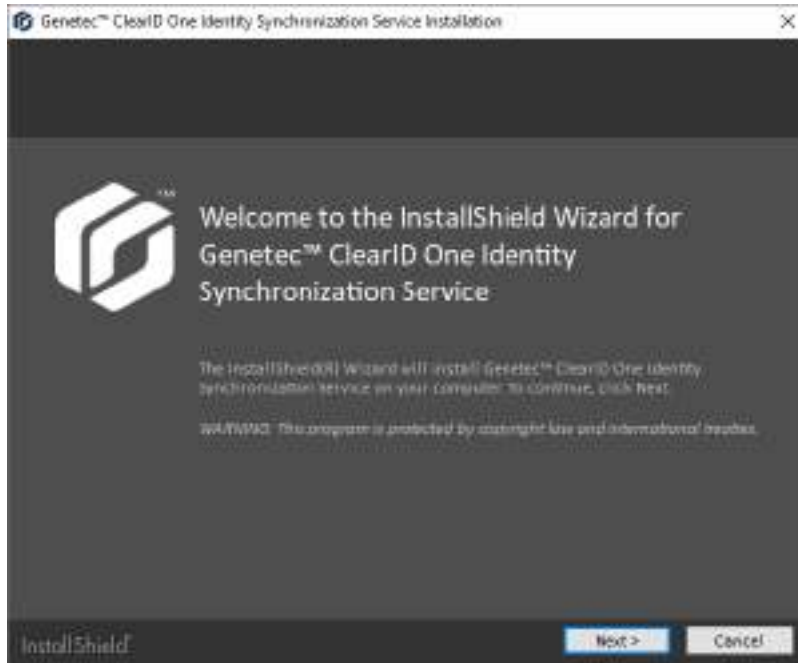
NOTE: The One Identity Synchronization Tool isn't generally available as a public download. The synchronizer download is supplied by your deployment contact when needed.

Procedure

- 1 Navigate to the ClearID One Identity Synchronization Tool installer supplied by your deployment contact.
- 2 Right-click the *setup.exe* file. Then click **Run as administrator** and follow the installation instructions.
- 3 In the *Genetec ClearID™ One Identity Synchronization Service Installation* dialog, select a setup language and click **Next**.



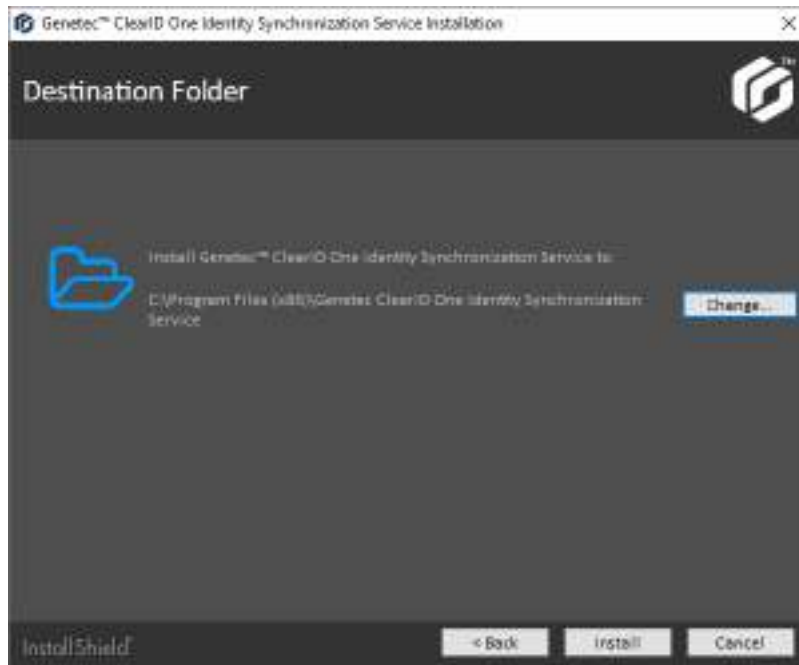
- 4 In the *Welcome to the InstallShield Wizard* section, click **Next**.



- 5 Review and accept the license agreement, then click **Next**.

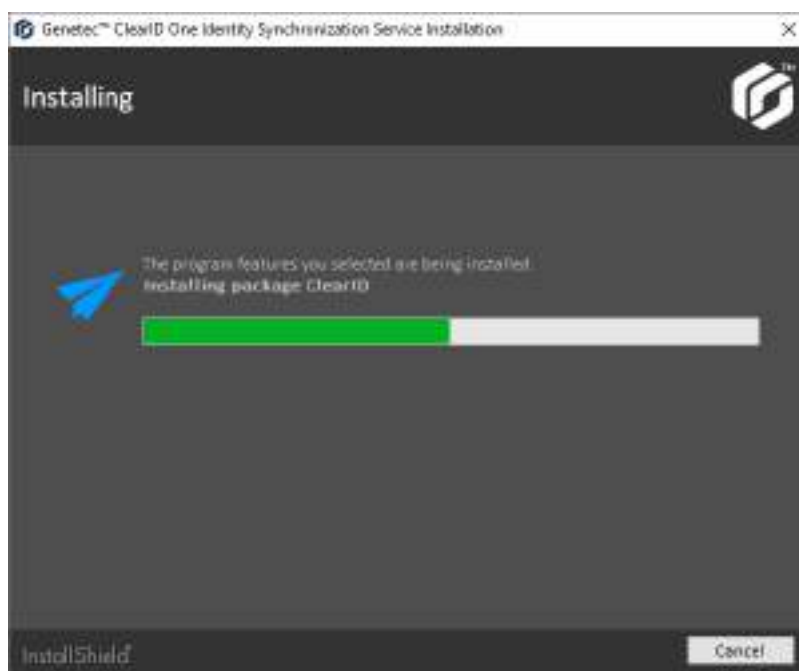


- 6 Specify your destination folder.

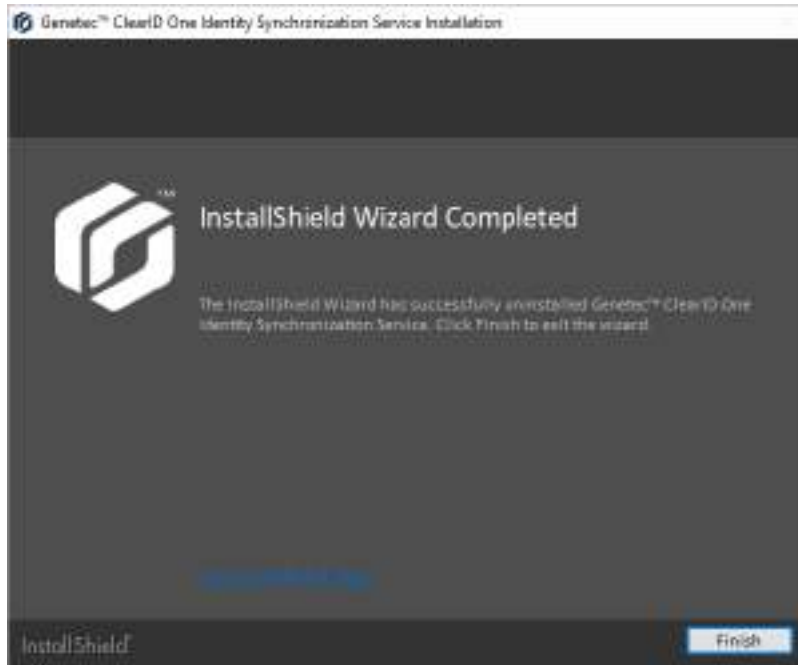


By default, the service is installed at *C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service*.

- 7 (Optional) Click **Change** to modify the destination folder.
- a) In the **Browse For Folder** dialog, browse to and select the folder where you want the service installed and click **OK**.
- 8 Click **Install**.



- Click **Finish** to complete the installation.



The ClearID One Identity Synchronization Tool is now installed.

After you finish

Configure the synchronization tool.

Uninstalling the One Identity Synchronization Tool

From time to time, you might want to uninstall the Genetec ClearID™ One Identity Synchronization Tool to fix a problem or install an updated version.

Before you begin

The Genetec ClearID One Identity Synchronization Tool must be installed.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

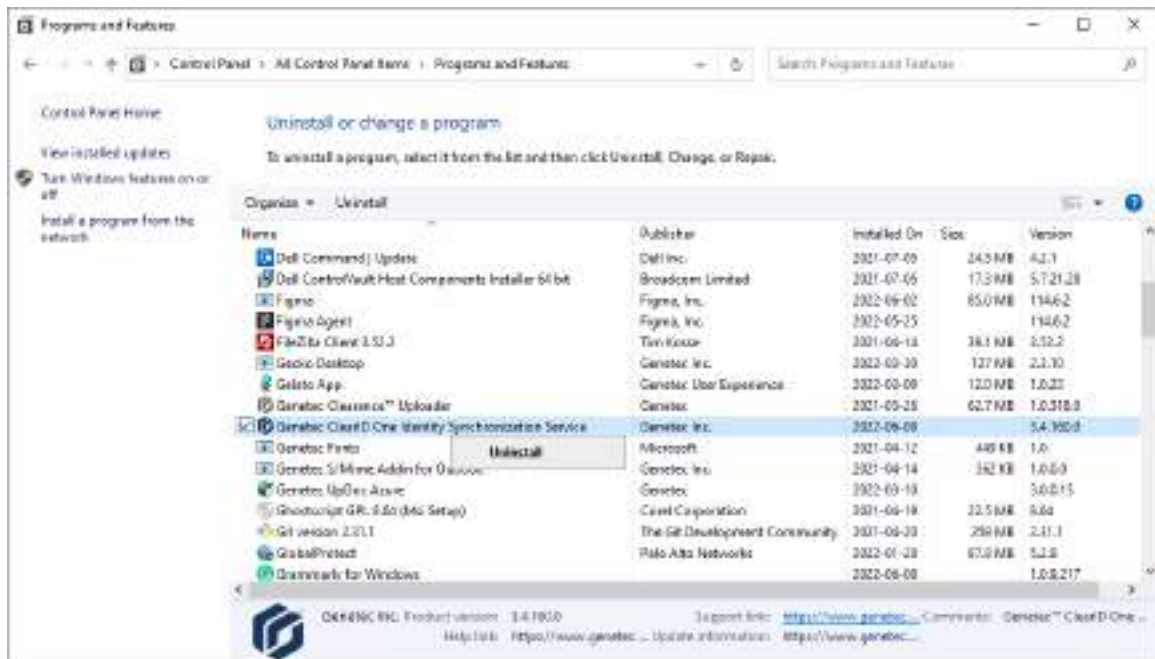
- The options that you encounter while uninstalling a program (service) might vary depending on the version of Windows that you're running.
- This procedure describes how to uninstall the synchronization tool (service) from a Windows 10 client.

CAUTION: The uninstall process deletes all configuration data. If you are upgrading, make sure that you back up your program data in the configuration folder `C:\ProgramData\Genetec\OneIdentity\Configuration`.

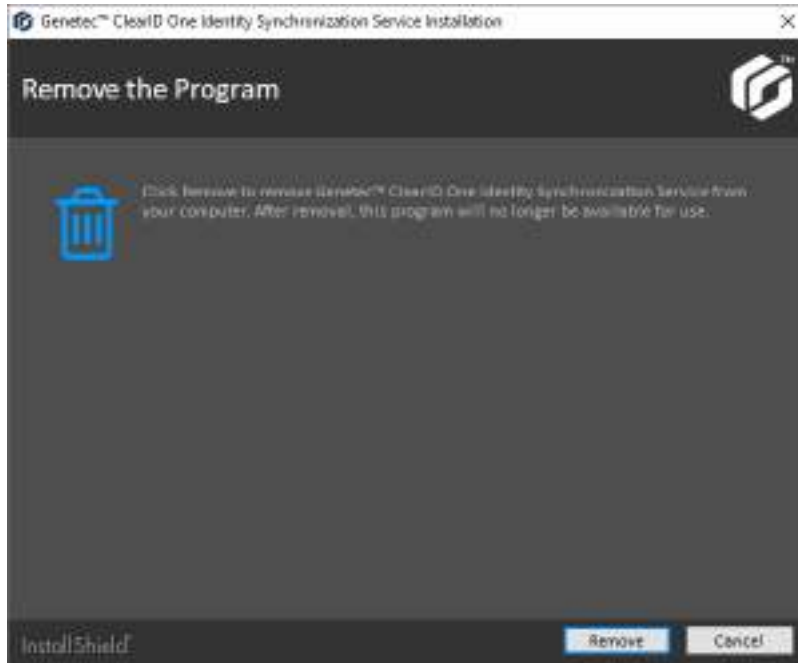
Procedure

- Open the Windows **Control Panel**, and in the *Programs* section click **Uninstall a program** to access **Programs and Features**.

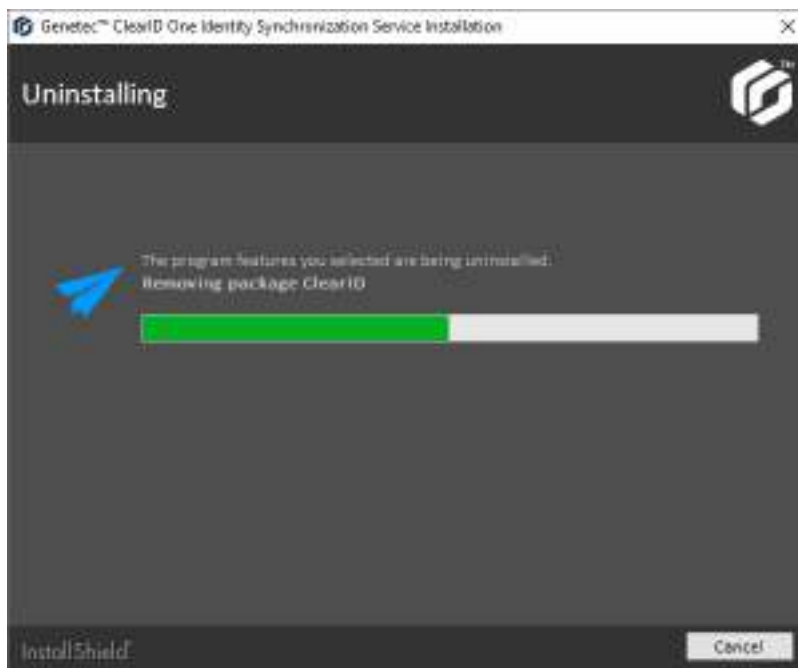
- Find the ClearID One Identity Synchronization Tool service and right-click to display the **Uninstall** option, then click **Uninstall**.



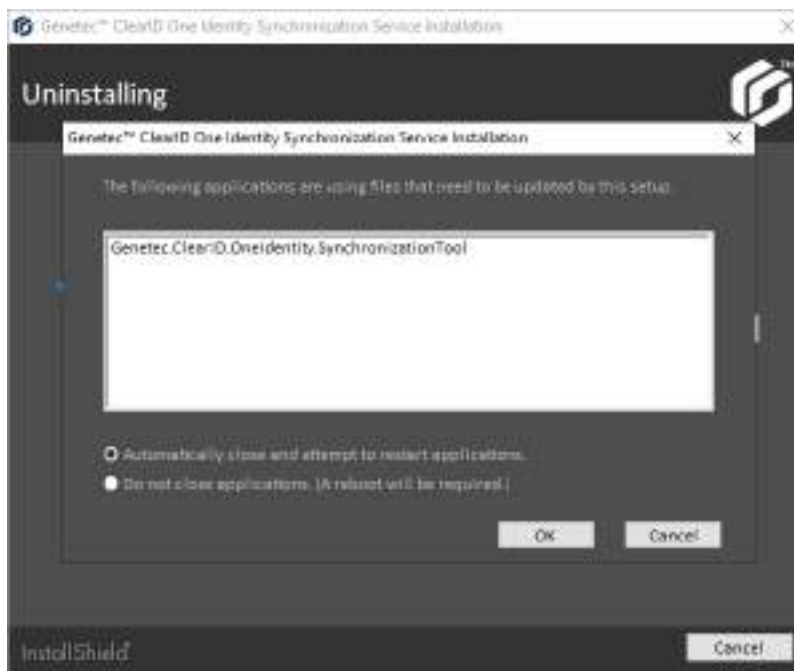
- 3 Click **Remove** to remove the program.



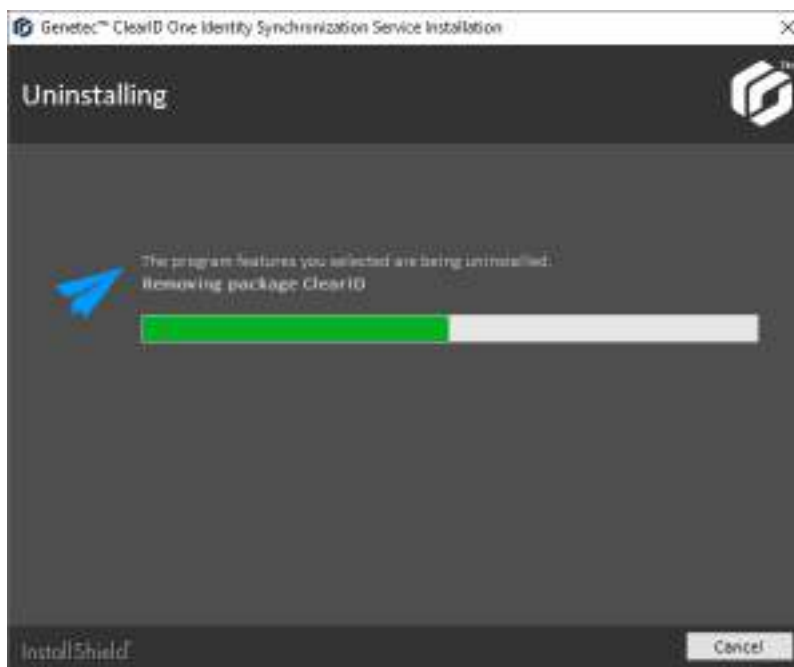
The program uninstall begins.



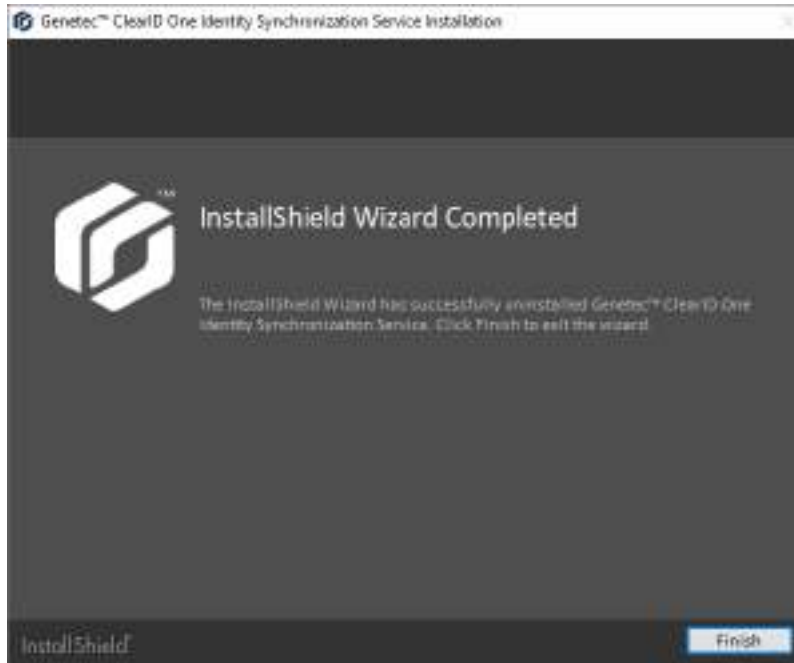
- 4 (Optional) If the following dialog is displayed, select **Automatically close and attempt to restart applications** then click **OK**.



The package continues to uninstall.



- 5 Click **Finish** to complete the uninstall.



The ClearID One Identity Synchronization Tool has now been uninstalled.

Upgrading the One Identity Synchronization Tool

Upgrade Genetec ClearID™ One Identity Synchronization Tool to the latest version when it becomes available so that you can use new features.

Before you begin

The Genetec ClearID One Identity Synchronization Tool must be installed.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

Procedure

- 1 Back up the configuration folder `C:\ProgramData\Genetec\OneIdentity\Configuration`.
The folder contains configuration settings. For example, *ApiConfiguration.dat*, *ClearIdEntityMappingFile.xml*, *Configuration.xml*, and *SingleCardEntityMapping.xml*.
NOTE: The *.dat* or *.xml* files that you encounter in the configuration folder vary depending on the settings that you configure in the ClearID One Identity Synchronization Tool.
- 2 [Uninstall ClearID One Identity Synchronization Tool](#) (previous version).
- 3 [Install ClearID One Identity Synchronization Tool](#) (latest version).
- 4 Validate the ClearID One Identity Synchronization Tool is working as expected.
NOTE: You should have the same data source configurations as before the upgrade.

The ClearID One Identity Synchronization Tool has now been upgraded.

Configuring the One Identity Synchronization Tool

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool.

Before you begin

- [Familiarize yourself with the One Identity attribute fields.](#)
- Verify the identities attributes values that you want to import and synchronize before synchronizing.
- [Download a service authentication key.](#)
- [Install the One Identity Synchronization Tool.](#)

IMPORTANT: Make sure that the file isn't being edited and is closed, because the synchronization tool locks the file during the synchronization process.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

Synchronization of external system attributes into ClearID identity attributes is INBOUND only.

CAUTION: Any changes only made to identities in ClearID can be overwritten during the next synchronization from the external system.

Procedure

- 1 [Configure your connection settings.](#)
- 2 Configure data source settings for one of the following sources:
 - [Azure AD \(Microsoft Entra ID\)](#)
 - [Database \(Microsoft SQL Server, Oracle Database, ODBC\)](#)
 - [File \(CSV\)](#)
- 3 [Configure your synchronization settings.](#)
- 4 Click **Save**.

After you finish

[Verify that the new attributes from the external system have been synchronized and contain the correct attributes.](#)

Configuring connection settings

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool connection settings.

Before you begin

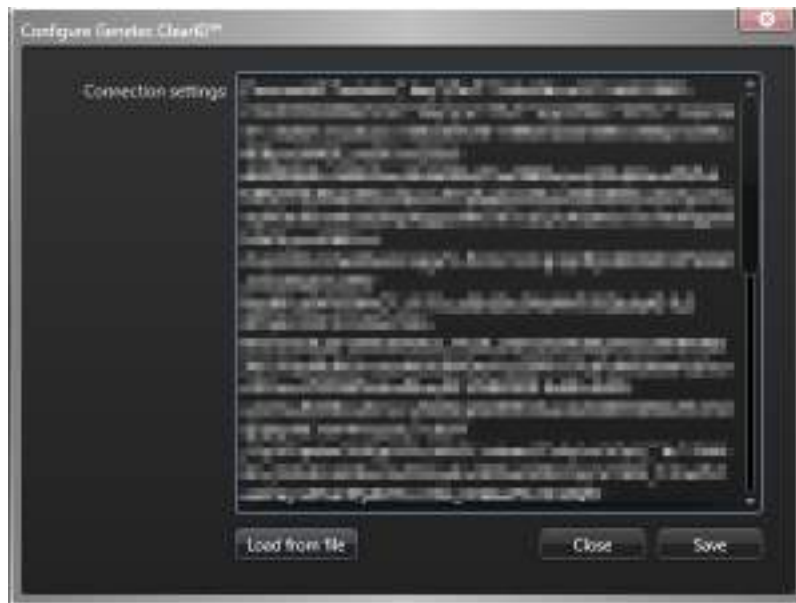
- Verify the attributes values for the identities that you want to import before synchronizing your identities.
- [Download a service authentication key.](#)

Procedure

- 1 Open the One Identity Synchronization Tool (*OneIdentityConfigurationTool.exe*) and configure your settings.



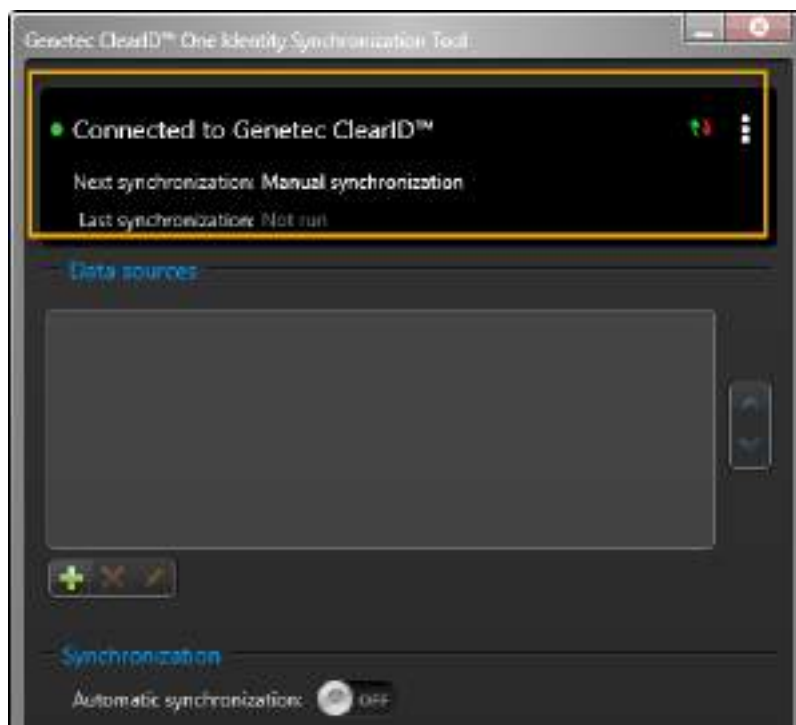
- 2 Configure your connection settings.
 - a) In the One Identity Synchronization Tool, click **Configure**.
 - b) In the *Configure Genetec ClearID™* dialog, click **Load from file**.
 - c) Navigate to and select your authentication key.



- 3 Click **Save**.

NOTE: The One Identity service is automatically restarted when the connection settings for the authentication key are changed.

Your One Identity Synchronization Tool is now connected to ClearID.



After you finish

Configure your data sources. Choose one of the following:

- [Configuring the data source for Azure AD synchronization](#) on page 211
- [Configuring the data source for Database synchronization](#) on page 219
- [Configuring the data source for File synchronization](#) on page 228

Configuring the data source for Azure AD synchronization

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool data sources for Azure Active Directory synchronization.

Before you begin

- [Familiarize yourself with the One Identity attribute fields.](#)
- [Familiarize yourself with the Azure web app.](#)
 - Make a note of the connection settings for the Azure web app for later use.
 - Make sure that the Azure AD API permissions are set up.
- Prepare an Azure Active Directory containing the identities attributes that you want to import and synchronize.

What you should know

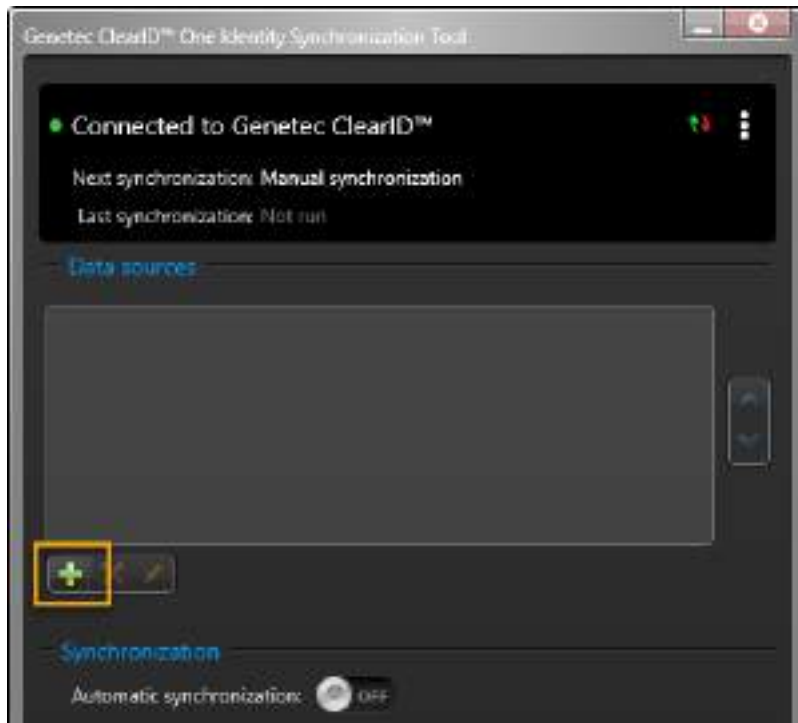
This procedure is for IT or security personnel responsible for external system attributes administration.

This procedure describes how to configure the data source for **Azure AD** (Microsoft Entra ID).

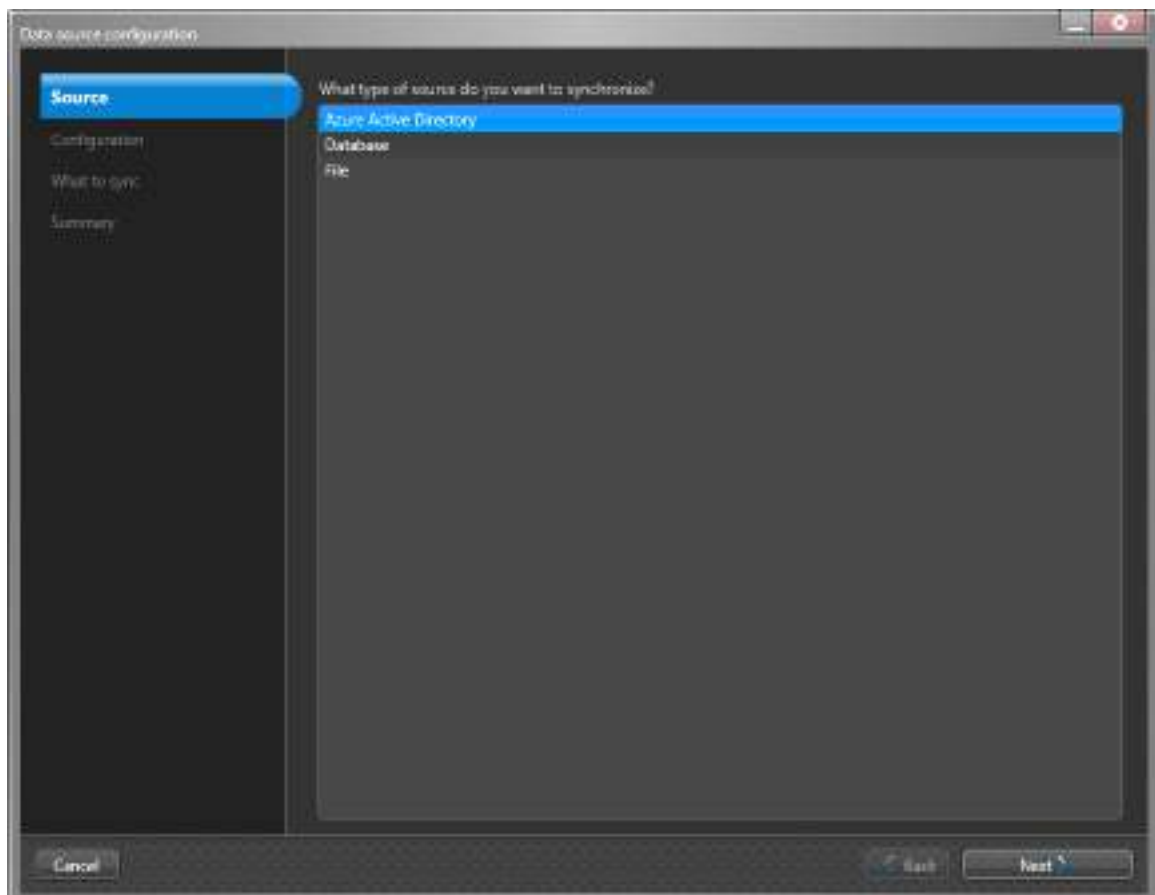
- The data source order is important because the first data source always overrides common fields.
- There is no limit to the number of data sources. However, the larger the data source, the memory requirements increase.
- When using an Azure data source to synchronize identities, the only possible field for **Unique ID** is the **UserId** field. When the Azure data source is selected, the **Unique ID** fields can't be configured and use of the Azure **UserId** field is triggered by default.

Procedure

- 1 In the One Identity Synchronization Tool *Data sources* section, click **Add data source** (+).



- 2 In the *Source* section of the *Data source configuration* dialog, select **Azure Active Directory** and click **Next**.

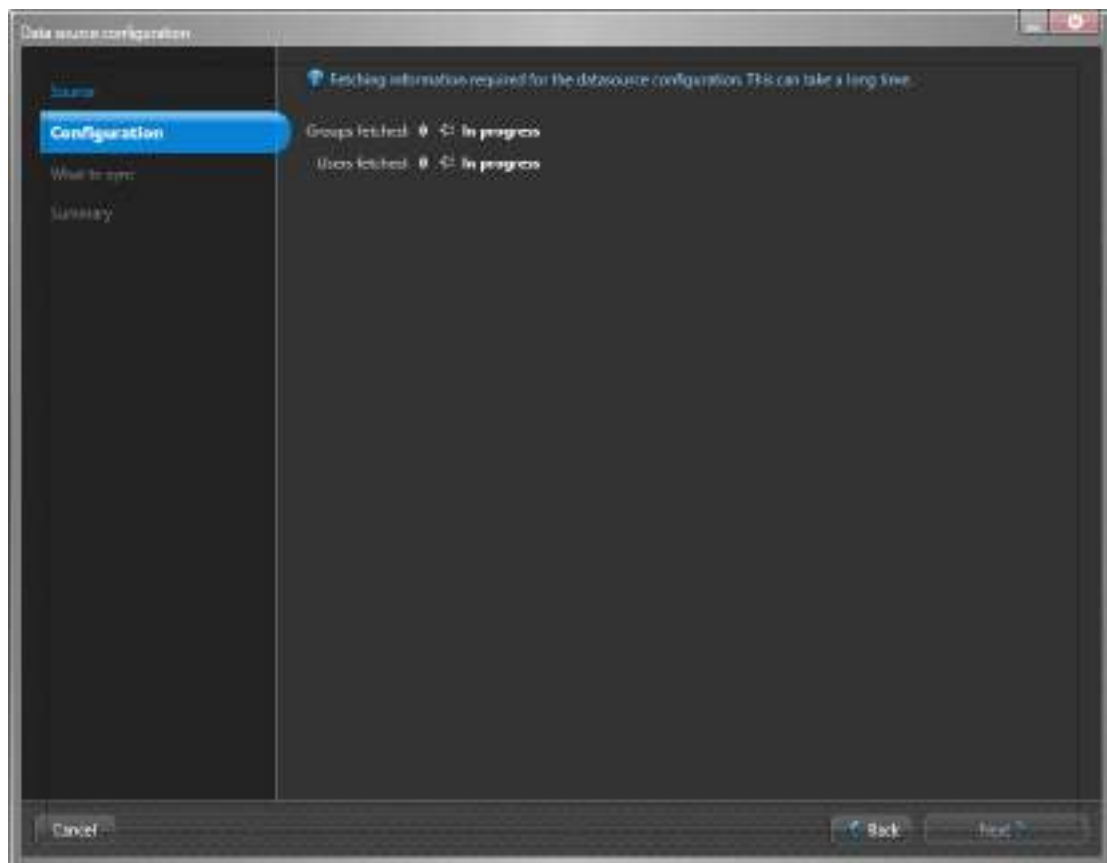


- 3 In the *Configuration* section of the *Data source configuration* dialog, complete the following mandatory fields:

- **Tenant name:** In the **Tenant name** field, enter your tenant name (account name). The tenant name is used to connect to the directory for the account. For example, a host address *account.onmicrosoft.com* or a GUID *nxnxxnxx-nnnn-nxnn-nnnn-nxnnnnnnnnnn*.
- **Client ID:** In the **Client ID** field, enter your client ID. The client ID is used to connect to the client application. The **Client ID** format is an alpha-numeric format as follows: *nxnxxnxx-nxnn-nnnn-xxxx-nxnnnnnnnnnn*.
- **App key:** In the **App key** field, enter your App key. The App key is used to authenticate communications with ClearID. The **App key** format is an alpha-numeric format as follows: *nXnxxxxXxxXnxxxXXXXXnxxxXXXXnxxxXnXXXXxxx=*.

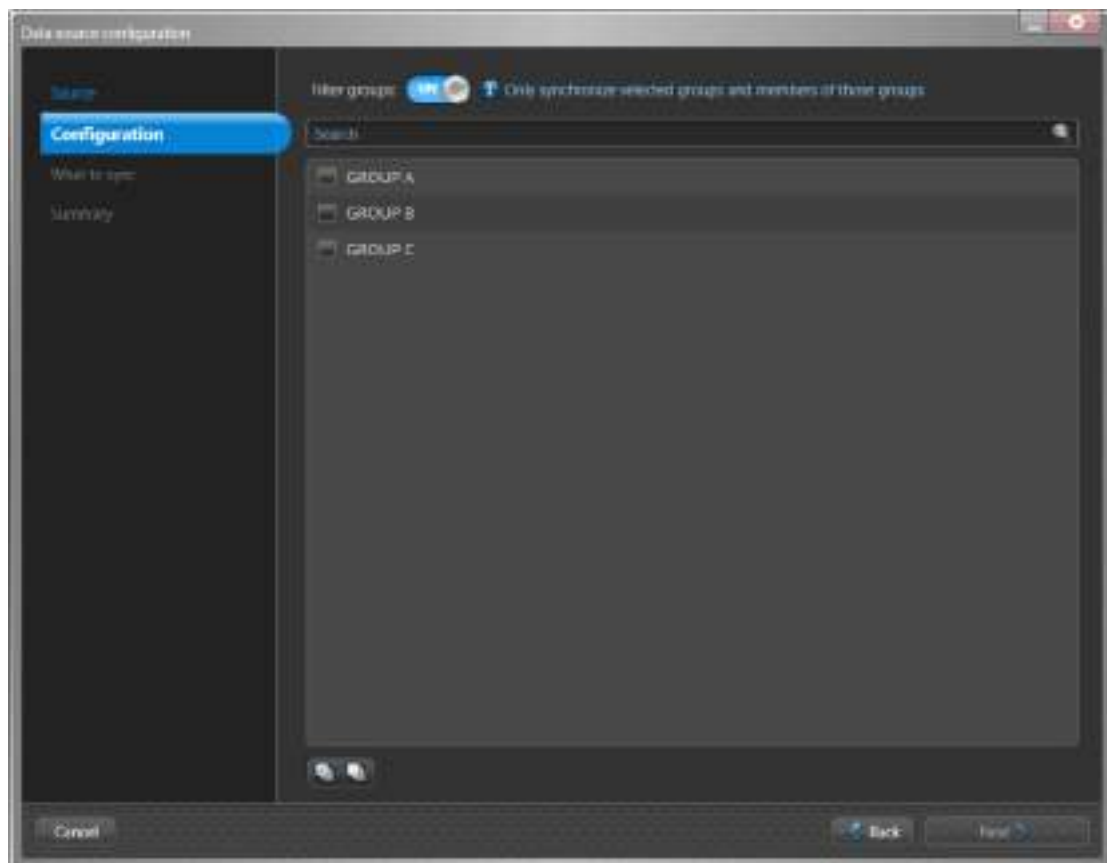
TIP: The Tenant name, Client ID, and App key can be obtained from your Azure Active Directory (Microsoft Entra ID) application registration.

- a) Click **Next**.



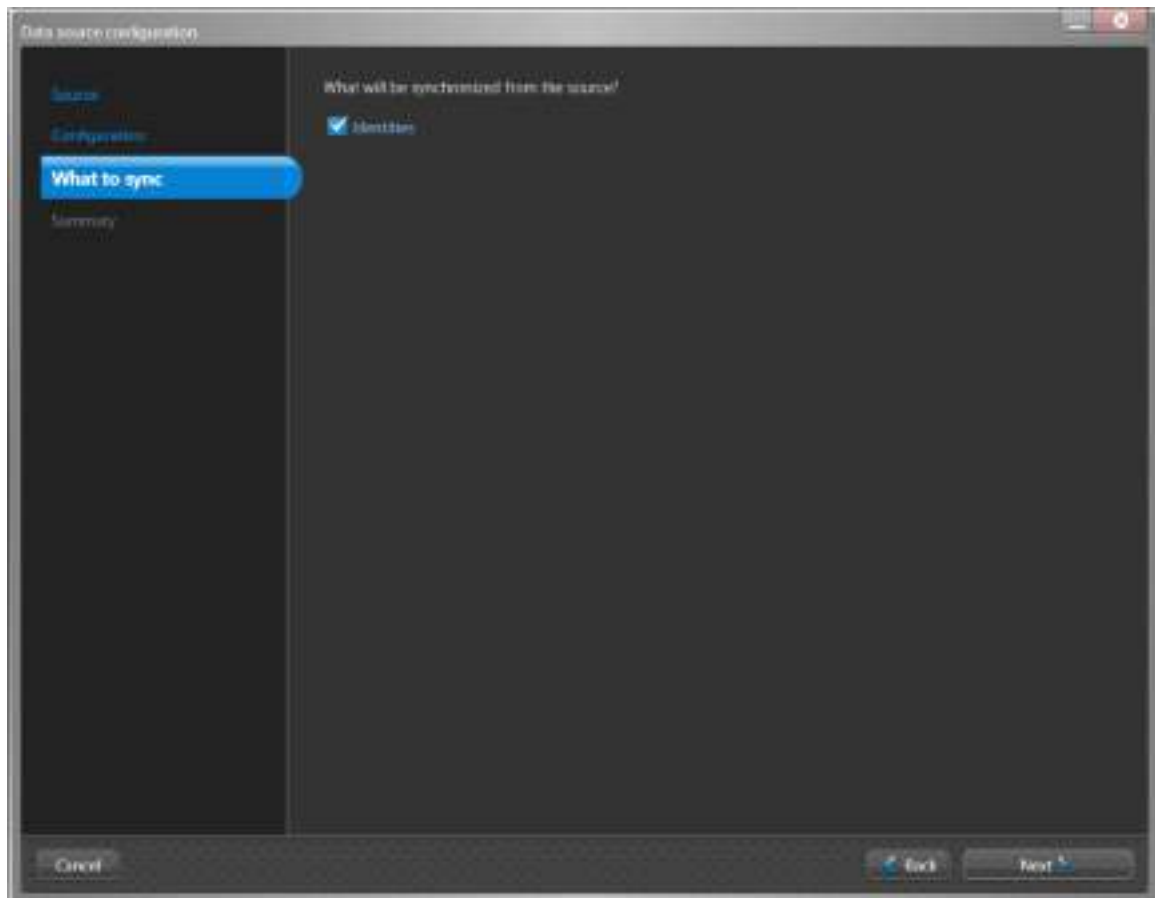
NOTE: Fetching information required for the data source configuration can take a long time and varies depending on the number of groups and users fetched.

- b) (Optional) Use the **Filter groups** option to only synchronize a subset of selected Azure AD groups and group members. Search for or select the groups that you require and click **Next**.



NOTE: If your Azure AD list is long, you can also use the **Check all** or **Uncheck all** icon to help you during your selection process.

- 4 In the *What to sync* section of the *Data source configuration* dialog, select **Identities** to synchronize from the external system data source.



- 5 If you selected **Identities** as a data source, in the *What to sync* section, configure the identity attributes settings.

NOTE: The fields that are displayed in the *Identities* section vary depending on the data source you selected in the *Source* section.

The following image shows the options that are displayed after selecting an **Azure AD** data source.

One Identity field	External field	Sample value
* Unique ID	Thumbnail	0f000000-0000-...
Activation date	Unassigned	
City	Unassigned	
Company	CompanyName	Genetec
Country code	Country	Canada
Date of birth	Unassigned	
Department	Department	
Description	Unassigned	
Email address	Unassigned	IT
Employee number	Unassigned	
Expiration date	Unassigned	
First name	GivenName	John
Job title	JobTitle	IT Manager
Last name	Unassigned	
Match name	Unassigned	
Mobile phone number	Unassigned	
Personal email	Unassigned	

- a) Configure your **External field** attribute mappings.

- **One Identity field:** Displays the ClearID identity attributes. Mandatory fields are highlighted using an asterisk (*).
- **External Field:** Select system attributes in the **External field** columns that you want to map from the external system to the ClearID identity attributes shown in the **One Identity field** column.

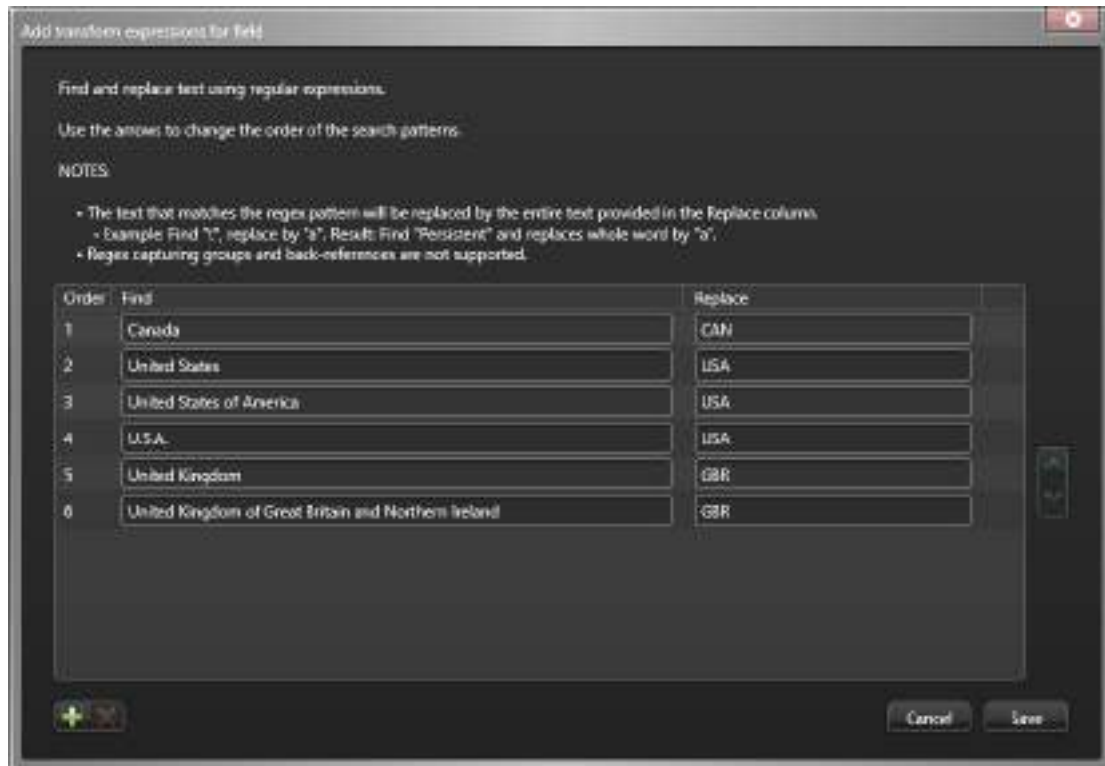
CAUTION: When using **Azure AD** as your data source, the One Identity **Unique ID** field must be mapped to the Azure AD **User ID** external field to ensure that the identity attributes are correctly mapped and synchronized.

- **Sample value:** If an **External field** is selected, an example of the selected external field data from your data source is displayed (if available) in the **Sample value** column next to the **External field** column.

TIP: Use the sample value column to check the format of the attributes data you are about to import from your external system fields into ClearID.

- b) (Optional) Click **Script**  to add a transform expression to find and replace external field text using regular expressions.

For example, you can look for variations of a country name to replace with the correct country code.

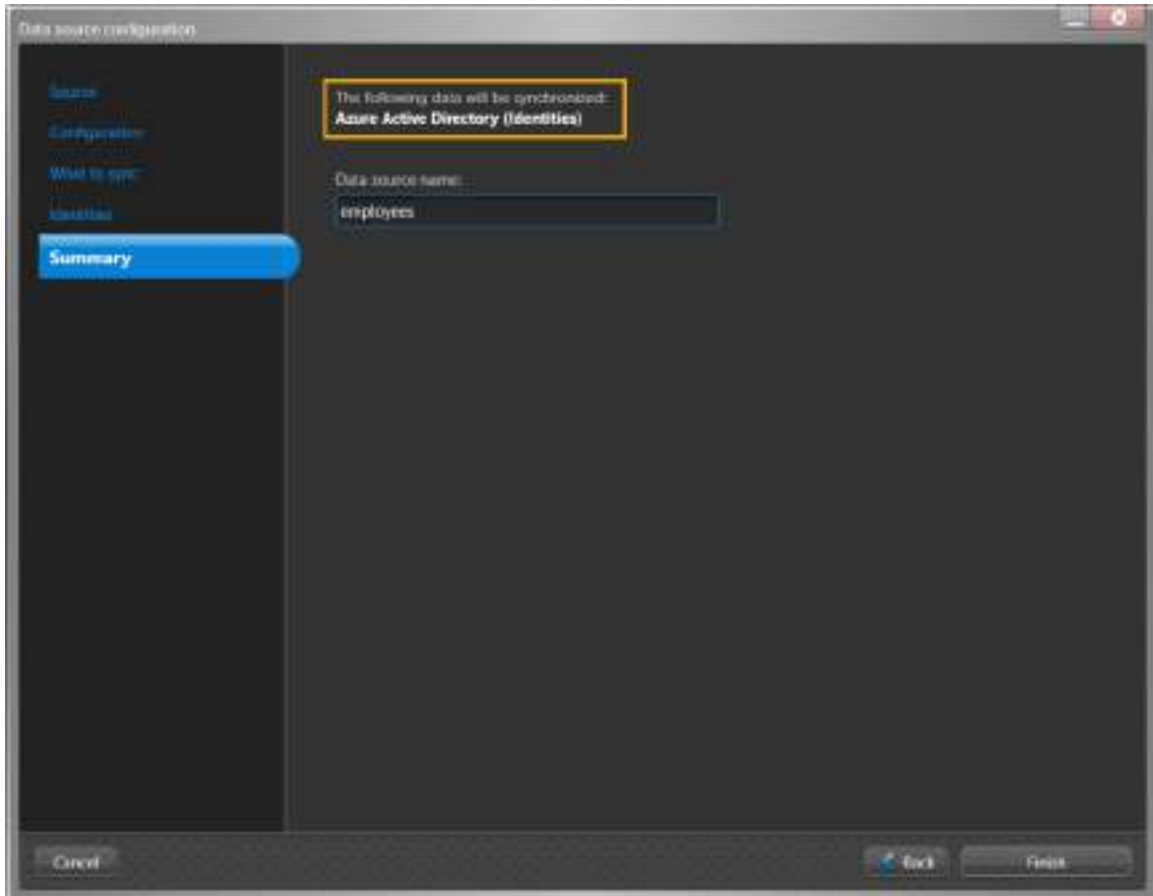


- A script icon  is shown in the **Sample value** column when the field text is being replaced with a regular expression.
- The transform expressions are processed in the order specified in the *Add transform expressions for field* dialog.

TIP: If required, you can select the row of any expressions that you no longer require, and click **delete** .

- c) (Optional) Click **Refresh**  to update the external fields data from your data source. This refresh option is used in situations where the existing data has been modified, new data rows have been added, or new attribute columns have been added.
- d) Click **Next**.

- 6 In the *Summary* section, review the data that will be synchronized.



NOTE: If multiple data sources are selected, only the first data source file is displayed in the *Summary* section **Data source name** field. If you want each of the data files listed in the **Data sources** section, you must add them individually.

- a) If the data synchronization details look correct, click **Finish**.

After you finish

[Configure your synchronization settings.](#)

Related Topics

[About One Identity Synchronization Tool attribute fields](#) on page 195

Configuring the data source for Database synchronization

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool data sources for database synchronization.

Before you begin

- [Familiarize yourself with the One Identity attribute fields.](#)
- Prepare a Database containing identities attributes that you want to import and synchronize.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

This procedure describes how to configure the data source for a **Database** (Microsoft SQL Server, Oracle Database, ODBC).

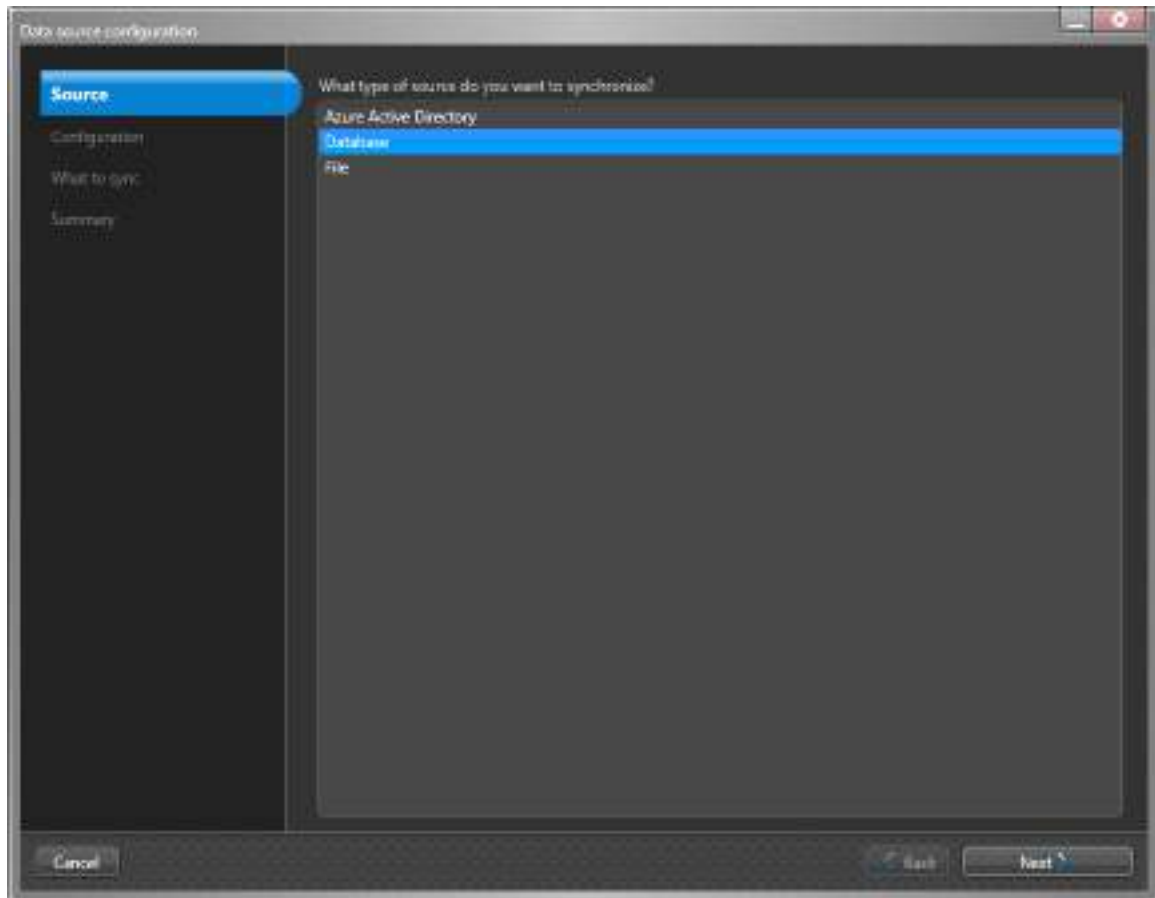
- The data source order is important because the first data source always overrides common fields.
- There is no limit to the number of data sources. However, the larger the data source, the memory requirements increase.

Procedure

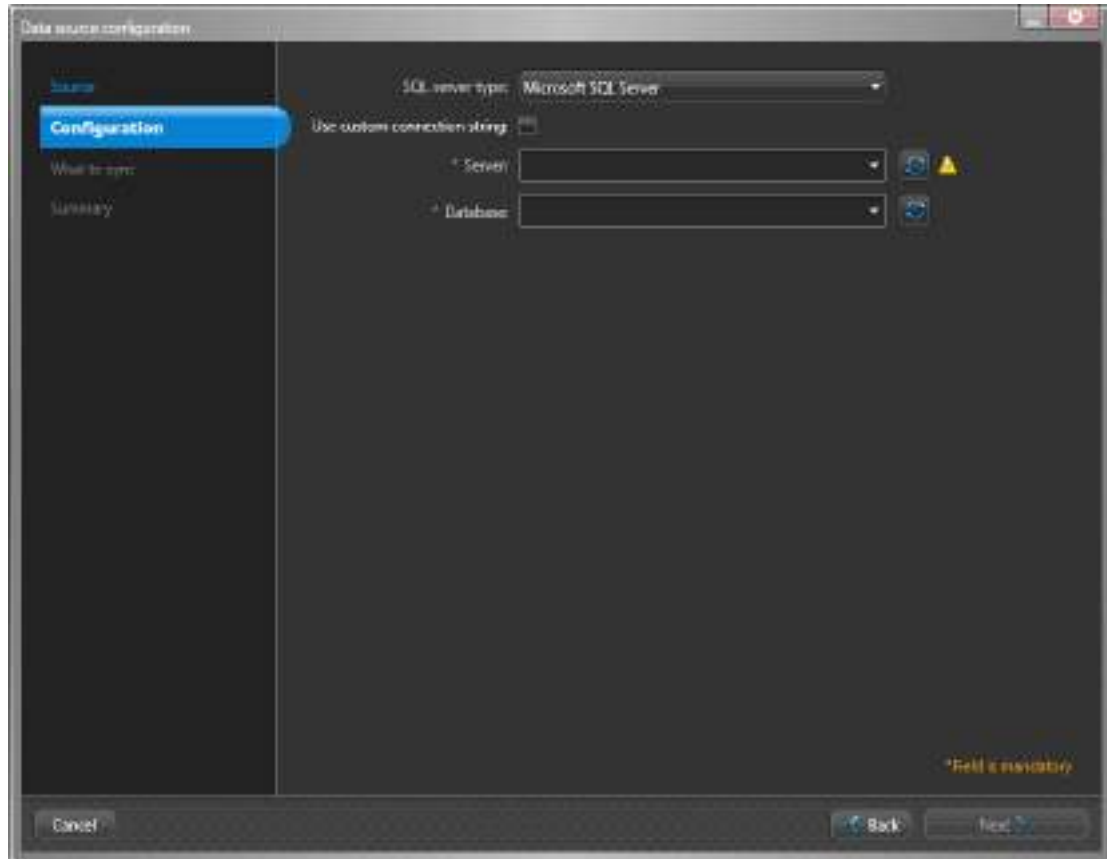
- 1 In the One Identity Synchronization Tool *Data sources* section, click **Add data source** (+).



- 2 In the *Source* section of the *Data source configuration* dialog, select **Database** and click **Next**.



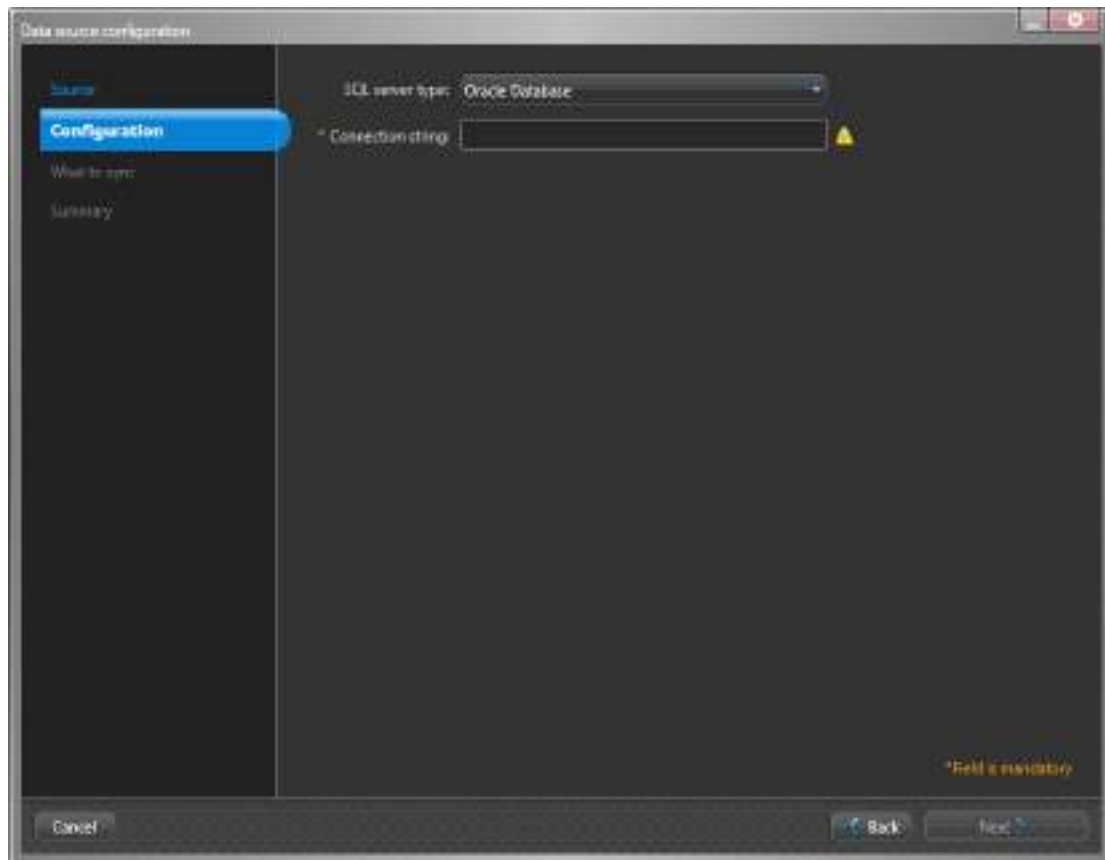
- 3 In the *Configuration* section of the *Data source configuration* dialog, configure the database settings.
 - a) Select an SQL server type:
 - Microsoft SQL Server
 - Oracle Database (only views are currently supported)
 - ODBC
 - b) If you selected **Microsoft SQL Server**, configure the following:



- **Use custom connection string:** Select the checkbox if you want to use a custom connection string.
NOTE: If you use the **Use custom connection string** option, the **Server** and **Database** fields are removed.

- **Connection string:** Enter the connection string.
- **Server:** Enter SQL Server information or select a server from the list.
- **Database:** Enter Database information or select a database from the list.

c) If you selected **Oracle Database**, configure the following:



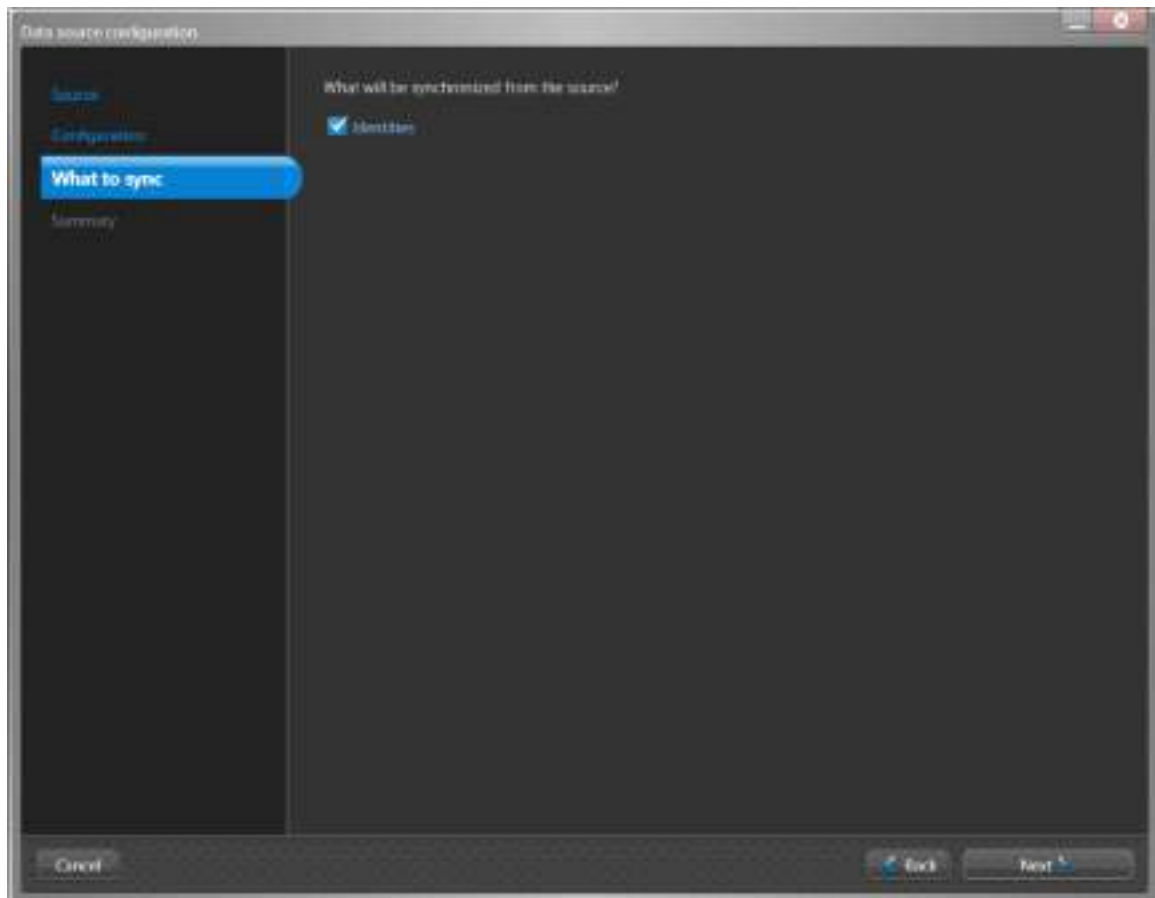
- **Connection string:** Enter the connection string.

d) If you selected **ODBC**, configure the following:

The image shows a 'Data source configuration' window with a dark theme. On the left is a sidebar with four tabs: 'Source', 'Configuration' (which is highlighted in blue), 'What to sync', and 'Summary'. The main area of the window is for configuration. It has a label 'SQL server type:' followed by a dropdown menu showing 'ODBC'. Below that is a label '* Connection string:' followed by a text input field. A yellow warning triangle icon is to the right of the input field. At the bottom right of the main area, there is a note '*Field is mandatory'. At the bottom of the window are three buttons: 'Cancel', 'Back', and 'Next'.

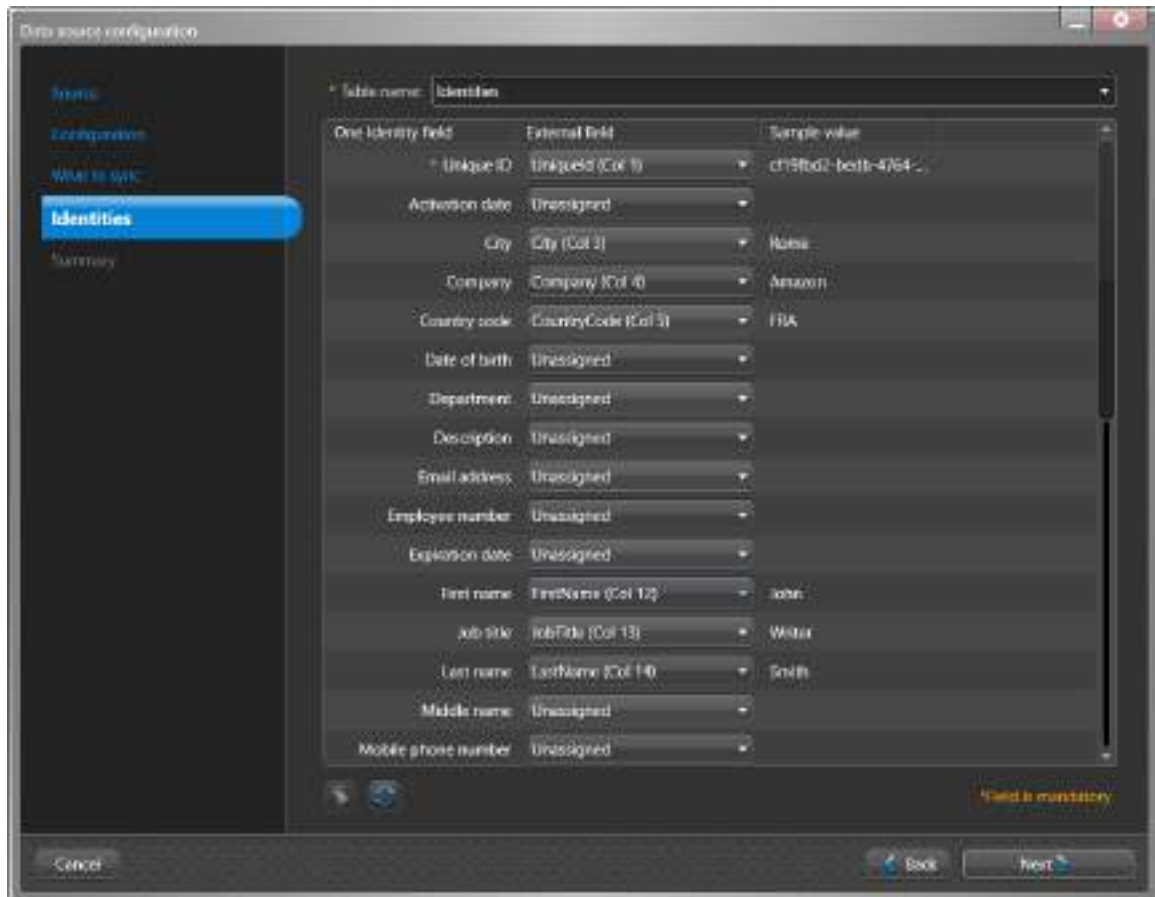
- **Connection string:** Enter the connection string.

- 4 In the *What to sync* section of the *Data source configuration* dialog, select **Identities** to synchronize from the external system data source.



- 5 If you selected **Identities** as a data source, in the *What to sync* section, configure the identity attributes settings.

NOTE: The fields that are displayed vary depending on the data source you selected in the *Source* section. The following image shows the options that are displayed after selecting a **Database** data source.



- a) Configure your **External field** attribute mappings.

- **One Identity field:** Displays the ClearID identity attributes. Mandatory fields are highlighted using an asterisk (*).

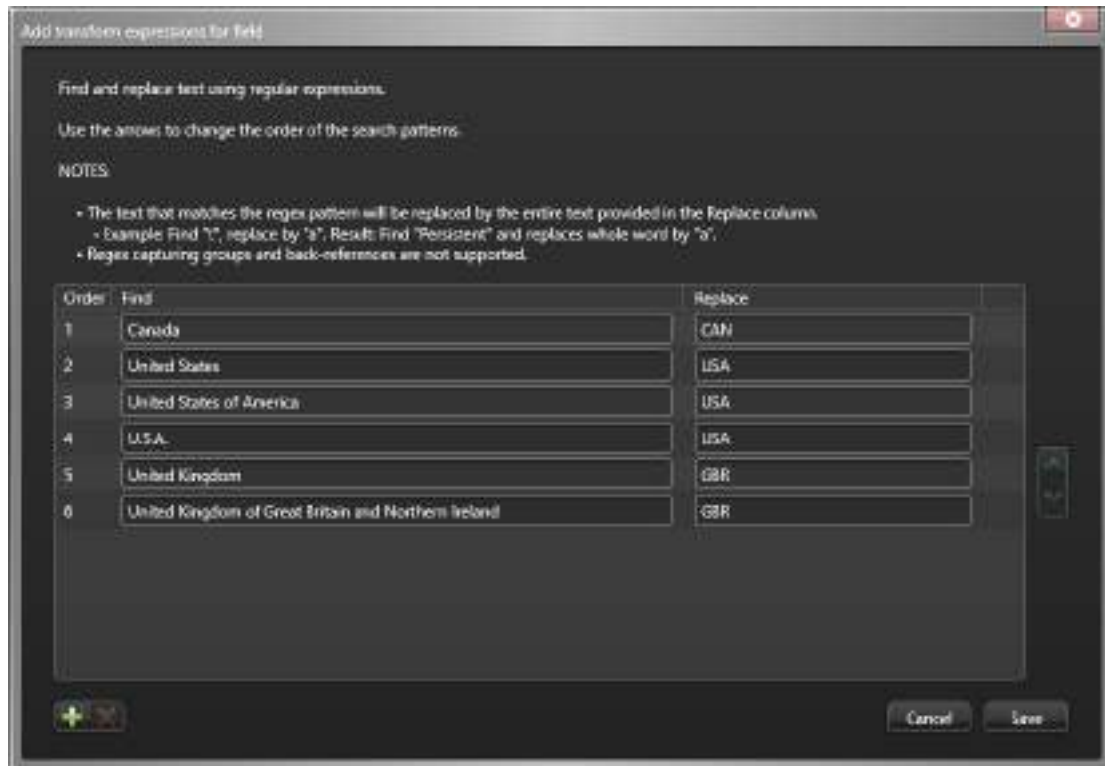
IMPORTANT: The Unique ID is used internally by One Identity as the primary key to identify what it is. For example, an employee number or email address could be used, as long as it is unique.

- **External Field:** Select system attributes in the **External field** columns that you want to map from the external system to the ClearID identity attributes shown in the **One Identity field** column.
- **Sample value:** If an **External field** is selected, an example of the selected external field data from your data source is displayed (if available) in the **Sample value** column next to the **External field** column.

TIP: Use the sample value column to check the format of the attributes data you are about to import from your external system fields into ClearID.

- b) (Optional) Click **Script**  to add a transform expression to find and replace external field text using regular expressions.

For example, you can look for variations of a country name to replace with the correct country code.

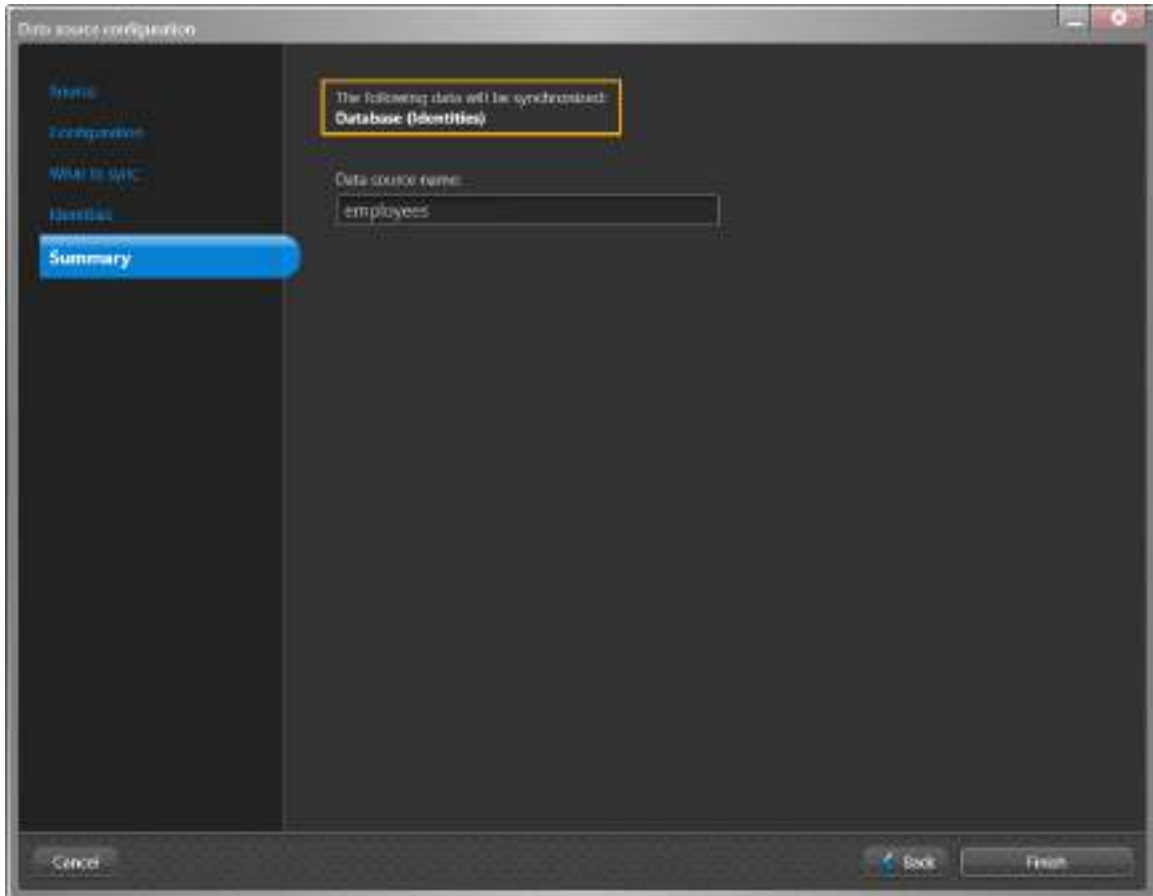


- A script icon  is shown in the **Sample value** column when the field text is being replaced with a regular expression.
- The transform expressions are processed in the order specified in the *Add transform expressions for field* dialog.

TIP: If required, you can select the row of any expressions that you no longer require, and click **delete** .

- c) (Optional) Click **Refresh**  to update the external fields data from your data source. This refresh option is used in situations where the existing data has been modified, new data rows have been added, or new attribute columns have been added.
- d) Click **Next**.

- 6 In the *Summary* section, review the data that will be synchronized.



NOTE: If multiple data sources are selected, only the first data source file is displayed in the *Summary* section **Data source name** field. If you want each of the data files listed in the **Data sources** section, you must add them individually.

- a) If the data synchronization details look correct, click **Finish**.

After you finish

[Configure your synchronization settings.](#)

Related Topics

[About One Identity Synchronization Tool attribute fields](#) on page 195

Configuring the data source for File synchronization

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool data sources for file (CSV) Synchronization.

Before you begin

- [Familiarize yourself with the One Identity attribute fields.](#)
- Prepare a CSV file containing the identities attributes that you want to import and synchronize.

IMPORTANT: Make sure that your CSV files aren't being edited and are closed, because the synchronization tool locks the files during the synchronization process.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

This procedure describes how to configure the data source for a **File** (CSV import).

- The data source order is important because the first data source always overrides common fields.
- One data source can include multiple CSV files containing identities.
- There's no limit to the number of data sources. However, the larger the data source (not only CSV files), the memory requirements increase.

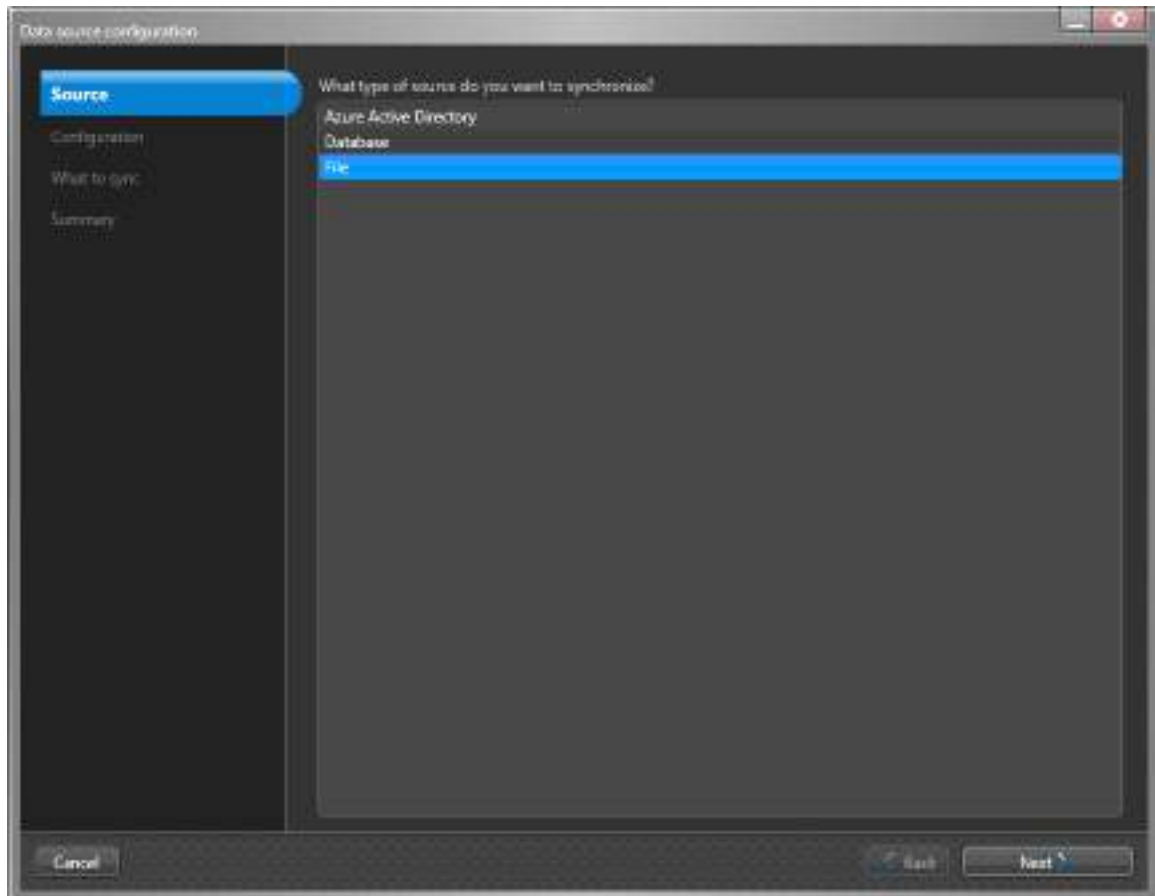
BEST PRACTICE: To avoid user permission issues when using CSV files with the ClearID One Identity Synchronization Tool, save them to a C: or C:\temp folder location. Do not save CSV files in a user-controlled file or folder locations (C:\Users folders or *desktop* folder location) or you might encounter File path is not valid user permissions issues.

Procedure

- 1 In the One Identity Synchronization Tool *Data sources* section, click **Add data source** (+).

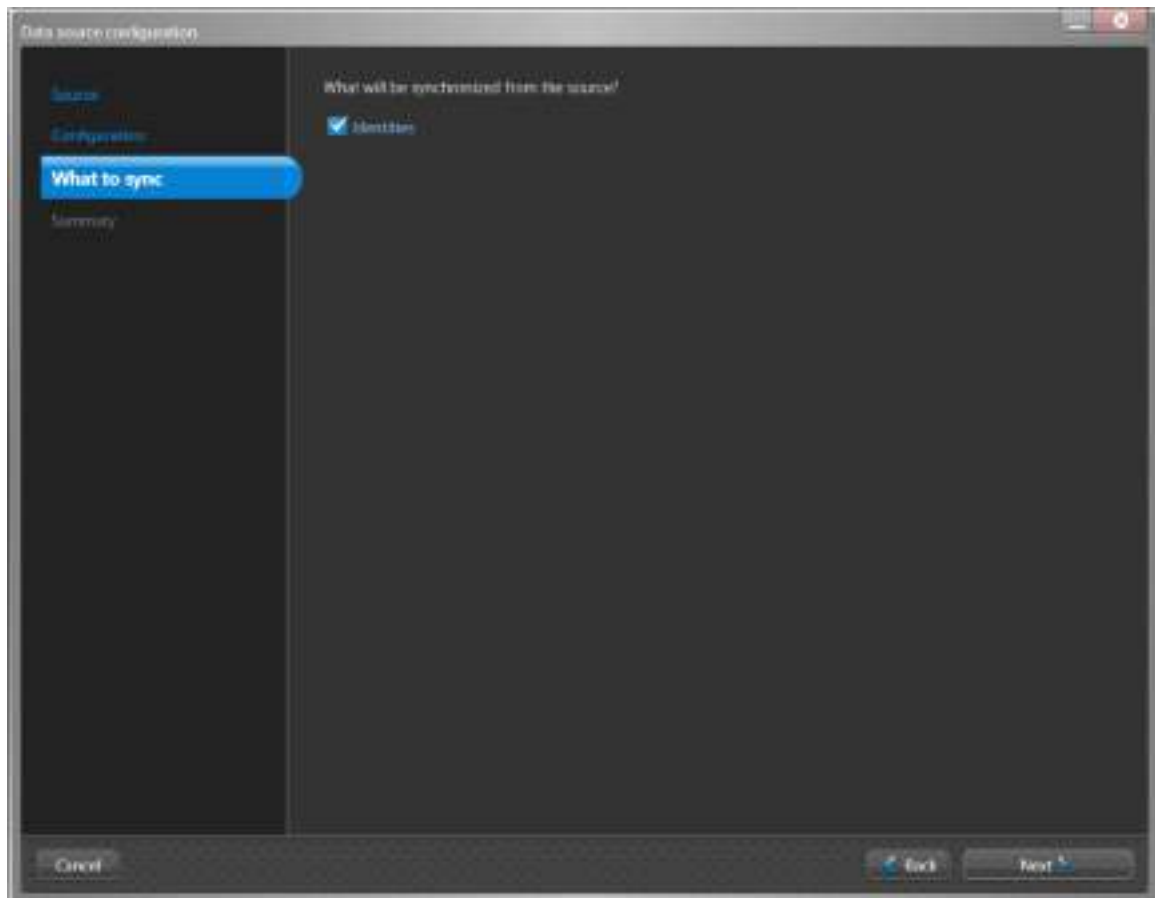


- 2 In the *Source* section of the *Data source configuration* dialog, select **File** and click **Next**.



NOTE: If you selected **File** in the *Source* section, the *Configuration* section of the *Data source configuration* dialog is skipped because it isn't required.

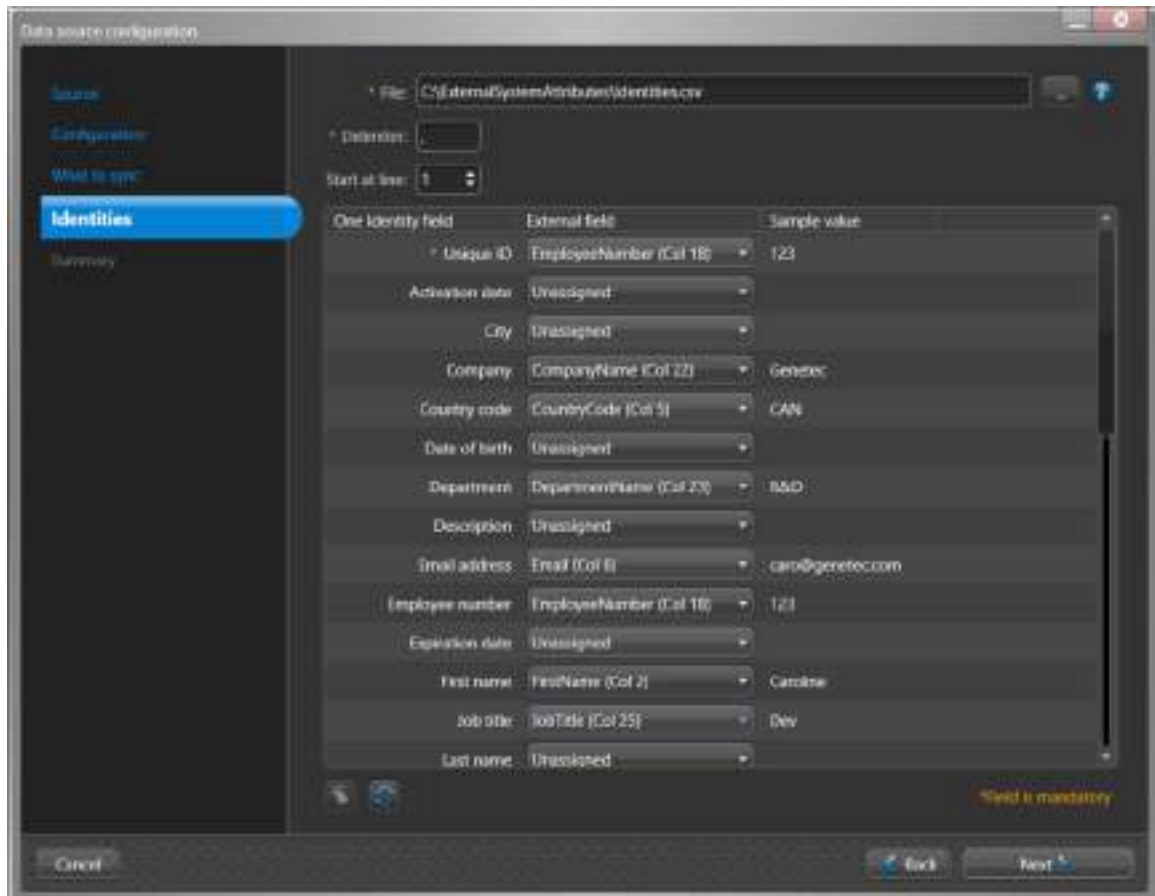
- 3 In the *What to sync* section of the *Data source configuration* dialog, select **Identities** to synchronize from the external system data source.



- 4 If you selected **Identities** as a data source, in the *What to sync* section, configure the identity attributes settings.

NOTE: The fields that are displayed vary depending on the data source selected in the *Source* section (step 2 on page 230) earlier.

The following image shows the options that are displayed after selecting a **File** (CSV) data source.



- a) If you selected **File** as your data source, configure the file settings.

- **File:** Click **More** (📁) to select the CSV file containing your attributes.
NOTE: The file path must exist on the server where the One Identity Configuration Tool is installed.
- **Delimiter:** Enter a **Delimiter value**.
For example, for a CSV file it's a comma-separated value (CSV).
- **Start at line:** Select a **Start at line**.

For example, the data in a table with no headings might start at line 0, whereas the data in a table with headings might start at line 1.

b) Configure your **External field** attribute mappings.

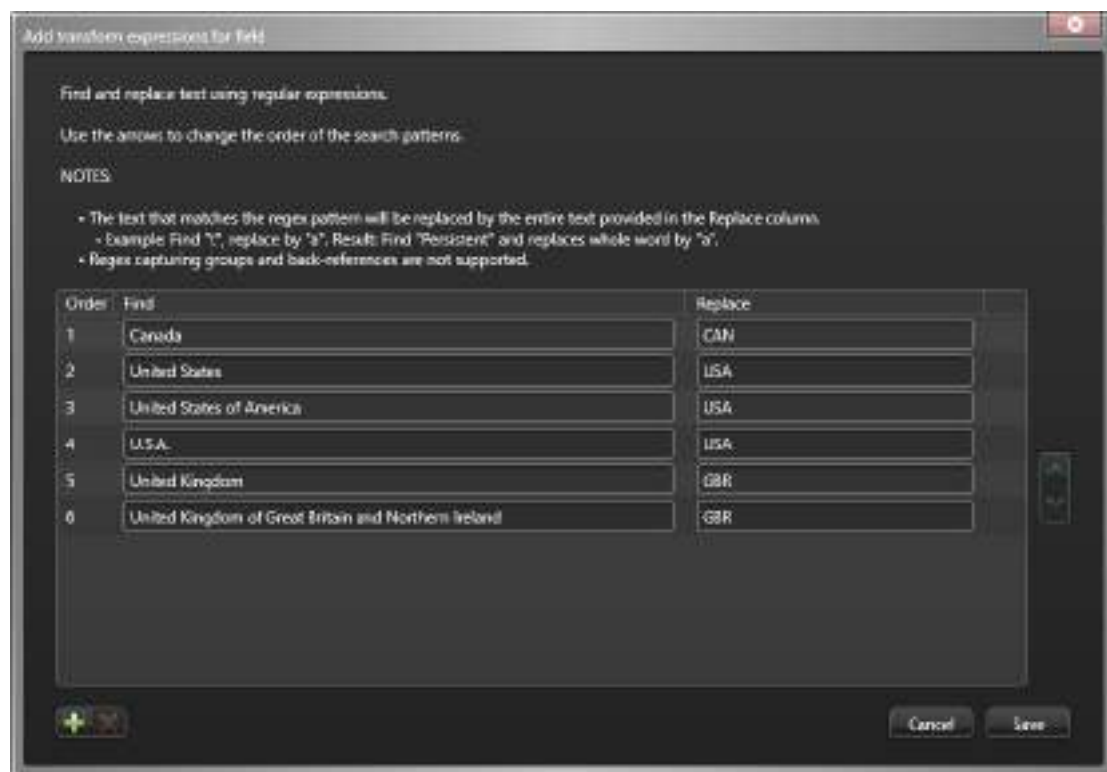
- **One Identity field:** Displays the ClearID identity attributes. Mandatory fields are highlighted using an asterisk (*).

IMPORTANT: The Unique ID is used internally by One Identity as the primary key to identify what it is. For example, an employee number or email address could be used, as long as it is unique.

- **External Field:** Select system attributes in the **External field** columns that you want to map from the external system to the ClearID identity attributes shown in the **One Identity field** column.
- If your CSV file contains column titles, the names are displayed.
- If your CSV file doesn't contain column titles, the column number is displayed.

c) (Optional) Click **Script**  to add a transform expression to find and replace external field text using regular expressions.

For example, you can look for variations of a country name to replace with the correct country code.



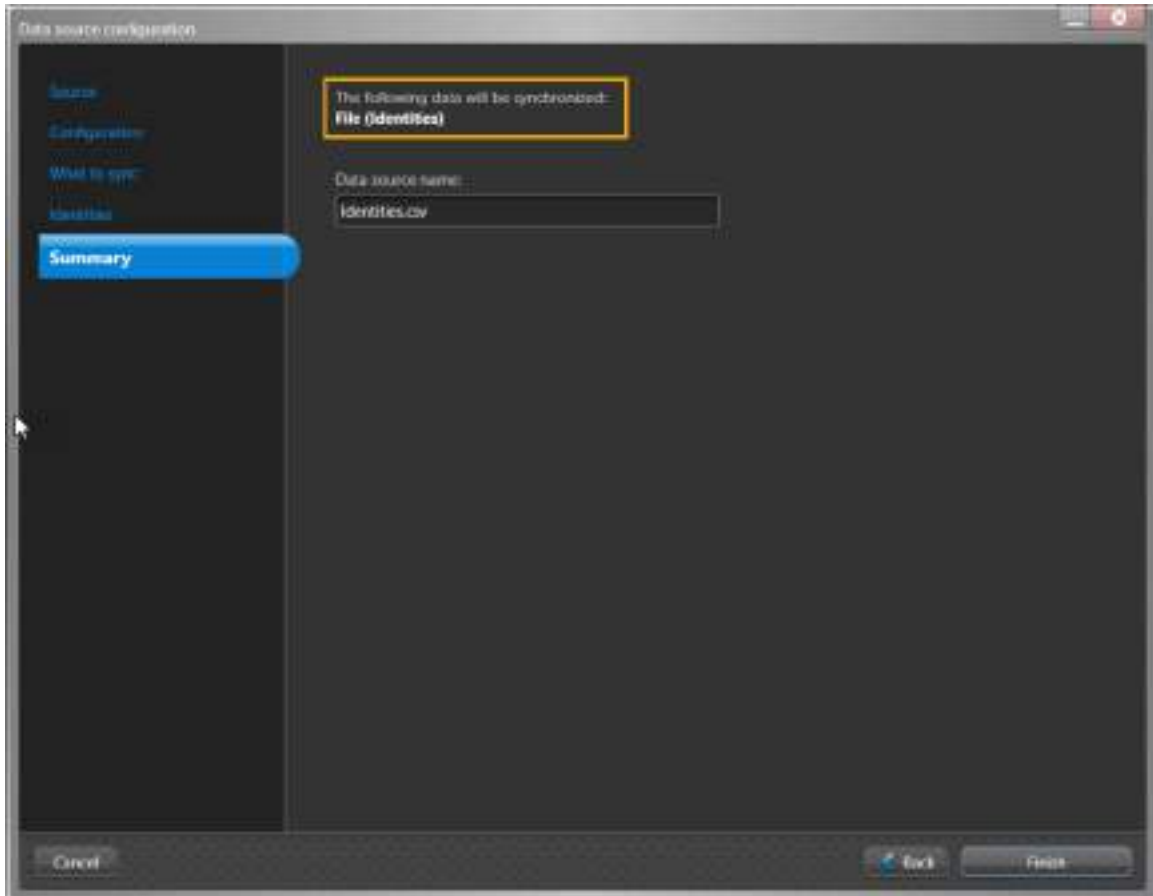
- A script icon  is shown in the **Sample value** column when the field text is being replaced with a regular expression.
- The transform expressions are processed in the order specified in the *Add transform expressions for field* dialog.

TIP: If required, you can select the row of any expressions that you no longer require, and click **delete** .

d) (Optional) Click **Refresh**  to update the external fields data from your data source. This refresh option is used in situations where the existing data has been modified, new data rows have been added, or new attribute columns have been added.

e) Click **Next**.

- 5 In the *Summary* section, review the data that will be synchronized.



NOTE: If multiple data sources are selected, only the first data source file is displayed in the *Summary* section **Data source name** field. If you want each of the data files listed in the **Data sources** section, you must add them individually.

- a) If the data synchronization details look correct, click **Finish**.

After you finish

[Configure your synchronization settings.](#)

Related Topics

[About One Identity Synchronization Tool attribute fields](#) on page 195

Configuring synchronization settings

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool synchronization settings.

Before you begin

IMPORTANT: Make sure that your files aren't being edited and are closed, because the synchronization tool locks the file during the synchronization process.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

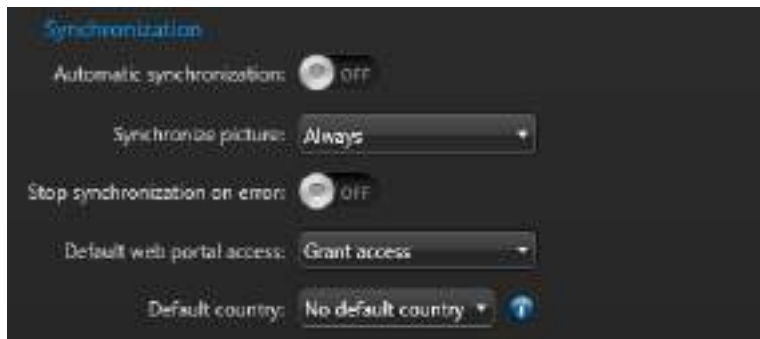
Synchronization can be performed manually using the **Synchronize now** (🔄) option, or automatically at the **Automatic synchronization** intervals specified in the One Identity Synchronization Tool.

Synchronization of external system attributes into ClearID identity attributes is INBOUND only.

CAUTION: Any changes only made to identities in ClearID can be overwritten during the next synchronization from the external system.

Procedure

- 1 In the One Identity Synchronization Tool **Synchronization** section, configure your synchronization settings.



- **Automatic synchronization:** Enable automatic synchronization if you want attributes synchronized at a specified interval.
 - **Interval:** If automatic synchronization is enabled, choose a synchronization interval:
 - **Fixed:** Enter a Synchronization interval using the following format: 000d 01h 00m 00s. For example, every 7 days would be 007d 00h 00m 00s, or every 12hrs 000d 12h 00m 00s.
 - **Cron Schedule:** Enter a synchronization interval using the Quartz Cron format. For example, 00***?*. For more information, see quartz-scheduler.org/documentation.
- TIP:** You can click **Synchronize now** (🔄) regardless of any scheduled settings to initiate an immediate synchronization.
- **Synchronize picture:** Choose when to synchronize identity pictures from the external system.
 - **Always:** Identity pictures are synchronized every time a synchronization occurs.
 - **Only if missing:** Identity pictures are only synchronized when a synchronization occurs, if they are missing.
- NOTE:** Including pictures increases the amount of time that it takes to import attributes.
- **Stop Synchronization on error:** Enable this option to stop synchronization if an error is encountered during the synchronization process.
- **Default web portal access:** Specifies web portal access for synchronized users.
 - **Grant access:** ClearID web portal access for synchronized users is enabled by default.
 NOTE: The **username** field must be mapped to give web portal access to a ClearID identity.
 - There are only two possible values for the **User type** mapping: **Admin** and **User**. Any other value entered defaults to **User**.
 - If the mapping for web portal access isn't set, or the value is empty, the **Default web portal access** global setting is used.
 - **No access:** Web portal access for synchronized users is disabled by default.
- **Default country:** Choose one of the following:

- **No default country:** If a synchronized identity doesn't include a country attribute, the country attribute is ignored.
- **Default country:** Select a default country. If a synchronized identity doesn't include a country attribute, the synchronized identity uses the default country specified here.

2 Click **Save**.

The ClearID One Identity Synchronization Tool is now configured to synchronize attributes from the external system using the **Data sources** and **Synchronization** settings specified in the tool.

After you finish

After the synchronization has occurred, [verify that the new attributes from the external system have been synchronized and contain the correct attributes](#).

Reviewing synchronization status

To check that your identity attributes were synchronized into Genetec ClearID™ correctly, you can review the synchronization status in the Genetec ClearID™ One Identity Synchronization Tool or the ClearID web portal.

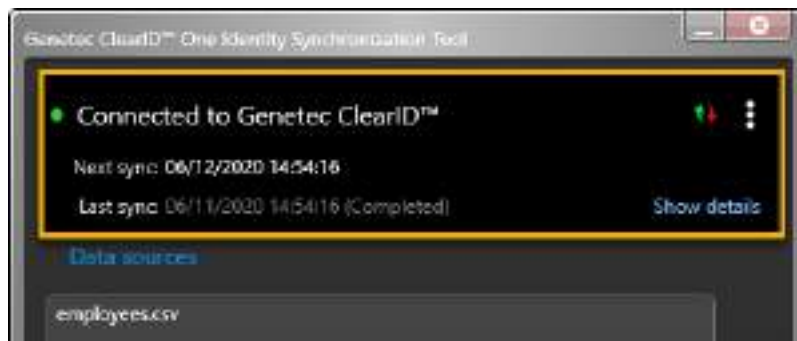
Before you begin

- [Configure the One Identity Synchronization Tool](#).
- Perform a manual or automatic synchronization using the One Identity Synchronization Tool.

Procedure

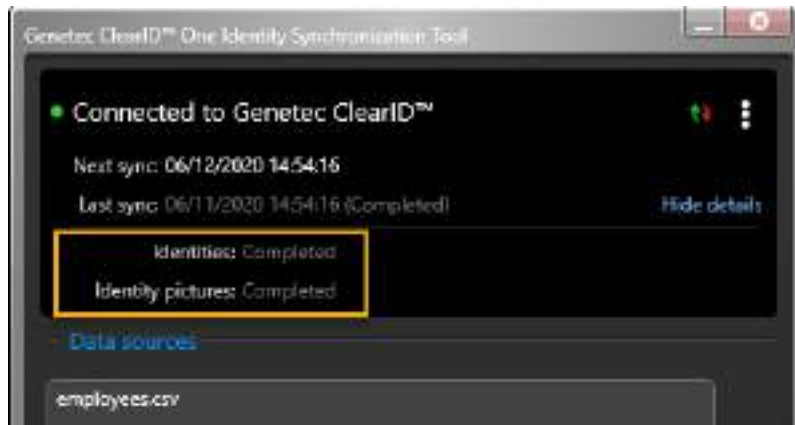
To review your attribute synchronization status in the One Identity Configuration Tool:

- 1 In the One Identity Synchronization Tool connection section, check your synchronization status.



- **Next sync:** Displays information about the next synchronization.

- If a date is displayed **06/16/2020 23:00:00**, this date indicates the **Fixed** or **Cron schedule** interval when the next synchronization is scheduled to occur.
- If **Manual synchronization** is displayed, the synchronization must be performed manually.
- **Last sync:** Displays information about the last synchronization.
- **Show details:** Click **Show details**, to check the status of synchronization for **Identities** and **Identity pictures**.



NOTE: If there's an issue with any of the synchronizations, a **Failed** message is displayed next to the failing synchronization.

- 2 (Optional) Review summary logs.
 - a) Click  then click **Open logs folder**.
 - b) Review CSV-formatted *Summary* logs to identify any issues that might occur during synchronization.
 - c) Read the overview *Recap.txt* file for a quick synchronization overview.

NOTE: The summary log files are saved in `C:\ProgramData\Genetec\OneIdentity\Logs\Summary`.

To review your attributes synchronization status in the ClearID web portal:

- 1 In the ClearID web portal, check to verify that the new attributes from the external system have been synchronized and contain the correct attributes.
 - a) Click **Organization > Identities** and verify that your synchronized identity data is correct.

About One Identity Synchronization Tool logs

The Genetec ClearID™ One Identity Synchronization Tool includes logs that can be used for troubleshooting. The logs can be used to check the status of the configuration tool, the windows service, or review synchronization activities.

The ClearID One Identity Synchronization Tool uses the industry-standard Apache log4net™ framework for logging.

The logging configuration can be changed for both the synchronization service and the synchronization tool.

- To change the **Genetec.ClearID.OneIdentity.SynchronizationService** (*OneIdentityService.exe*) logging configuration, you can modify the *log4net.service.config* file.
- To change the **Genetec.ClearID.OneIdentity.SynchronizationTool** (*OneIdentityConfigurationTool.exe*) logging configuration, you can modify the *log4net.ct.config* file.

These log configuration files are found in the installation folder `C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service`.

The default settings are as follows:

- Log level is **WARN**.

- File size before rolling is 10Mb.
- Max rolling backups is 10.

For more information about the supported values and how to change them, see the [Apache log4net](#) documentation.

Viewing One Identity Synchronization Tool logs

You can use the Genetec ClearID™ One Identity Synchronization Tool logs to check the status of the configuration tool, the windows service, or review synchronization activities.

Before you begin

- [Configuring the One Identity Synchronization Tool](#) on page 208
- [Configuring synchronization settings](#) on page 234

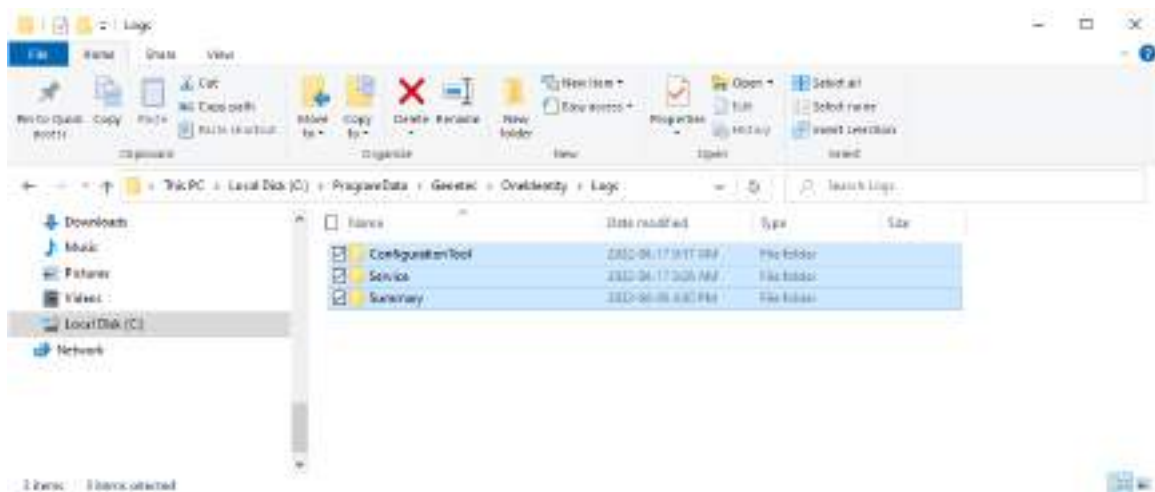
What you should know

Logs are subdivided into three separate folders as follows:

- **Configuration:** Logs related to the *Genetec ClearID One Identity Synchronization Tool (OneIdentityConfigurationTool.exe)*.
- **Service:** Logs related to the *Genetec.ClearID.OneIdentity.SynchronizationService (OneIdentityService.exe)*.
- **Summary:** Logs related to synchronization summaries.

Procedure

- 1 Click  then click **Open logs folder**.



- 2 Review the *ConfigurationTool* logs if you're having connectivity issues. For example, if the synchronization tool is unable to connect to Genetec ClearID™ or unable to connect to Azure AD (Microsoft Entra ID).
- 3 Review the *Service* logs if you're having data synchronization issues. For example, missing data fields, missing name fields, or missing email addresses.

- 4 Review the *Summary* logs to see a summary of synchronization activities. For example, when a synchronization started or ended and what occurred during the synchronization.
 - a) Read the *Recap.txt* file for a quick synchronization overview.

NOTE: The summary log files are CSV-formatted files to facilitate sorting information in Microsoft Excel if required. They are automatically generated at the end of the synchronization.

- If the synchronization completely fails, the summary log files aren't generated.
- If there's nothing to import, the summary log files aren't created.

Updating existing identities from an external data source

When users that have already been created have the same external ID as existing users, you can use Genetec ClearID™ One Identity Synchronization Tool to update the existing identities information from an external data source.

What you should know

This procedure is relevant for newly installed ClearID One Identity Synchronization Tool service when the Genetec ClearID™ environment already contains identities that are also present in the external system data source.

- When an external ID already exists in ClearID, that identity is updated with the values provided in the data sources.
- When an identity from the data source doesn't exist in One Identity (for example, on the first synchronization), the service tries to create the identity in ClearID.
- When the creation fails because the identity already exists, that identity is then fetched and updated.

Procedure

- 1 To reproduce a newly installed service, delete the file mappings under *%ProgramData%\Genetec\OneIdentity\Configuration*.
- 2 Configure a data source that already contains one or more identities that are present in ClearID.
The identities in the data source should have the same external ID and email as the identities in ClearID.
- 3 Start the synchronization and wait for completion.

The identities in ClearID are updated with the mappings from the data source.

Self-Service Kiosk

About ClearID Self-Service Kiosk

Genetec ClearID™ Self-Service Kiosk is a mobile app that simplifies the management of visitors enrolled using the Genetec ClearID™ self-service portal. The self-service kiosk is intended for visitor centers or gated facilities where guests check-in by themselves.



Visitors can check in at the ClearID Self-Service Kiosk using several methods:

- Find a visitor associated with a visit by scanning their invitation QR code.
- Find a visitor associated with a visit by scanning their drivers license.
- Find a visitor associated with a visit by scanning their passport or citizen card (MRZ data).
- Find a visitor associated with a visit by scanning their Identity Document (various ID types from more than 200 countries).
- Find a visitor associated with a visit by their email.

NOTE: After visitors are checked-in from the ClearID Self-Service Kiosk, the host is notified using email and SMS message (if enabled).

With the ClearID Self-Service Kiosk, you can also do the following:

- Screen visitors during a self-service check-in or a self-registration.
- Take a photo of the visitor¹.
- Print a visitor badge using a wireless label printer (Bluetooth or Wi-Fi). The badge includes a photo and identifies the visitor and the event they are attending.
- Visitor self-registration.
- Company logos on the ClearID Self-Service Kiosk and visitor badges.
- Customer-specific welcome and assistance messages on the ClearID Self-Service Kiosk.

NOTE: ¹This photo is only used on the printed badge. The photo isn't saved or stored for later use to ensure that visitor information is protected.

Visitor badges

The following examples show visitor badges in *portrait* and *landscape* orientation.



Badge dimensions: **10 x 6.1 cm's** or **3.94 x 2.56 inches**.

To download the Genetec ClearID™ Self-Service Kiosk mobile app, visit the [App Store](#).

Related Topics

[Supported devices](#) on page 12

[Identity document types](#) on page 293

[ClearID Self-Service Kiosk Datasheet \(2 pages\)](#)

Self-Service Kiosk check-in

Use this information to help you understand how visitors check in at a Genetec ClearID™ Self-Service Kiosk.

Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



NOTE: Visitors can check in up to 1 hour before a visit event.

Scenario 1: Kiosk check-in (paper badge)

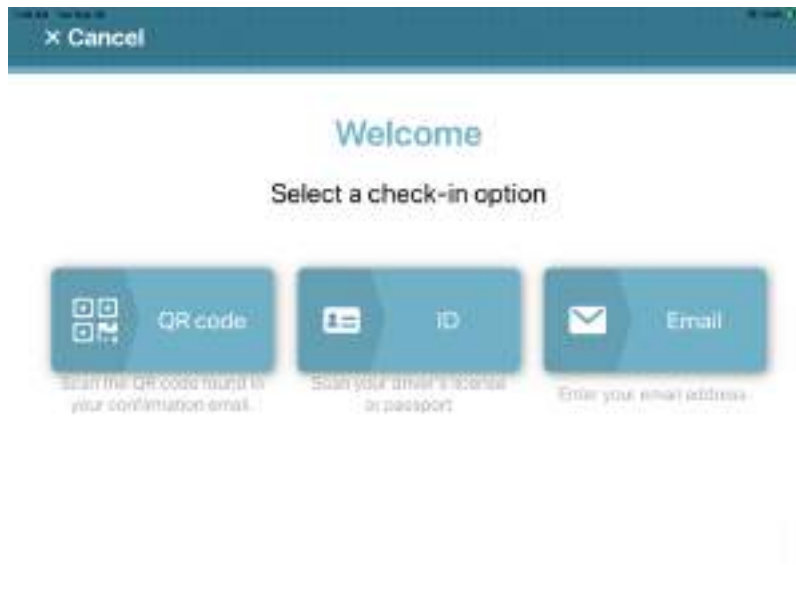
Visitors can easily check in at a ClearID Self-Service Kiosk. Using their emailed QR code, visitors scan the code, take a picture, and print a visitor badge that identifies the visitor and the event they are attending.

Scenario 2: Kiosk check-in (cardholder credential)

Using Security Center SaaS, a receptionist can assign a credential to Genetec ClearID™ visitors. The visitor can then use their card to access specified areas in the building when accompanied by their host.

Self-service check-in

The self-service check-in is intended for visitors who have been invited or pre-registered.



You can use the ClearID Self-Service Kiosk to check in yourself using QR code, ID, or email up to 1 hour before a visit event:

- If duplicate names are found, you can select your unique email from the list.
- If you scan a QR code that isn't found, the Self-Service Kiosk switches to looking for visitor by email.
- If an ID or email isn't found the Self-Service Kiosk switches to the self-registration process.

NOTE: The check-in choices displayed on the Kiosk **Welcome** page can be customized to hide options that aren't relevant to your site or your visitor experience.

For more information, see the **Kiosks** tab section in [Enabling visitor management for sites](#) on page 50.

Related Topics

[Enabling visitor management for sites](#) on page 50

Self-Service Kiosk self-registration

The Genetec ClearID™ Self-Service Kiosk self-registration process is designed to manage unplanned visits or visitors who haven't been invited or pre-registered.

If enabled for your account, the self-registration workflow is triggered during the self-service check-in process when a visitor arrives on site without an invite and they aren't found in the system.

NOTE: Any pre-filled entries can't be modified.

The self-registration process is linked to a site. Visitors are accepted automatically with default entry-level visitor access to the site. For example, Front door, reception, or check-in area to ensure a smooth check-in experience.

IMPORTANT: Any visitors on a block list will be denied access if the *watchlist* function is enabled for your account, and the *watchlist manager* is notified. In this situation, the visitor should talk to security or reception staff.

Configuring the Self-Service Kiosk iPad

Before visitors can use the self-service kiosk to check in or check out, you must add the Genetec ClearID™ Self-Service Kiosk iPad device to Genetec ClearID™. Then you can register and activate the device in the ClearID Self-Service Kiosk mobile app.

Before you begin

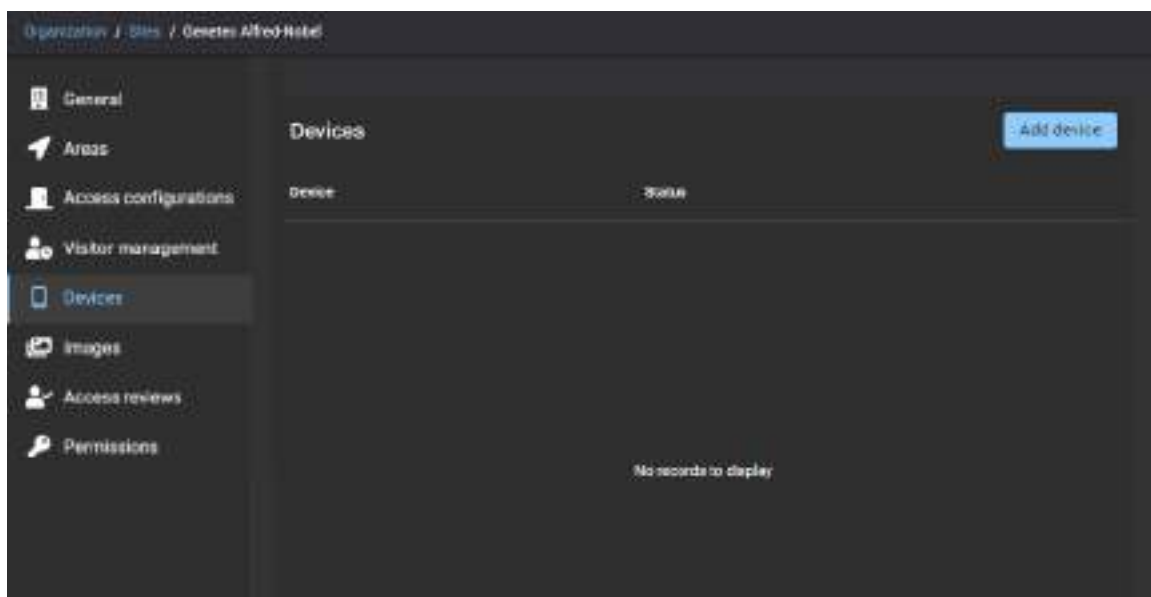
- Wi-Fi must be enabled on the self-service kiosk device before activating the device.

What you should know

- Only a site administrator can generate a device activation code in ClearID.
- You can only activate and associate a ClearID Self-Service Kiosk with one site at a time.
- The ClearID Self-Service Kiosk iPad must be on the same Wi-Fi network as the label printer.

Procedure

- 1 In ClearID, click **Organization** and select your site.
- 2 On the *site* page, click **Devices**.



- a) Click **Add device** to define your ClearID Self-Service Kiosk in ClearID.
- b) In the *Add device* dialog, enter a name and click **Add**.

TIP: Consider including the associated site or area in the name to help you easily identify your kiosk in the future.

3 Activate your kiosk in ClearID:

- a) In the devices list, find your kiosk and then in the **Status** field, click **Generate activation code**.



- b) Make a note of the activation code for later use.

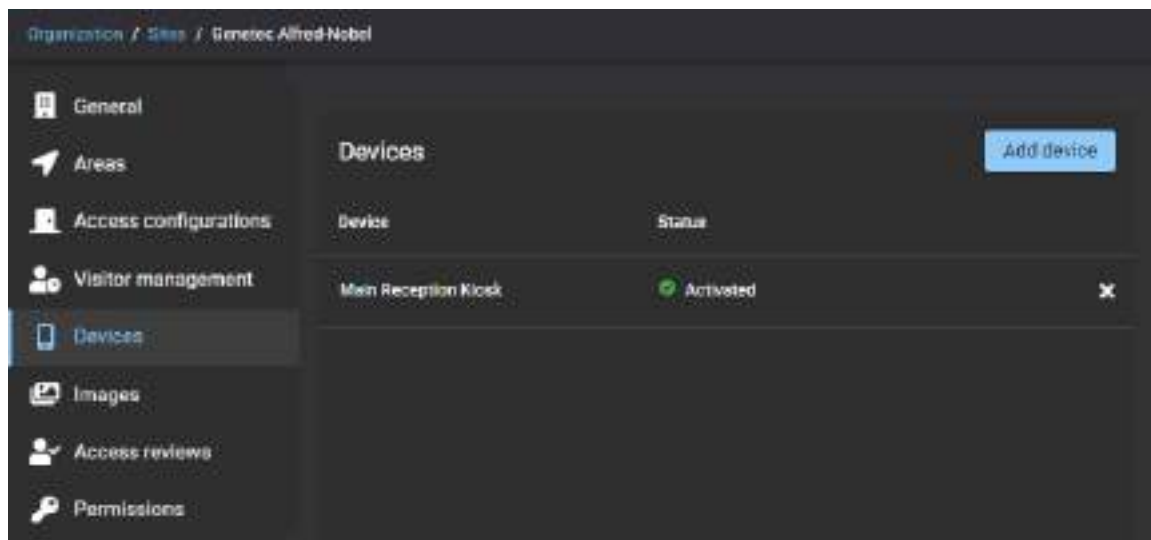
- c) (Optional) Copy to clipboard.

TIP: Use **Copy to clipboard** when the person who registers the ClearID Self-Service Kiosk device in the ClearID portal is different to the person who activates the self-service kiosk. Once the code is in the clipboard, it can be emailed to the person who activates the kiosk.

- d) Click **OK**.

4 In the ClearID Self-Service Kiosk mobile app, enter your device activation code and tap **Register**.

Your self-service kiosk is now activated in ClearID and ready for use.



Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



After you finish

- [Configure your kiosk label printer](#)
- (Optional) [Customize your banner image for email notifications](#)
- (Optional) [Customize your Self-Service Kiosk configuration](#)
- (Optional) [Customize your Self-Service Kiosk badge logo](#)

Related Topics

[Supported devices](#) on page 12

[Firewall ports](#) on page 11

Customizing the Self-Service Kiosk configuration

Configure your site images and kiosk options to customize the choices that are displayed to visitors using your Genetec ClearID™ Self-Service Kiosk during the check-in or check-out process. Customization can include company logos, kiosk themes, and customer-specific welcome and assistance messages.

Before you begin

[Configuring the Self-Service Kiosk iPad](#) on page 245

TIP: Ensure that your welcome screen images meet the requirements described in the  tooltip on the **Visitor management > Kiosks** page of the Genetec ClearID™ web portal.

What you should know

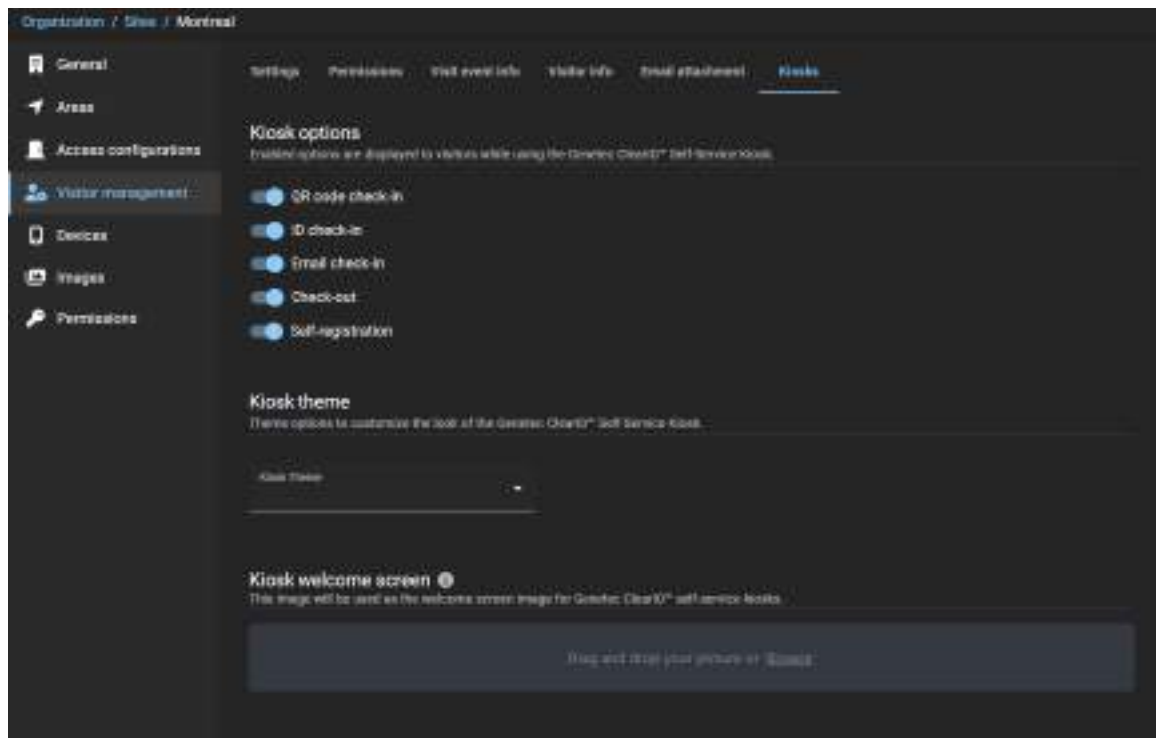
Only a site owner or account administrator can customize the kiosk configuration options.

- Customized kiosk options changes are synchronized with your kiosk every 60 seconds.

BEST PRACTICE: For optimum results, use transparent .PNG images when customizing your welcome screen image.

Procedure

- 1 In the ClearID web portal, click **Organization > Sites**.
- 2 Search for and select a site.
- 3 Click **Visitor management > Kiosks**.



- 4 In the *Kiosk* tab, customize your kiosk configuration options as required:
 - a) (Optional) In the *Kiosk options* section, select the kiosk options that you want displayed to your visitors while using the kiosk.
 - b) (Optional) In the *Kiosk theme* section, choose a theme to customize the look of the kiosk.
For example, select the **White** theme and choose an **Accent color** that aligns with your corporate branding.
 - c) (Optional) In the *Kiosk welcome screen* section, upload an image to use as the welcome screen logo.
For example, a *company name* or *logo* that aligns with your corporate branding.
For more detailed information and to see examples of these kiosk customizations, see [Enabling visitor management for sites](#) on page 50.
- 5 Click **Save**.

Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



Customizing the Self-Service Kiosk visitor badge logo

You can customize the visitor badge logo image that is used on temporary badges or visitor badges printed by the kiosk.

Before you begin

[Configuring the Self-Service Kiosk iPad](#) on page 245

TIP: Ensure that your badge logo images meet the requirements described in the  tooltip on the **Images** page of the Genetec ClearID™ web portal.

What you should know

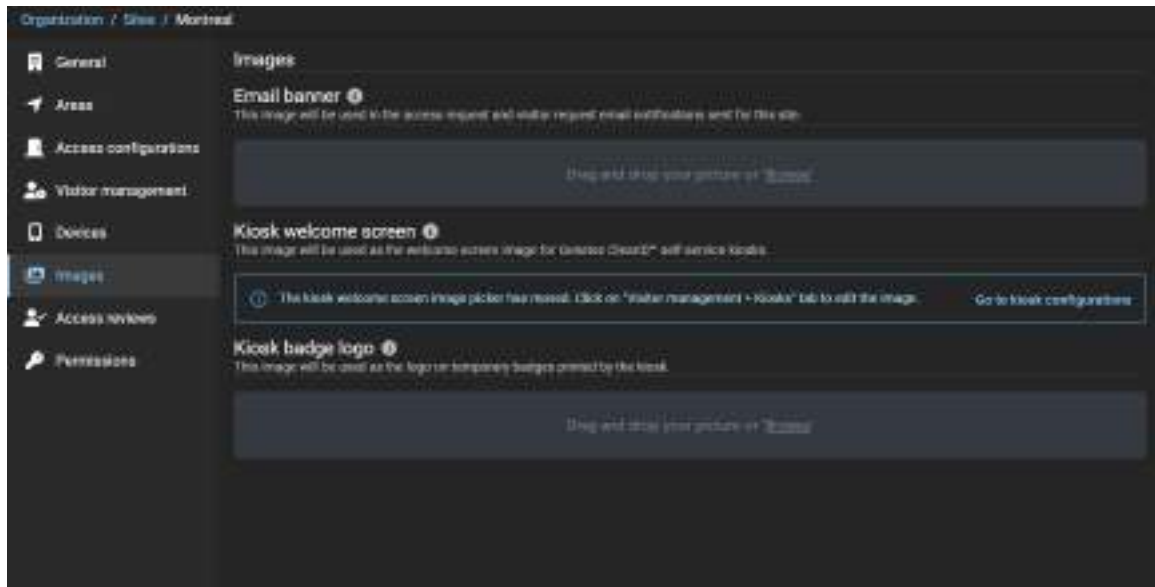
Only a site owner or account administrator can customize the visitor badge logo.

- Customized Kiosk options changes are synchronized with your kiosk every 60 seconds.

BEST PRACTICE: For optimum results, use transparent *.PNG* images when customizing your visitor badge logo.

Procedure

- 1 In the ClearID web portal, click **Organization > Sites**.
- 2 Search for and select a site.

3 Click **Images**.

- In the *Kiosk badge logo* section, drag and drop your picture or browse to select a **Kiosk badge logo**. This image is used as the logo on temporary badges printed by the kiosk.
- Click **Save**. The following example shows a custom badge logo for the kiosk.



Configuring the Self-Service Kiosk label printer (Brother QL-820NWBc, QL-820NWB, or QL-810W)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother QL-810W/820NWB Quick Setup Guide \(English\)](#)
- [Brother QL-810W/QL-820NWB User Guide \(English\)](#)
- [Brother QL-820NWB LED Status indicators](#)

NOTE: The Brother QL-820NWBc replaced the Brother QL-820NWB printer (discontinued). For more information about the differences, see [Brother QL-820NWBc Specifications changes](#).

What you should know

BEST PRACTICE: Use only one label printer per kiosk and pair the printer with the kiosk using Bluetooth.

If you require one label printer for many kiosk devices, or the label printer is far away from the kiosk devices use Wi-Fi or Ethernet. For example, two kiosks by the entrance and one label printer on the reception desk.

NOTE: A rechargeable Li-ion battery unit (power supply) can also be purchased and used in situations where mains power is unavailable.

Procedure

- Choose one of the following:
 - [Configuring Bluetooth mode \(Brother QL-820NWBc or QL-820NWB\)](#)
 - [Configuring Wi-Fi mode \(Brother QL-820NWBc, QL-820NWB, or QL-810W\)](#)
 - [Configuring Ethernet mode \(Brother QL-820NWBc or QL-820NWB\)](#)

After you finish

From time to time you might need to order supplies, replace the coin cell battery, recharge the optional battery unit (if used), or clean the label printer.

For more information, see *Brother QL-810W/QL-820NWB Quick Setup Guide* and *Brother QL810W/QL-820NWB User Guide*.

Related Topics

[Brother QL-820NWB Label Printer FAQs](#)

[Brother QL-820NWB printer supplies](#)

[Supported devices](#) on page 12

[Self-Service Kiosk options](#) on page 282

Configuring the Self-Service Kiosk label printer for Bluetooth mode (Brother QL-820NWBc or QL-820NWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother QL-810W/820NWB Quick Setup Guide \(English\)](#)
- [Brother QL-810W/QL-820NWB User Guide \(English\)](#)
- [Brother QL-820NWB LED Status indicators](#)

NOTE: The Brother QL-820NWBc replaced the Brother QL-820NWB printer (discontinued). For more information about the differences, see [Brother QL-820NWBc Specifications changes](#).

What you should know

When using the Brother QL-820NWBc or QL-820NWB label printer in Bluetooth printing mode, the following applies:

- One label printer can be paired with only one kiosk.
- The label printer must be within 30ft of the kiosk.

NOTE: A rechargeable Li-ion battery unit (power supply) can also be purchased and used in situations where mains power is unavailable.

Procedure

- 1 Plug printer AC adapter into a power outlet and connect the power lead to the label printer.



Figure 6: Brother QL-820NWBc label printer (rear)

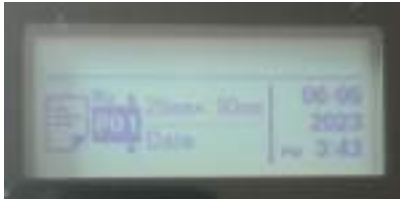


Figure 7: Brother QL-820NWB label printer (rear)

- 2 Press the **Power** button to turn the label printer on.



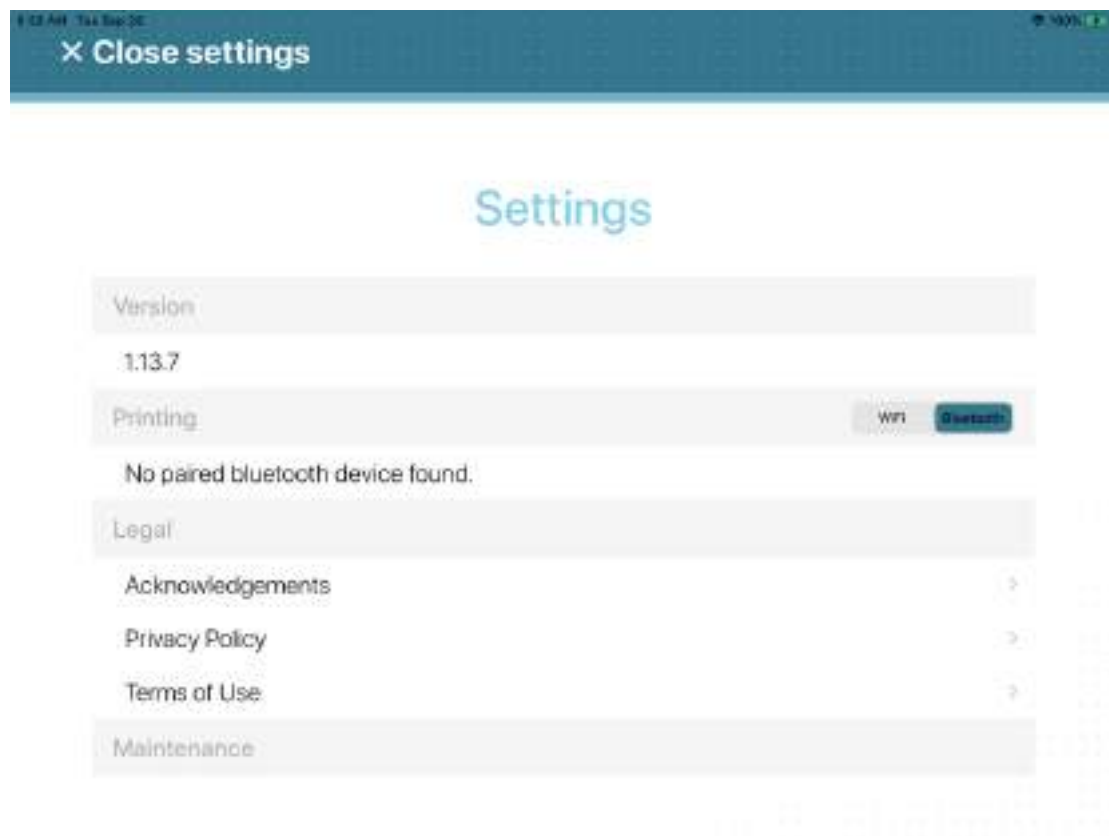
- 3 (Optional) If you see **Template Mode** menu and the incorrect label size displayed, disable it.



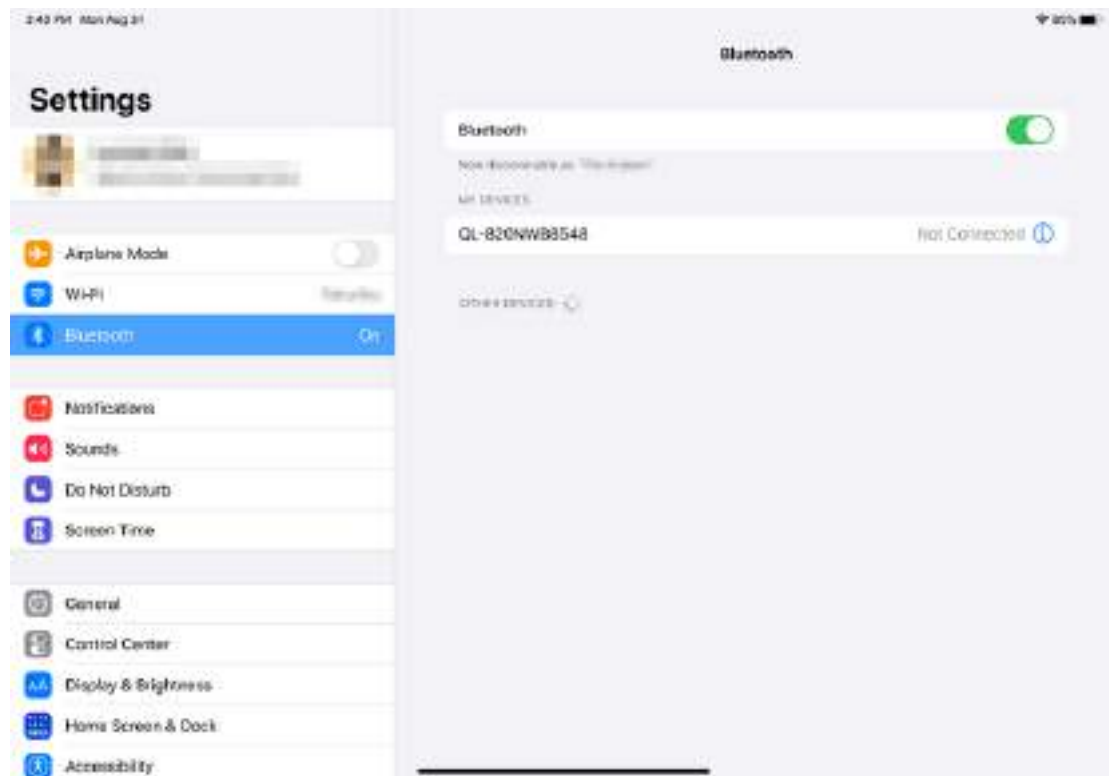
- a) Press **Menu**, navigate to **Template Settings** and turn off the **Template Mode** setting.
- 4 Use the arrow buttons to navigate the label printer menu.



- a) Select **Bluetooth** > **Bluetooth (On/Off)** > **On** in the settings menu and press **OK**.
- b) Select **Bluetooth** > **Automatic Reconnection (On/Off)** > **On** in the settings menu and press **OK**.
- 5 Pair your Bluetooth label printer with your ClearID Self-Service Kiosk iPad.
- a) In the Self-Service Kiosk mobile app, tap **Settings** (⚙️).
- b) In the *Printing* section, tap the slider control to select **Bluetooth**.

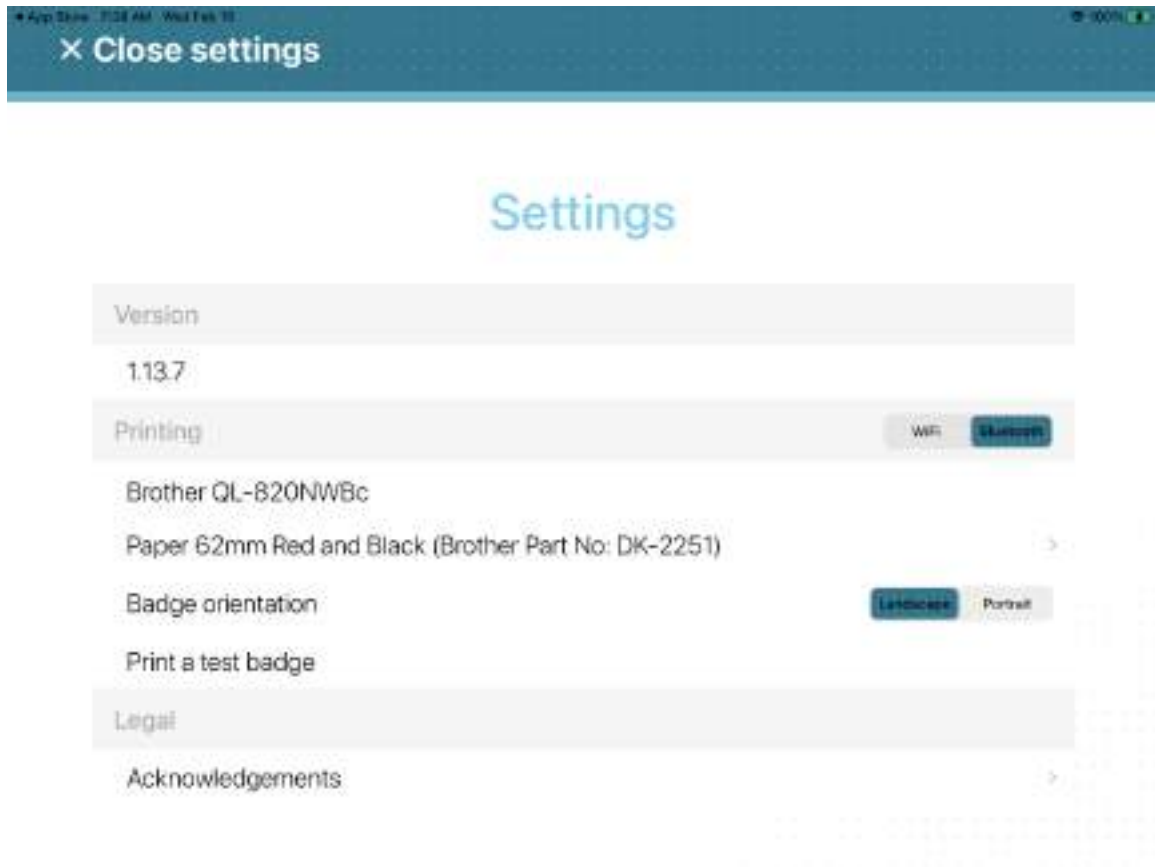


- 6 On your iPad, navigate to the Apple **Settings** icon, tap **Settings** > **Bluetooth**.
- a) (Optional) If **Bluetooth** is disabled, tap the slider to enable Bluetooth.



- b) Click the correct printer to pair the ClearID Self-Service Kiosk iPad with your printer.

- 7 In the Self-Service Kiosk mobile app, tap **Settings** (⚙️).



- a) In the *Printing* section, check that your Brother QL-820NWBc or QL-820NWB printer is displayed.

TIP: If the printer is not displayed or bluetooth is not selected, tap **WiFi** then tap **Bluetooth** to trigger discovery again.

After you finish

(Optional) [Print a test badge](#).

Related Topics

[Firewall ports](#) on page 11

Configuring the Self-Service Kiosk label printer for Wi-Fi mode (Brother QL-820NWBc, QL-820NWB, or QL-810W)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother QL-810W/820NWB Quick Setup Guide \(English\)](#)
- [Brother QL-810W/QL-820NWB User Guide \(English\)](#)
- [Brother QL-820NWB LED Status indicators](#)

NOTE: The Brother QL-820NWBc replaced the Brother QL-820NWB printer (discontinued). For more information about the differences, see [Brother QL-820NWBc Specifications changes](#).

What you should know

- One label printer can support up to five self-service kiosks
- The label printer must be on the same Wi-Fi network as the ClearID Self-Service Kiosk iPad.

The Wi-Fi network must be enabled for use and support the following:

- Bonjour - required for device search.
- SNMP - required to check printer status information.
- UDP or TCP Port 9100 - required to send print data.

NOTE: A rechargeable Li-ion battery unit (power supply) can also be purchased and used in situations where mains power is unavailable.

Procedure

- 1 Plug printer AC adapter into a power outlet and connect the power lead to the label printer.



Figure 8: Brother QL-820NWBc label printer (rear)

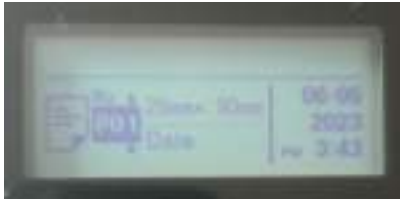


Figure 9: Brother QL-820NWB label printer (rear)

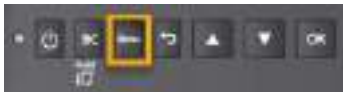
- 2 Press the **Power** button to turn the label printer on.



- 3 (Optional) If you see **Template Mode** menu and the incorrect label size displayed, disable it.



- a) Press **Menu**, navigate to **Template Settings** and turn off the **Template Mode** setting.
- 4 Press the **Menu** button.



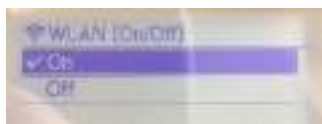
- 5 Use the arrow buttons to navigate the label printer menu.



- 6 Scroll down to the **WLAN (5/7)** settings and press **OK**.



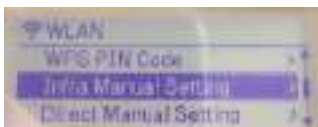
- a) Select **WLAN On** and press **OK**.



- b) In the *Network Mode* menu items, select **Infrastructure Mode** and press **OK**.



- 7 Scroll down to **Infra Manual Setting** and press **OK**.



- a) After the search completes, scroll down and select your Wi-Fi network from the Service Set Identifier (SSID) list and press **OK**.



NOTE: Typically this network is a Wi-Fi network with AirPrint enabled.

- b) When prompted enter the Wi-Fi password.

- 8 Navigate to **WLAN Status** and press **OK** to verify your Wi-Fi network status and IP address.



TIP: Make a note of the **SSID** (Wi-Fi network) and **IP Addr** (Label Printer IP) for later use.

- The SSID is used to verify that you are on the same Wi-Fi network as the ClearID Self-Service Kiosk iPad.
- The IP address is used later when selecting a label printer to verify you have the correct printer.

- 9 [Select your Wi-Fi label printer.](#)

After you finish

(Optional) [Print a test badge.](#)

Related Topics

[Firewall ports](#) on page 11

Configuring the Self-Service Kiosk label printer for Ethernet mode (Brother QL-820NWBc or QL-820NWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother QL-810W/820NWB Quick Setup Guide \(English\)](#)
- [Brother QL-810W/QL-820NWB User Guide \(English\)](#)
- [Brother QL-820NWB LED Status indicators](#)

NOTE: The Brother QL-820NWBc replaced the Brother QL-820NWB printer (discontinued). For more information about the differences, see [Brother QL-820NWBc Specifications changes](#).

What you should know

- One label printer can support up to five self-service kiosks

NOTE: A rechargeable Li-ion battery unit (power supply) can also be purchased and used in situations where mains power is unavailable.

Procedure

- 1 Plug printer AC adapter into a power outlet and connect the power lead to the label printer.



Figure 10: Brother QL-820NWBc label printer (rear)



Figure 11: Brother QL-820NWB label printer (rear)

- 2 Make sure that the printer is turned **OFF** before connecting the LAN cable.



Figure 12: Brother QL-820NWBc label printer (rear)



Figure 13: Brother QL-820NWB label printer (rear)

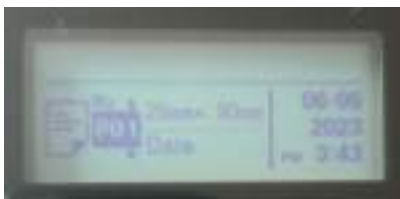
- a) Connect a LAN cable to the LAN port on the back of the printer.

TIP: Use a straight-through Category 5 (or greater) twisted-pair cable for 10BASE-T or 100BASE-TX Fast Ethernet Network.

- 3 Press the **Power** button to turn the label printer on.



- 4 (Optional) If you see **Template Mode** menu and the incorrect label size displayed, disable it.



- a) Press **Menu**, navigate to **Template Settings** and turn off the **Template Mode** setting.

- 5 [Select your Ethernet label printer.](#)

After you finish

(Optional) [Print a test badge.](#)

Related Topics

[Firewall ports](#) on page 11

Configuring the Self-Service Kiosk label printer (Brother TD-4550DNWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the Brother TD-4550DNWB label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother TD-4550DNWB Quick Setup Guide](#)
- [Brother TD-4550DNWB User Guide](#)
- [Brother TD-4550DNWB online User Guide \(HTML\)](#)
- [Brother TD-4550DNWB LED status indicators](#)

What you should know

BEST PRACTICE: Use only one label printer per kiosk and pair the printer with the kiosk using Bluetooth.

If you require one label printer for many kiosk devices, or the label printer is far away from the kiosk devices use Wi-Fi or Ethernet. For example, two kiosks by the entrance and one label printer on the reception desk.

Procedure

- Choose one of the following:
 - [Configuring Bluetooth mode \(Brother TD-4550DNWB\)](#)
 - [Configuring Wi-Fi mode \(Brother TD-4550DNWB\)](#)
 - [Configuring Ethernet mode \(Brother TD-4550DNWB\)](#)

After you finish

From time to time you might need to order supplies, replace the coin cell battery, or clean the label printer.

For more information, see *Brother TD-4550DNWB Quick Setup Guide* and *Brother TD-4550DNWB User Guide*.

Related Topics

[Brother TD-4550DNWB Label Printer FAQs](#)

[Brother TD-4550DNWB printer supplies](#)

[Supported devices](#) on page 12

Configuring the Self-Service Kiosk label printer for Bluetooth mode (Brother TD-4550DNWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother TD-4550DNWB Quick Setup Guide](#)
- [Brother TD-4550DNWB User Guide](#)
- [Brother TD-4550DNWB online User Guide \(HTML\)](#)
- [Brother TD-4550DNWB LED status indicators](#)

What you should know

When using the Brother TD-4550DNWB label printer in Bluetooth printing mode, the following applies:

- One label printer can be paired with only one kiosk.
- The label printer must be within 30ft of the kiosk.

Procedure

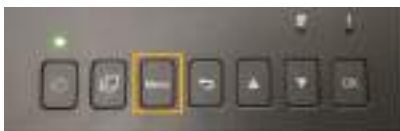
- 1 Plug printer AC adapter into a power outlet and connect the power lead to the label printer.



- 2 Press the **Power** button to turn the label printer on.



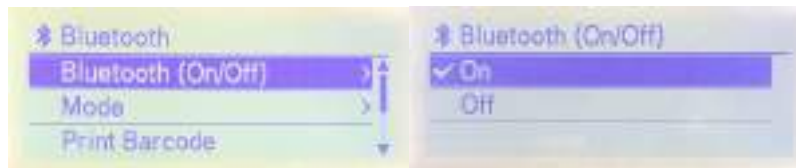
- 3 Press the **Menu** button.



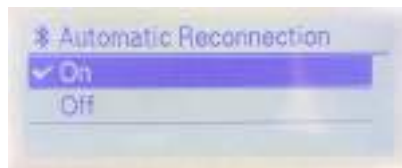
- 4 Use the arrow buttons to navigate the label printer menu.



- a) Select **BLUETOOTH** > **BLUETOOTH (On/Off)** > **On** in the settings menu and press **OK**.

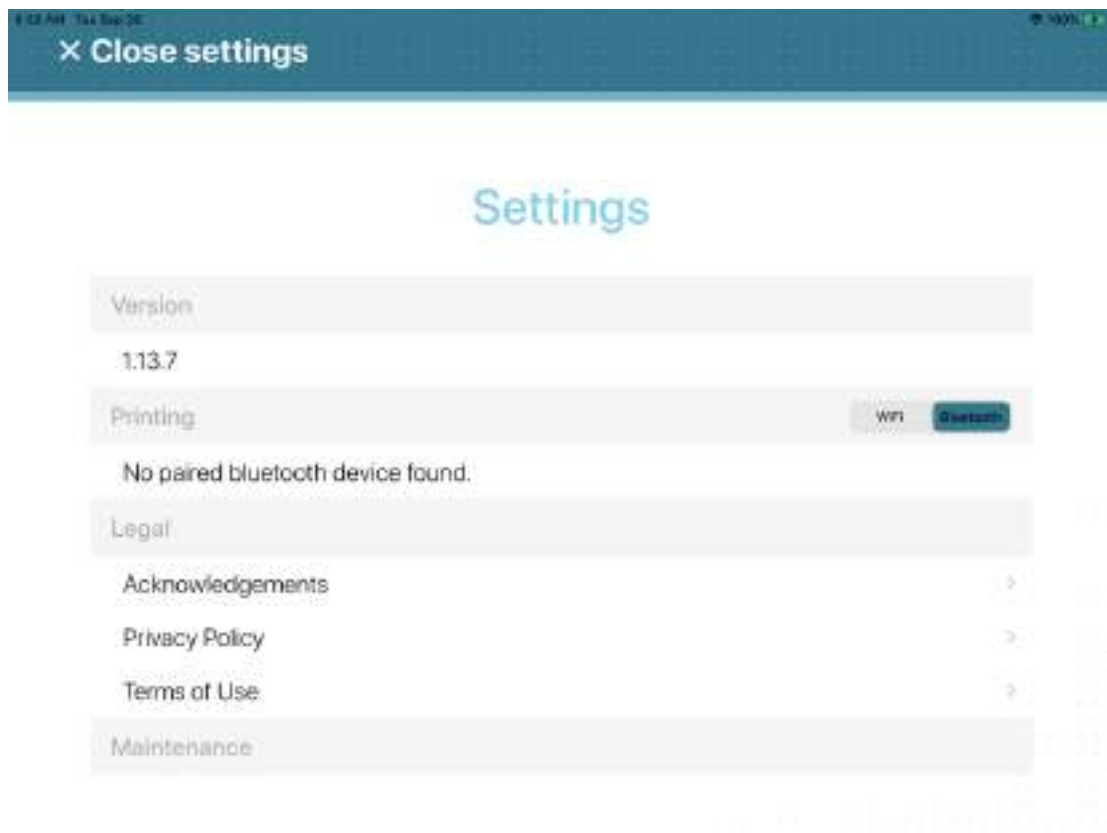


- b) Select **BLUETOOTH** > **Automatic Reconnection (On/Off)** > **On** in the settings menu and press **OK**.

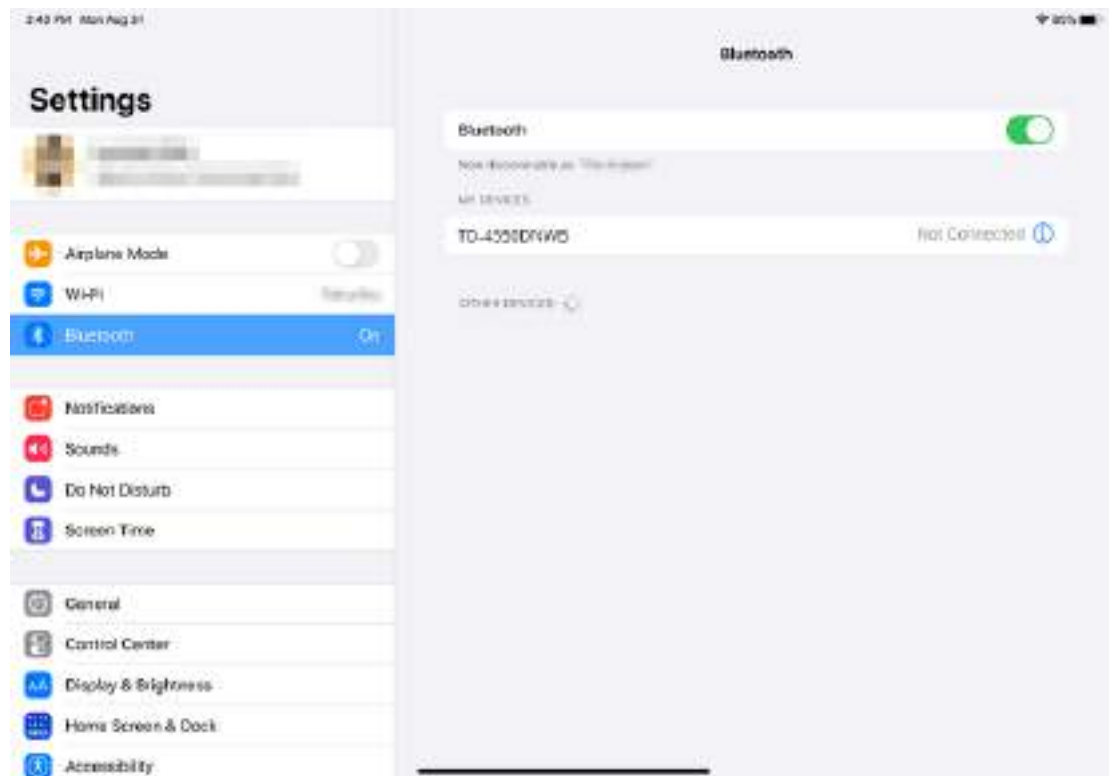


- 5 Pair your Bluetooth label printer with your ClearID Self-Service Kiosk iPad.

- a) In the Self-Service Kiosk mobile app, tap **Settings** (👤).
- b) In the *Printing* section, tap the slider control to select **Bluetooth**.

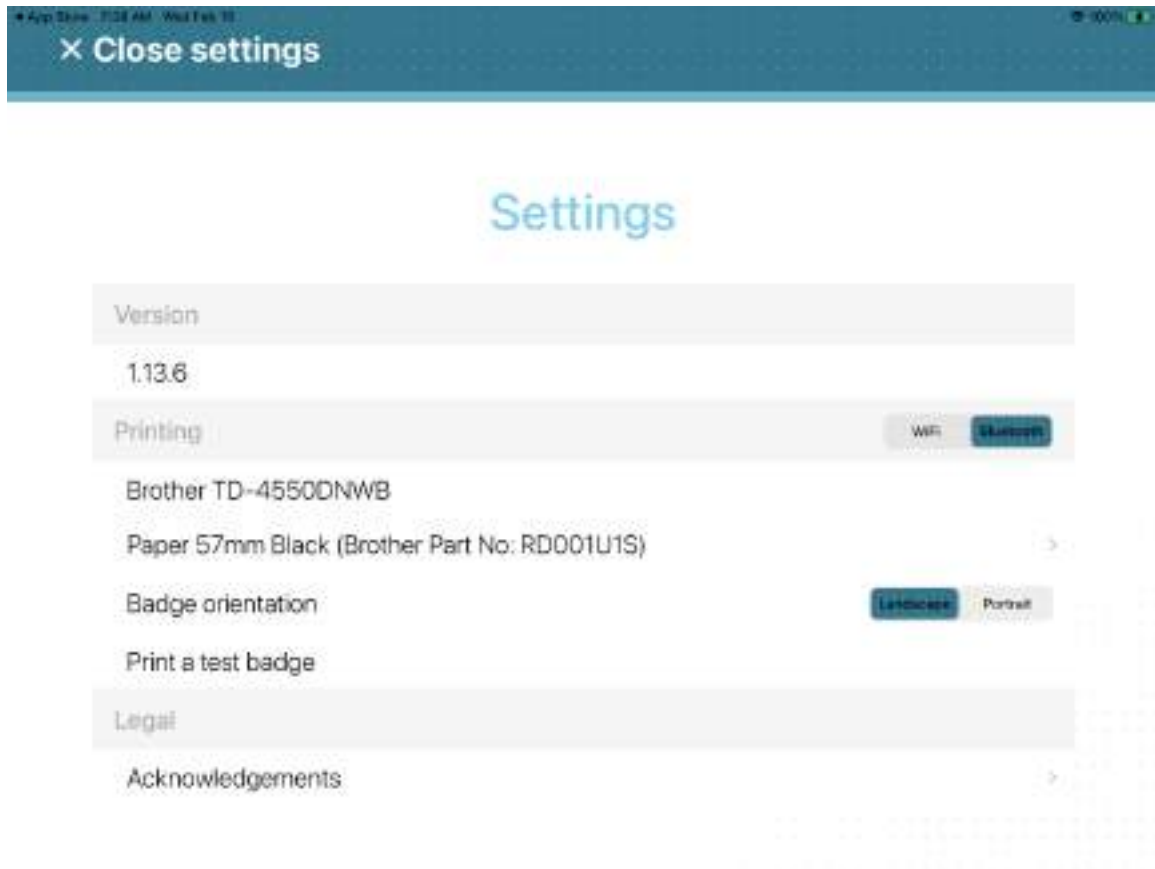


- 6 On your iPad, navigate to the Apple **Settings** icon, tap **Settings** > **Bluetooth**.
- a) (Optional) If **Bluetooth** is disabled, tap the slider to enable Bluetooth.



- b) Click the correct printer to pair the ClearID Self-Service Kiosk iPad with your printer.

- 7 In the Self-Service Kiosk mobile app, tap **Settings** (⚙️).



- a) In the *Printing* section, check that your Brother TD-4550DNWB printer is displayed.

TIP: If the printer is not displayed or bluetooth is not selected, tap **WiFi** then tap **Bluetooth** to trigger discovery again.

After you finish

(Optional) [Print a test badge](#).

Related Topics

[Firewall ports](#) on page 11

Configuring the Self-Service Kiosk label printer for Wi-Fi mode (Brother TD-4550DNWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother TD-4550DNWB Quick Setup Guide](#)
- [Brother TD-4550DNWB User Guide](#)
- [Brother TD-4550DNWB online User Guide \(HTML\)](#)
- [Brother TD-4550DNWB LED status indicators](#)

What you should know

- One label printer can support up to five self-service kiosks
- The label printer must be on the same Wi-Fi network as the ClearID Self-Service Kiosk iPad.

The Wi-Fi network must be enabled for use and support the following:

- Bonjour - required for device search.
- SNMP - required to check printer status information.
- UDP or TCP Port 9100 - required to send print data.

Procedure

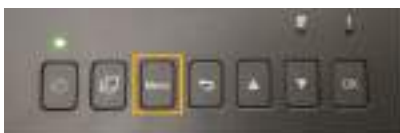
- 1 Plug printer AC adapter into a power outlet and connect the power lead to the label printer.



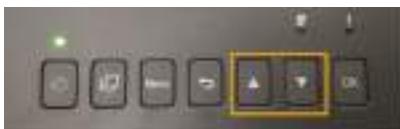
- 2 Press the **Power** button to turn the label printer on.



- 3 Press the **Menu** button.



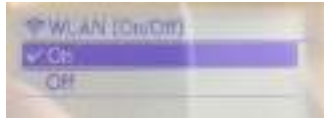
- 4 Use the arrow buttons to navigate the label printer menu.



- 5 Scroll down to the **WLAN (6/8)** settings and press **OK**.



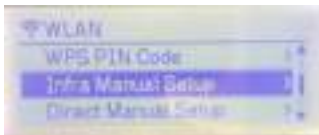
- a) Select **WLAN (On/Off) > On** and press **OK**.



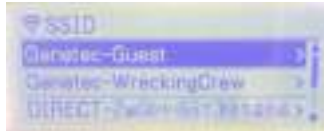
- b) In the *Network Mode* menu items, select **Infrastructure Mode** and press **OK**.



- 6 Scroll down to **Infra Manual Setup** and press **OK**.



- a) After the search completes, scroll down and select your Wi-Fi network from the Service Set Identifier (SSID) list and press **OK**.



NOTE: Typically this network is a Wi-Fi network with AirPrint enabled.

- b) When prompted enter the Wi-Fi password.

- 7 Navigate to **WLAN Status > Infrastructure Mode** and press **OK** to verify your Wi-Fi network status and IP address.



TIP: Make a note of the **SSID** (Wi-Fi network) and **IP Addr** (Label Printer IP) for later use.

- The SSID is used to verify that you are on the same Wi-Fi network as the ClearID Self-Service Kiosk iPad.
- The IP address is used later when selecting a label printer to verify you have the correct printer.

- 8 [Select your Wi-Fi label printer](#).

After you finish

(Optional) [Print a test badge](#).

Related Topics

[Firewall ports](#) on page 11

Configuring the Self-Service Kiosk label printer for Ethernet mode (Brother TD-4550DNWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother TD-4550DNWB Quick Setup Guide](#)
- [Brother TD-4550DNWB User Guide](#)
- [Brother TD-4550DNWB online User Guide \(HTML\)](#)
- [Brother TD-4550DNWB LED status indicators](#)

What you should know

- One label printer can support up to five self-service kiosks

IMPORTANT: Do not connect this product to any LAN connection that's subject to overvoltages.

Procedure

- 1 Plug printer AC adapter into a power outlet and connect the power lead to the label printer.



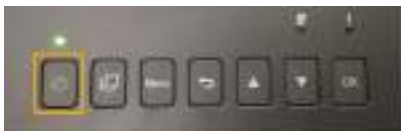
- 2 Make sure that the printer is turned **OFF** before connecting the LAN cable.



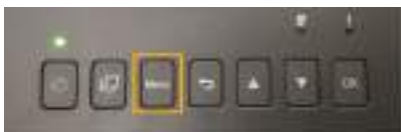
- a) Connect a LAN cable to the LAN port on the back of the printer.

TIP: Use a straight-through Category 5 (or greater) twisted-pair cable for 10BASE-T or 100BASE-TX Fast Ethernet Network.

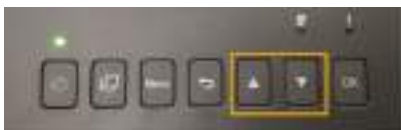
- 3 Press the **Power** button to turn the label printer on.



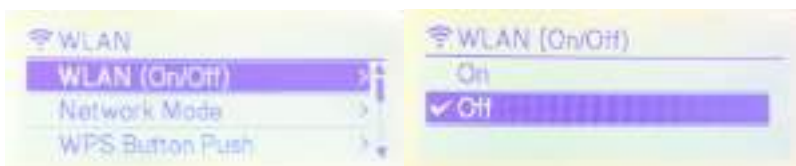
- 4 Press the **Menu** button.



- 5 Use the arrow buttons to navigate the label printer menu.



- 6 From the label printer **Settings** menu, turn OFF **WLAN** (Wi-Fi).



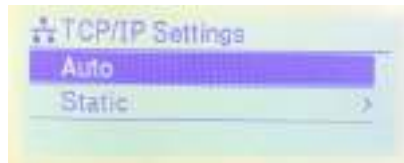
- 7 From the label printer **Settings** menu, turn OFF **Bluetooth**.



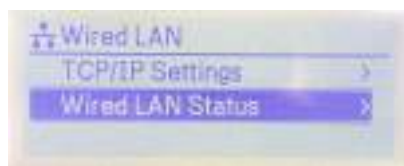
- 8 Scroll down to the **Wired LAN (5/8)** settings and press **OK**.



- a) Click **TCP/IP Settings** and select **AUTO**.



- b) Click **Wired LAN Status** to check your printer.



- c) Check your connection **Status**, **IPConfig**, and **IP Addr**.



TIP: Make a note of your IP address and other settings for later use when selecting your printer.

- 9 [Select your label printer \(Ethernet\)](#).

After you finish

(Optional) [Print a test badge](#).

Related Topics

[Firewall ports](#) on page 11

Selecting a Self-Service Kiosk label printer

Before you can print visitor badges from the Genetec ClearID™ Self-Service Kiosk, you must select a label printer.

Before you begin

Do one of the following:

- [Configure the Brother QL-820NWBc or QL-820NWB Self-Service Kiosk Label Printer](#)
- [Configure the Brother TD-4550DNWB Self-Service Kiosk Label Printer](#)

What you should know

Wi-Fi or Ethernet only: Make sure that you have the IP address of the label printer so that you can verify your selection.

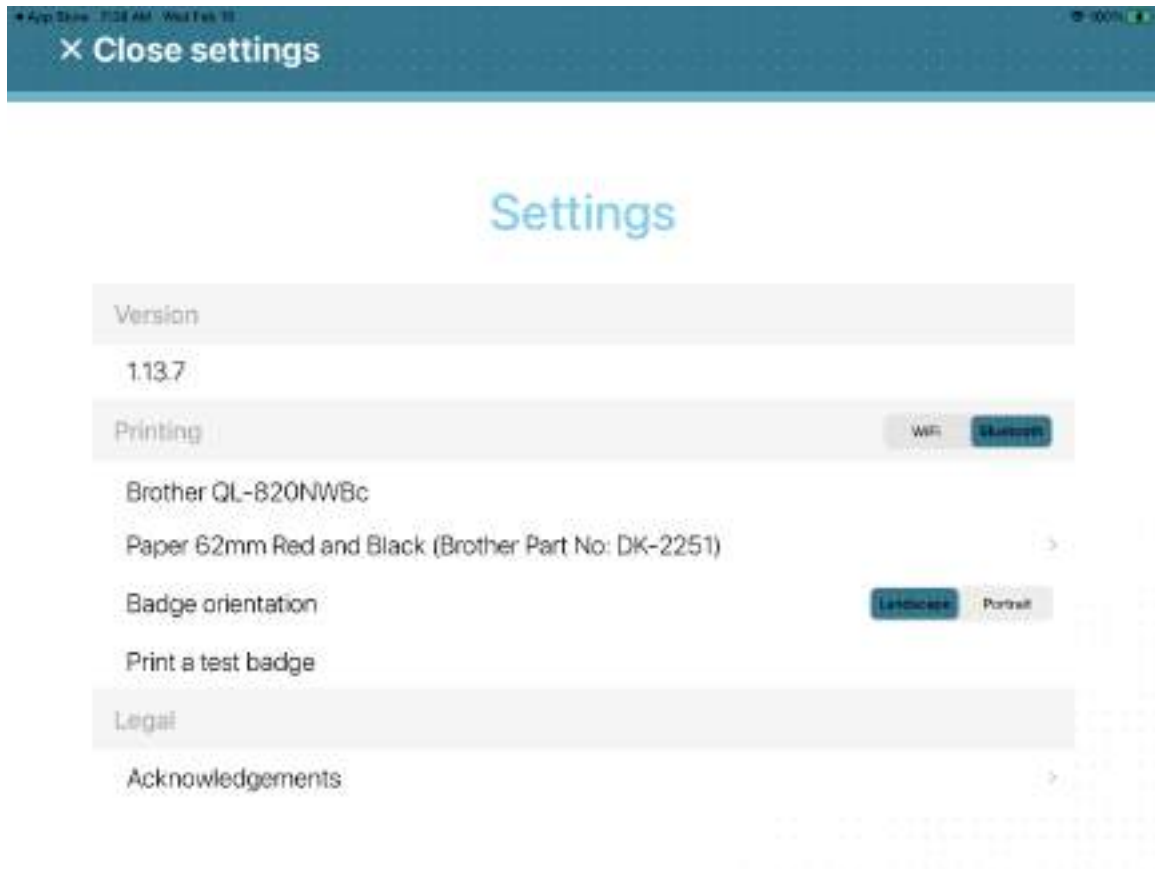
Procedure

To select a Bluetooth kiosk label printer:

- 1 In the Self-Service Kiosk mobile app, tap **Settings** (⚙️).
- 2 On the **Settings** page, tap **Bluetooth** to select the printing mode you require.
 - a) If requested, enter your user authentication details.



- 3 If you selected **Bluetooth**, in the **Printing** section, your selected printer should be displayed.



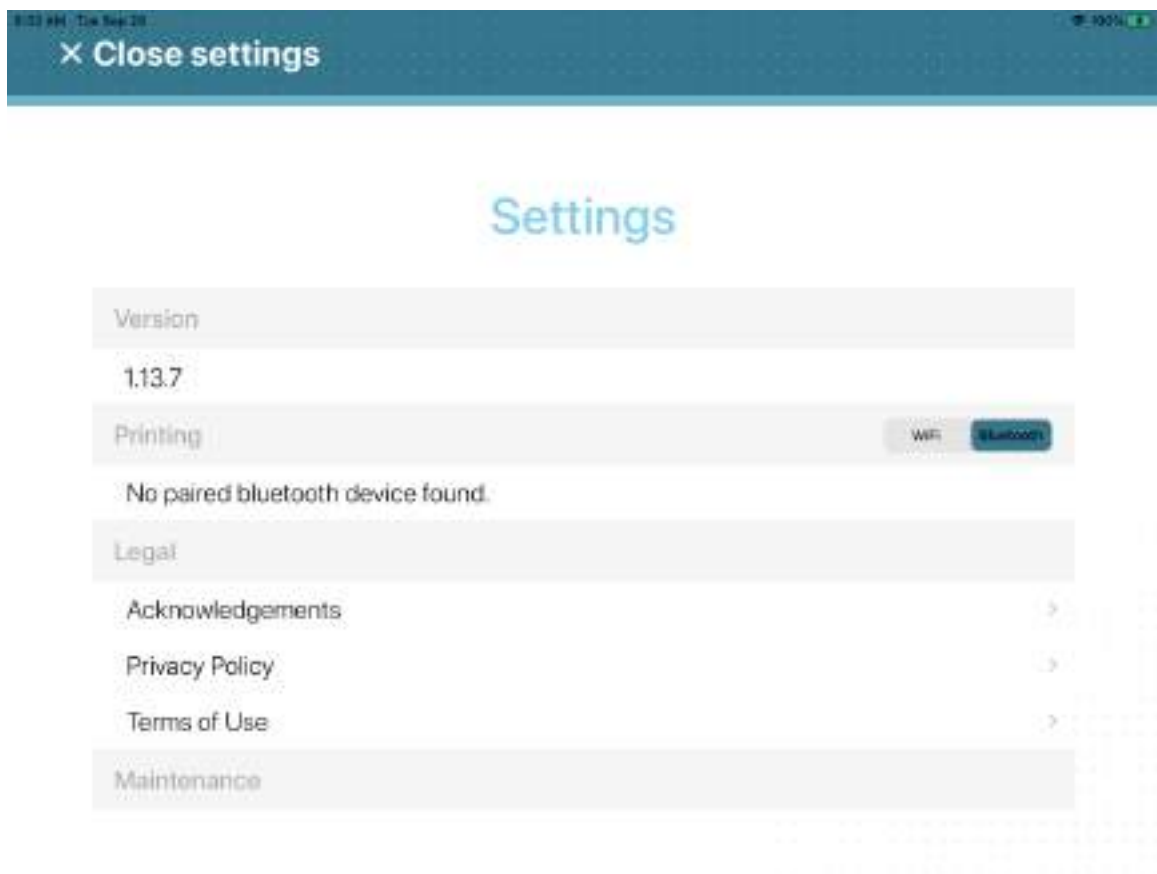
TIP: Bluetooth mode: If the printer is not displayed or bluetooth is not selected, tap **WiFi** then tap **Bluetooth** to trigger discovery again.

- 4 Tap **Close settings** to complete your printer selection setup.

To select a Wi-Fi kiosk label printer:

- 1 In the Self-Service Kiosk mobile app, tap **Settings** (⚙️).

- 2 On the **Settings** page, tap **WiFi** to select the printing mode you require.
 - a) If requested, enter your user authentication details.



3 Choose one of the following:

- **Discover WiFi printer**
- **Set printer manually (IP address)**

a) If you selected **Discover WiFi printer**, wait for the **Printers** list to be displayed then select your printer.

Verify that the IP address of the printer you're selecting matches the IP address seen during printer configuration.

TIP: Wi-Fi mode: If the printer isn't displayed or Wi-Fi is not selected, tap **Bluetooth** then tap **WiFi** to trigger discovery again.

b) If you selected **Set printer manually (IP address)**, enter the IP address of the printer and tap **Save**.

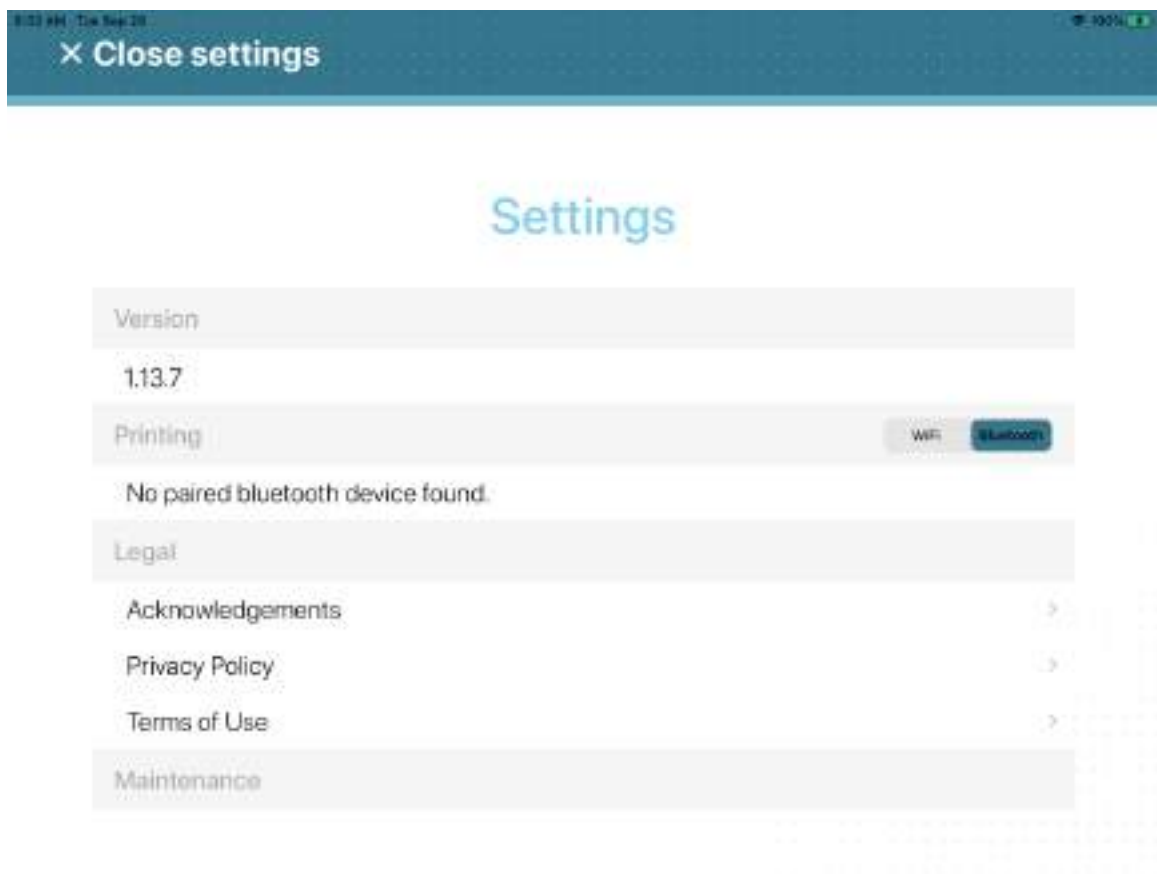


4 Tap **Close settings** to complete your printer selection setup.

To select an Ethernet kiosk label printer:

1 In the Self-Service Kiosk mobile app, tap **Settings** (⚙️).

- 2 On the **Settings** page, tap **WiFi** to select the printing mode you require.
 - a) If requested, enter your user authentication details.



3 Choose one of the following:

- **Discover WiFi printer**
- **Set printer manually (IP address)**

a) If you selected **Discover WiFi printer**, wait for the **Printers** list to be displayed then select your printer.

Verify that the IP address of the printer you're selecting matches the IP address seen during printer configuration.

TIP: Wi-Fi mode: If the printer isn't displayed or Wi-Fi is not selected, tap **Bluetooth** then tap **WiFi** to trigger discovery again.

b) If you selected **Set printer manually (IP address)**, enter the IP address of the printer and tap **Save**.



4 Tap **Close settings** to complete your printer selection setup.

After you finish

[Print a test badge.](#)

Printing a test badge from the Self-Service Kiosk

To help you understand if the printer is working as expected, you can print a test badge. This test print can be performed either after first initial setup or after replacing a label roll.

Before you begin

- [Select a kiosk label printer.](#)
- Make sure that labels are loaded in the printer.
- [Make sure that labels are correctly aligned.](#)

What you should know

The Brother QL-820NWBc, QL-820NWB, and QL-810W label printers can print either **Black** or **Red and Black** badges:

- 62mm Black (Brother Part No: DK-2205)
- 62mm Red and Black (Brother Part No: DK-2251)

The Brother TD-4550DNWB label printer can only print **Black** badges:

- 57mm Black (Brother Part No: RD001U1S)

IMPORTANT: The labels for the Brother TD-4550DNWB printer **MUST** be orientated correctly otherwise badge printing issues can occur.

Badges can be printed in either *Portrait* or *Landscape* format.

Procedure

- 1 In the Genetec ClearID™ Self-Service Kiosk mobile app, tap settings ().

- 2 In the *Settings* page, tap **Print a test badge**.

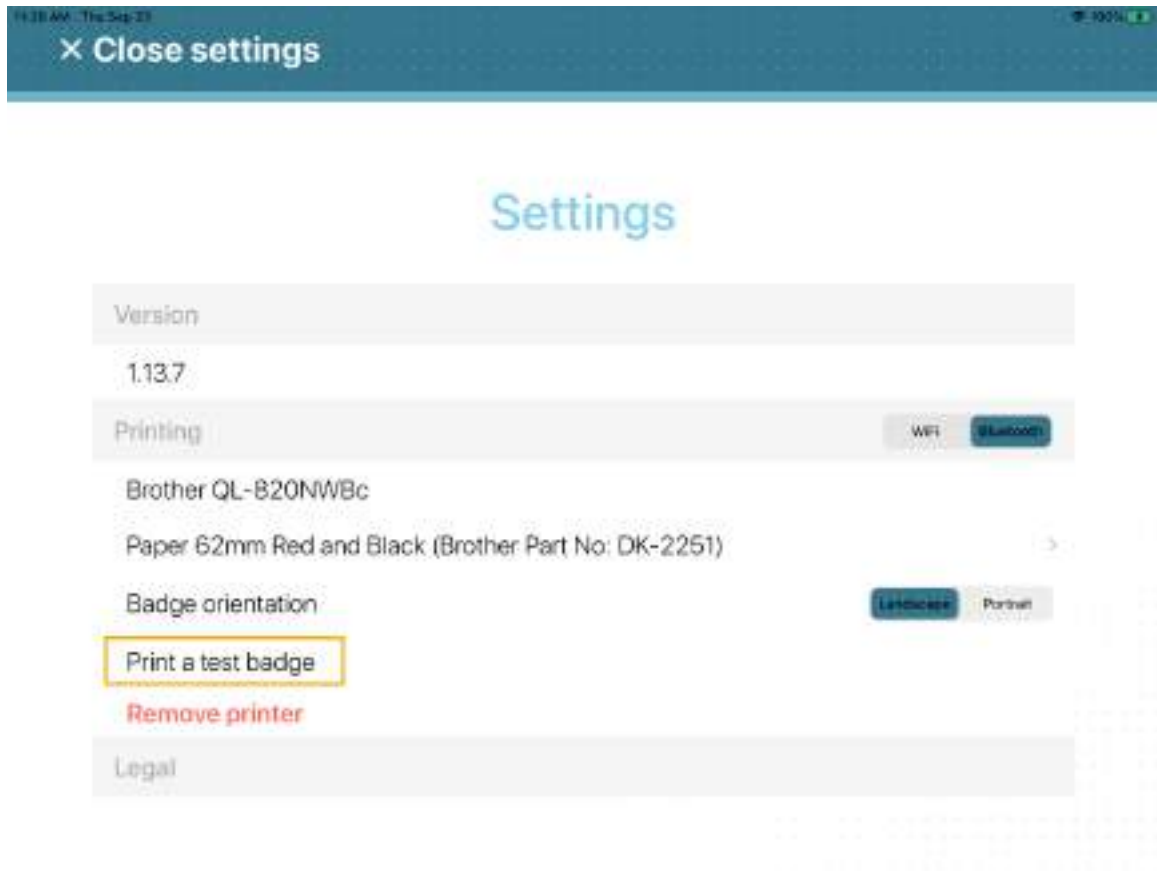


Figure 14: Settings page - Brother QL-820NWBc printer

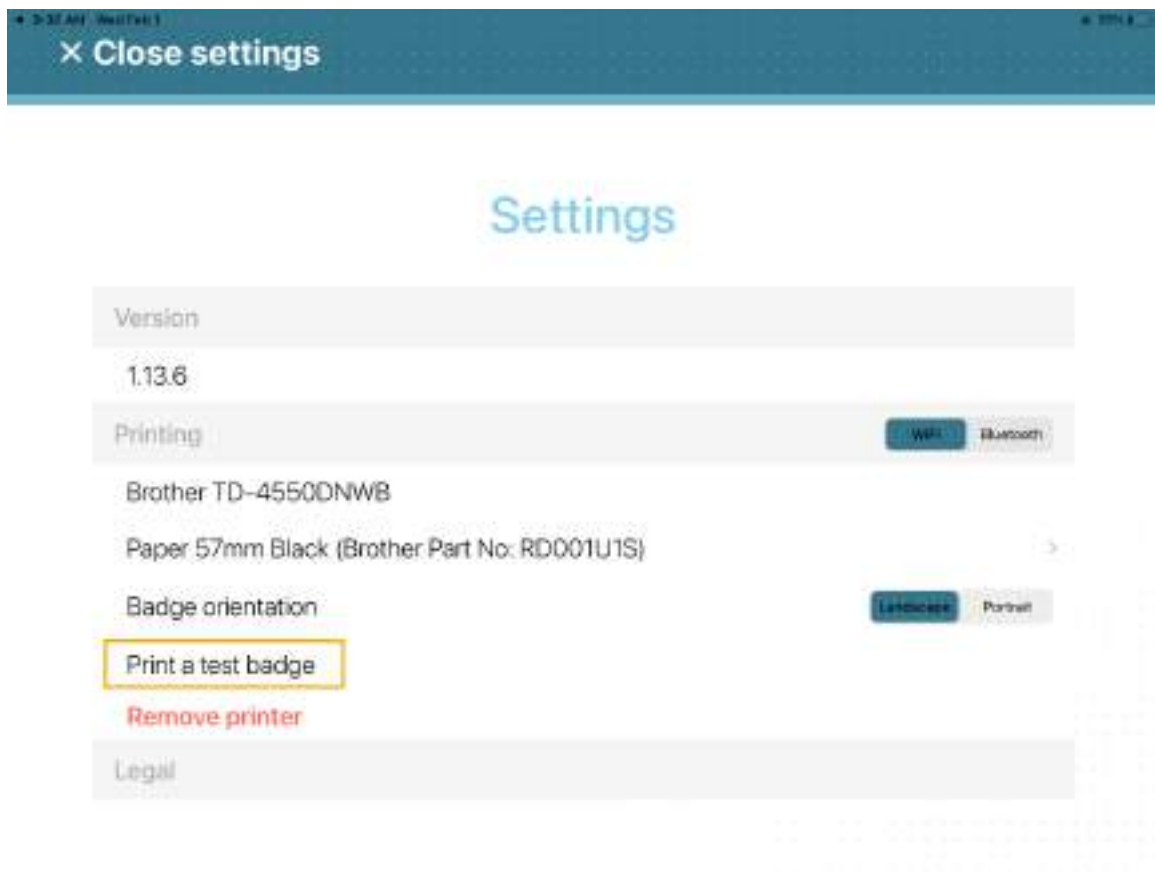


Figure 15: Settings page - Brother TD-4550DNWB printer

- 3 Collect and examine your test badge.



Badge dimensions: **10 x 6.1 cm's** or **3.94 x 2.56 inches**.

NOTE: When printing to a Brother TD-4550DNWB label printer, your badges are printed in black and white.

You are now ready for visitors to use the ClearID Self-Service Kiosk and print their own visitor badges during their check-in.

After you finish

From time to time you might need to order supplies, replace the coin cell battery, recharge the optional battery unit (Brother QL-820NWBc or QL-820NWB only), or clean the label printer. For more information, see the third-party user guide documentation for your printer.

Related Topics

[Self-Service Kiosk label printer issues](#) on page 330

Resetting the Self-Service Kiosk mobile app

In some situations, you might need to perform a hard reset of the Genetec ClearID™ Self-Service Kiosk mobile app. For example, if you encounter issues with selecting the label printer, printing labels, listing people, or if you want to move the kiosk to another site.

Before you begin

- Make sure that you have your Apple ID information.
- Make sure that you have your Wi-Fi network information.

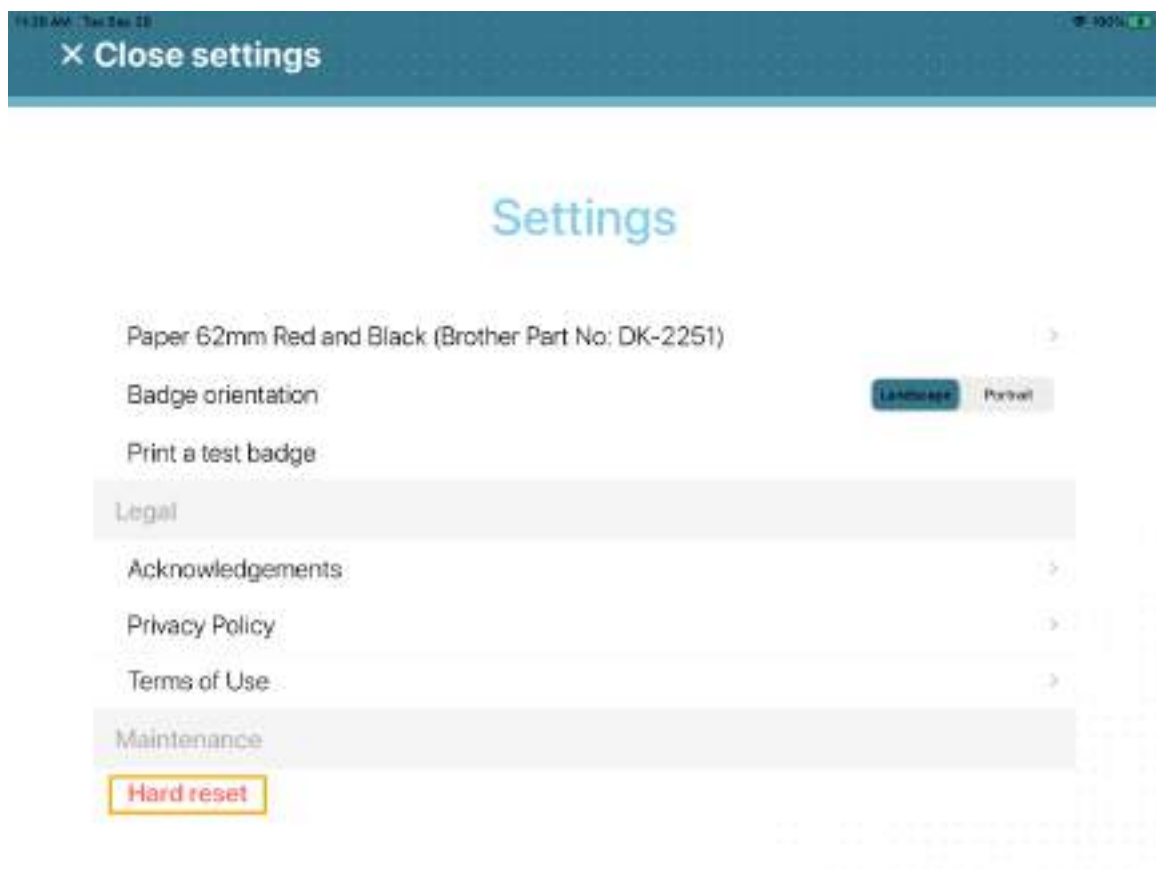
What you should know

- Only a site administrator can generate a device activation code in ClearID.

CAUTION: The hard reset action erases all application data, user data, and visit, check-in, check-out information from the Kiosk device and performs a hard reset of the mobile app. If you proceed, you must register the kiosk device again.

Procedure

- 1 In the Self-Service Kiosk mobile app, tap **Settings** (⚙️).
- 2 In the *Settings page*, scroll to the bottom of the page and in the *Maintenance* section tap **Hard reset**.



- 3 [Configure your Self-Service Kiosk iPad.](#)
- 4 [Configure your Self-Service Kiosk label printer.](#)

- 5 [Select your Self-Service Kiosk label printer.](#)
- 6 [Print a test badge.](#)

Your Self-Service Kiosk is now ready for use.

Related Topics

[Self-Service Kiosk label printer issues](#) on page 330

Self-Service Kiosk options

Use the following information to help you understand the Genetec ClearID™ Self-Service Kiosk options that are available.

Item description	Part	
Kiosk tabletop stand Apple iPad 10.9 inch (Wi-Fi) with Apple Care Table top kiosk kit (Printer <u>not included</u>) NOTE: Depending on your check-in requirements, the kiosk iPad housing can be configured on this floor stand for use in either <i>Portrait</i> or <i>Landscape</i> mode.	CD-KIOSK-TABLETOP-KIT-V2¹	
Kiosk floor stand Apple iPad 10.9 inch (Wi-Fi) with Apple Care Floor stand kit (Printer <u>not included</u>) NOTE: Depending on your check-in requirements, the kiosk iPad housing can be configured on this floor stand for use in either <i>Portrait</i> or <i>Landscape</i> mode.	CD-KIOSK-FLOORSTAND-KIT-V2¹	
Visitor label printer Brother QL-820NWBc thermal printer - Network (Ethernet), Wi-Fi, and Bluetooth - Prints black and red labels NOTE: Only the Brother DK Roll - 62mm Black (Brother Part No: DK-2205) or 62mm Red and Black (Brother Part No: DK-2251) labels are supported.	Brother QL-820NWBc Kit part numbers: - CD-KIOSK-PRINTER-AU-KIT - CD-KIOSK-PRINTER-BRA-KIT - CD-KIOSK-PRINTER-EU-KIT - CD-KIOSK-PRINTER-NA-KIT - CD-KIOSK-PRINTER-UK-KIT	
Visitor label printer Brother TD-4550DNWB thermal printer - Network (Ethernet), Wi-Fi, and Bluetooth - Prints black labels	NOTE: This printer is no longer available for purchase through Genetec™. We now support and sell the Brother QL-820NWBc (CD-KIOSK-PRINTER-NA-KIT).	

Item description	Part	Item
NOTE: Only the Brother RD Roll - 57mm Black (Brother Part No: RD001U1S) labels are supported.		
Annual subscription for one kiosk (Volume pricing available for 10 kiosks or more)	CD-KIOSK-LIC-1Y	Kiosk subscription license

IMPORTANT: ¹ For **EMEA**, **APAC**, and some **LATCAR** regions (when ordering either the CD-KIOSK-FLOORSTAND-KIT-V2 or the CD-KIOSK-TABLETOP-KIT-V2) you must include **CD-KIOSK-WORLD-ADAPTER-KIT**.

The CD-KIOSK-WORLD-ADAPTER-KIT part number includes a World Travel Adapter kit and power adapter plugs to fit different electrical outlets around the world. These include North America, Japan, China, United Kingdom, Continental Europe, Korea, Australia, Hong Kong, and Brazil. Without this kit, the plug isn't compatible with the electrical outlets in your region.

For more information or to order kiosk parts, see [Genetec Parts Manager](#).

Related Topics

[ClearID Self-Service Kiosk Datasheet \(2 pages\)](#)

[Supported devices](#) on page 12

Kiosk floor stand

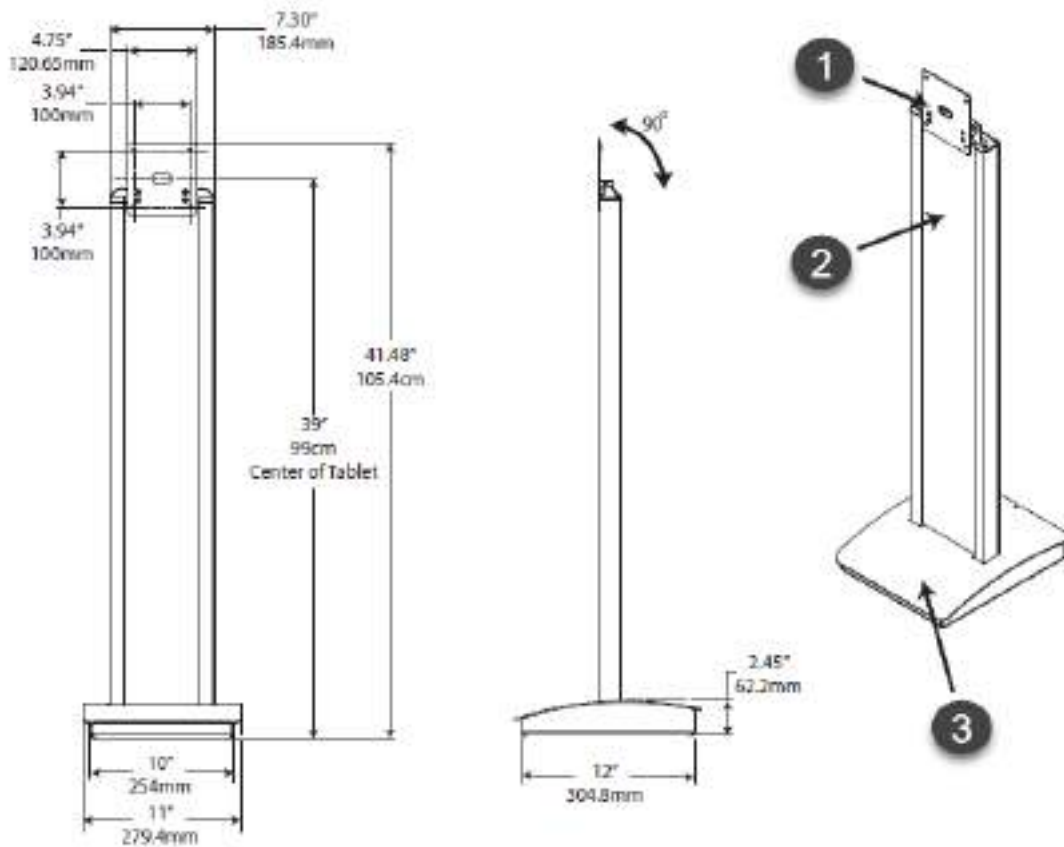
Use the following information to help you understand the Genetec ClearID™ Self-Service Kiosk floor stand dimensions, mounting, and features.



NOTE: Depending on your check-in requirements, the iPad housing can be configured for use in either *Portrait* or *Landscape* mode with this floor stand.

Floor stand dimensions

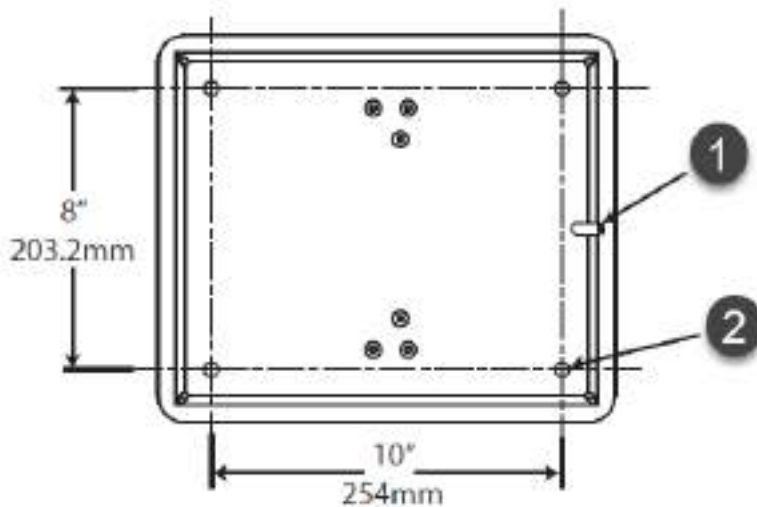
The following diagram illustrates the floor stand dimensions including the height and footprint of the stand.



- ¹ Mount supports any tablet enclosure with a standard VESA mount (100mm x 100mm) or a 90° degree rotation adapter.
- ² Removable signage panel (included).
- ³ Removable cover provides access to the storage area for the power supply.

Floor mount

The following diagram illustrates the floor mount dimensions and underside view of the kiosk floor stand.



¹ Opening for power supply cable.

² 4x floor mounting holes for 0.25inch or 6mm screw hardware (not included) used to secure the floor stand to the floor surface.

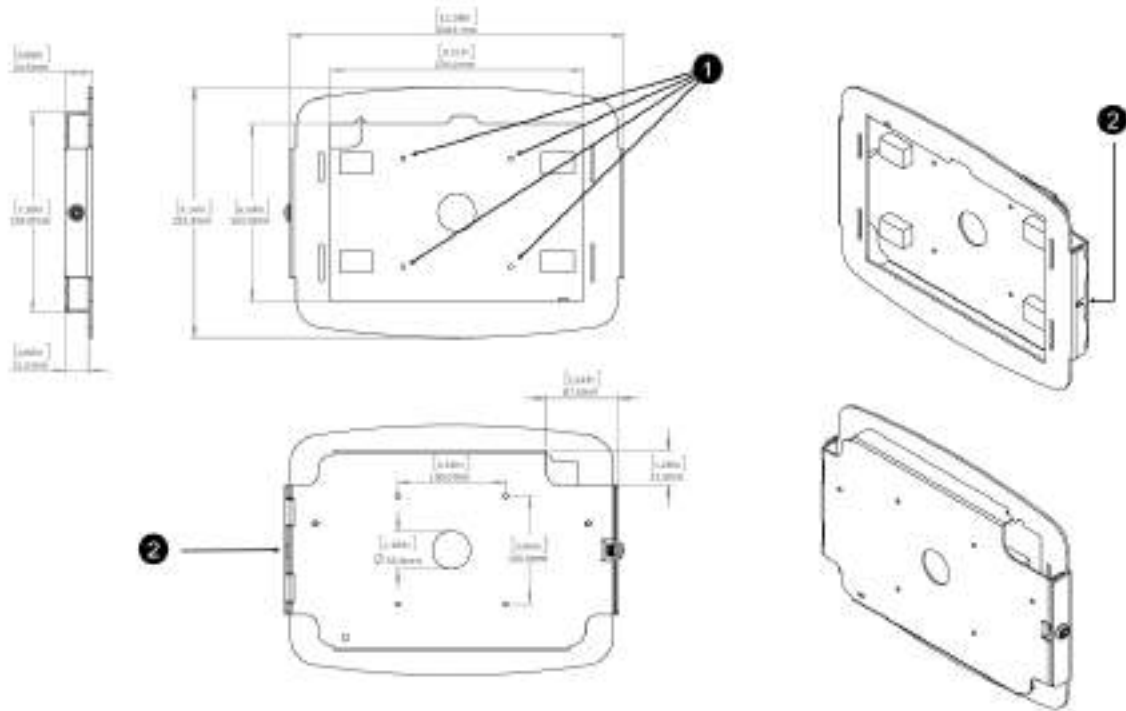
Floor stand features

The floor stand includes the following features:

- Free standing or floor mount option.
- The mount supports any tablet enclosure with a standard VESA mount (100mm x 100mm).
- Tablet power supply can be stored in the base.
- Tablet power cable can be concealed in the legs.
- The enclosure mounting surface can be rotated 90° degrees. This rotation function means that the iPad housing can be orientated for use in either *Portrait* or *Landscape* mode with this floor stand.

iPad enclosure

The following diagram illustrates the floor stand iPad enclosure dimensions.



¹ 4x holes for mounting iPad enclosure to floor stand.

² Opening for power supply cable.

Related Topics

[Self-Service Kiosk options](#) on page 282

[About ClearID Self-Service Kiosk](#) on page 241

[ClearID Self-Service Kiosk Datasheet \(2 pages\)](#)

Kiosk floor stand printer shelf

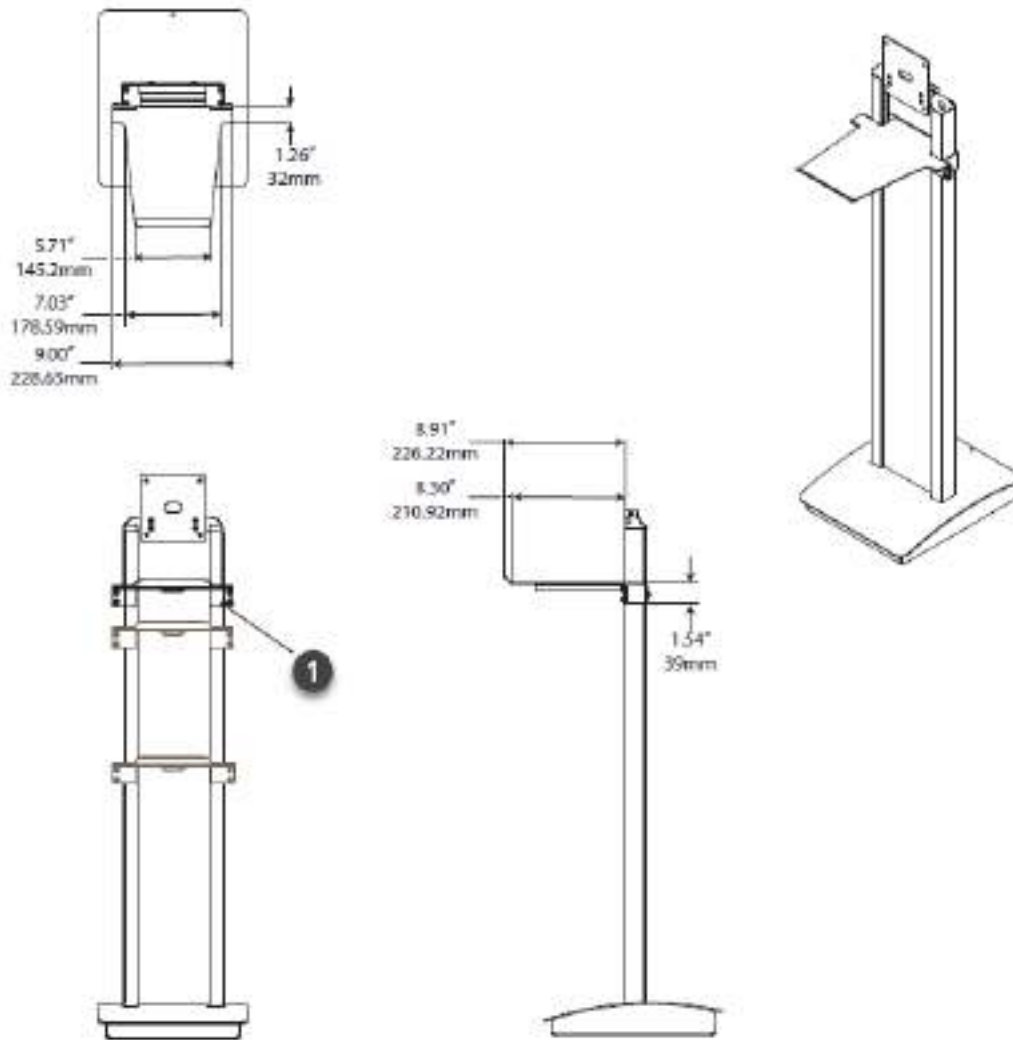
Use the following information to help you understand the dimensions and features of the printer shelf for the Genetec ClearID™ Self-Service Kiosk floor stand.



NOTE: Depending on the size and model of printer that you choose, you might need to trim or modify the center panel (graphic panel) of the floor stand to allow for cable access.

Printer shelf dimensions

The following diagram illustrates the printer shelf dimensions.



¹ Height adjustable printer shelf.

Printer shelf features

The printer shelf includes the following features:

- Mounts to floor stand
- Height adjustable
- Fits various printers

Related Topics

[Self-Service Kiosk options](#) on page 282

[About ClearID Self-Service Kiosk](#) on page 241

[ClearID Self-Service Kiosk Datasheet \(2 pages\)](#)

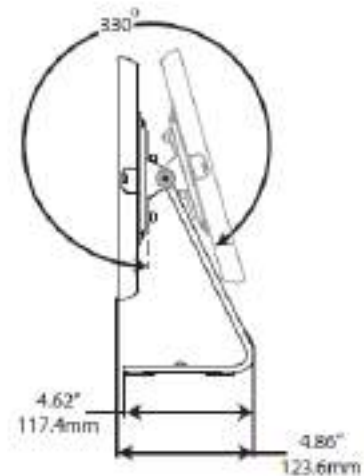
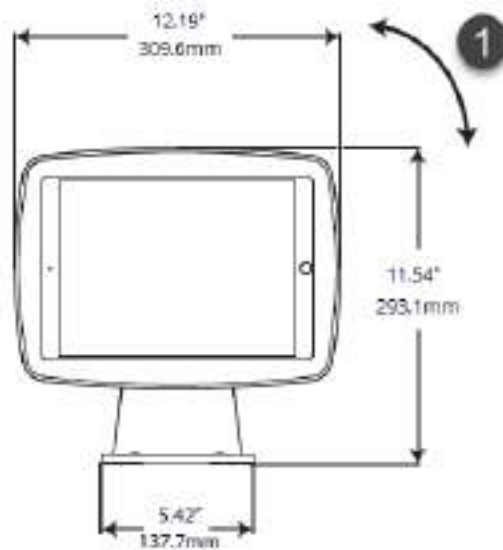
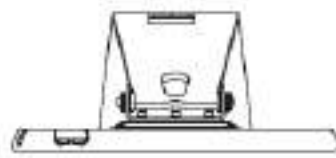
Kiosk tabletop stand

Use the following information to help you understand the Genetec ClearID™ Self-Service Kiosk tabletop stand dimensions, mounting, and features.



Tabletop stand dimensions

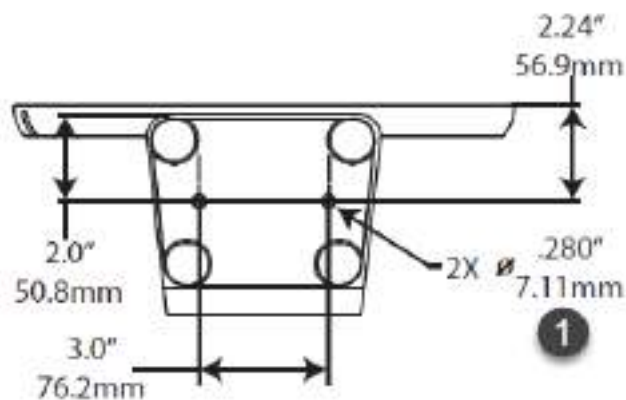
The following diagram illustrates the tabletop stand dimensions including the height and footprint of the stand.



¹ 90° rotation (portrait or landscape orientation).

Tabletop stand mounting

The following diagram illustrates the tabletop mount dimensions.



¹ 2x Tabletop mounting holes for 0.25inch or 6mm screw hardware (not included).

Tabletop stand features

The tabletop stand includes the following features:

- 90° degree rotation (portrait or landscape orientation).
- Flip tablet function.
- Counter mounting option.

Related Topics

[Self-Service Kiosk options](#) on page 282

[About ClearID Self-Service Kiosk](#) on page 241

[ClearID Self-Service Kiosk Datasheet \(2 pages\)](#)

Identity document types

Use the following information to help you understand all the different identity document types that are supported by the Genetec ClearID™ Self-Service Kiosk during the check-in process.

NOTE: All identity document processing is performed locally on the ClearID Self-Service Kiosk iPad. This local processing during check-in ensures that ID data or pictures are never sent to the cloud for maximum security and compliance.

Supported identity documents (Asia)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Afghanistan	ID Card	تذکره الکترونیکی	Front, back	Latin
Afghanistan	Paper Passport ^{BETA}	پاسپورٹ	Bio-data page	Latin
Armenia	ID Card	նույնականացման քարտը	Front, back	Latin
Azerbaijan	ID Card	Şəxsiyyət vəsiqəsi	Front, back	Latin
Azerbaijan	Polycarbonate Passport ^{BETA}	Pasport	Bio-data page	Latin
Bangladesh	Driving License ^{BETA}	মোটর ড্রাইভিং লাইসেন্স	Front, back	Latin
Bangladesh	ID Card	জাতীয় পরিচয় পত্র	Front, back	Latin
Bangladesh	Paper Passport	পাসপোর্ট	Bio-data page	Latin
Brunei	ID Card	Kad Pengenalan (Kuning)	Front, back	Latin
Brunei	Military ID ^{BETA}	Kad Pengenalan Tentera (ABDB)	Front, back	Latin
Brunei	Residence Permit ^{BETA}	Kad Pengenalan (Ungu)	Front, back	Latin
Brunei	Temporary Residence Permit ^{BETA}	Kad Pengenalan (Hijau)	Front, back	Latin
Cambodia	Driving License ^{BETA}	#####	Front	Latin
Cambodia	ID Card	#####	Front	Latin
Cambodia	Polycarbonate Passport	#####	Bio-data page	Latin
China	ID Card	中华人民共和国居民身份证	Front, back	Latin
China	Paper Passport	中华人民共和国护照	Bio-data page	Latin
Hong Kong	ID Card	香港身份證	Front	Latin
Hong Kong	Polycarbonate Passport ^{BETA}	護照	Bio-data page	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
India	ID Card ^{BETA}	Aadhaar card, आधार कार्ड	Front, back	Latin
India	PAN Card	स्थायी खाता संख्या कार्ड	Front	Latin
India	Paper Passport		Bio-data page	Latin
India	Voter ID	भारतीय मतदाता पहचान पत्र	Front, vertical	Latin
India, Gujarat	Driving License ^{BETA}	इराइवंगि लाईसेंस	Front	Latin
India, Karnataka	Driving License	इराइवंगि लाईसेंस	Front	Latin
India, Kerala	Driving License ^{BETA}	इराइवंगि लाईसेंस	Front, back	Latin
India, Madhya Pradesh	Driving License ^{BETA}	इराइवंगि लाईसेंस	Front	Latin
India, Maharashtra	Driving License	इराइवंगि लाईसेंस	Front	Latin
India, Punjab	Driving License ^{BETA}	इराइवंगि लाईसेंस	Front	Latin
India, Tamil Nadu	Driving License ^{BETA}	इराइवंगि लाईसेंस	Front, back	Latin
Indonesia	Driving License	Surat Izin Mengemudi (SIM)	Front	Latin
Indonesia	ID Card	Kartu Tanda Penduduk (KTP)	Front	Latin
Indonesia	Paper Passport	Paspor	Bio-data page	Latin
Japan	Driving License ^{BETA}	運転免許	Front	Latin
Japan	My Number Card	マイナンバーカード	Front	Latin
Japan	Paper Passport	旅券	Bio-data page	Latin
Japan	Residence Permit ^{BETA}	在留カード	Front	Latin
Kazakhstan	ID Card	Жеке куәлік, Удостоверение личности	Front, back	Latin
Kyrgyzstan	ID Card	идентификациялык карта, идентификационная карта	Front, back	Latin
Malaysia	Driving License	Lesen Memandu	Front	Latin
Malaysia	MyKAS		Front, back	Latin
Malaysia	MyKad		Front, back	Latin
Malaysia	MyKid		Front, back	Latin
Malaysia	MyPR		Front, back	Latin
Malaysia	MyPolis ^{BETA}		Front, back	Latin
Malaysia	MyTentera		Front, back	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Malaysia	Refugee ID	UNHCR Card	Front	Latin
Malaysia	Polycarbonate Passport	Pasport	Bio-data page	Latin
Malaysia	i-Kad		Front	Latin
Maldives	ID Card	##### #####	Front, back	Latin
Myanmar	Driving License	#####	Front, back	Latin
Nepal	Paper Passport	राहदानी	Bio-data page	Latin
Pakistan	Consular ID	National Identity Card for Overseas Pakistanis (NICOP)	Front, back	Latin
Pakistan	ID Card	Computerized National Identity Card (CNIC), Smart National Identity Card (SNIC)	Front, back	Latin
Pakistan	Paper Passport		Bio-data page	Latin
Pakistan, Punjab	Driving License		Front	Latin
Philippines	Driving License		Front	Latin
Philippines	ID Card	PhilSys ID, PhilID	Front, back	Latin
Philippines	Multipurpose ID	Unified Multi-Purpose ID	Front	Latin
Philippines	Paper Passport		Bio-data page	Latin
Philippines	Professional ID	PRC License	Front	Latin
Philippines	Social Security Card	SSS ID	Front	Latin
Philippines	Tax ID ^{BETA}	TIN ID card	Front	Latin
Philippines	Voter ID ^{BETA}		Front	Latin
Singapore	Driving License		Front, back	Latin
Singapore	Employment Pass		Front	Latin
Singapore	Fin Card		Front	Latin
Singapore	ID Card	NRIC (Pink)	Front, back	Latin
Singapore	Resident ID	NRIC (Blue)	Front, back	Latin
Singapore	Polycarbonate Passport		Bio-data page	Latin
Singapore	S Pass		Front, back	Latin
Singapore	Work Permit		Front, back	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
South Korea	Driving License	자동차운전면허증	Front	Latin
South Korea	ID Card ^{BETA}	주민등록증	Front	Latin
South Korea	Paper Passport ^{BETA}	여권	Bio-data page	Latin
Sri Lanka	Driving License	#####	Front	Latin
Sri Lanka	ID Card	#####, தகைய அடையாள அட்டை	Front, back, vertical	Latin
Sri Lanka	Paper Passport	#####, கடவுச்சீட்டு	Bio-data page	Latin
Taiwan	ID Card ^{BETA}	中華民國國民身分證	Front	Latin
Taiwan	Temporary Residence Permit ^{BETA}	中華民國居留證 (ARC)	Front	Latin
Latin	Latin	Latin	Latin	Latin
Thailand	Alien ID	บัตรประจำตัวคนซึ่งไม่มีสัญชาติไทย (บัตรสีชมพู)	Front	Latin
Thailand	Driving License ^{BETA}	ใบอนุญาตขับรถ	Front, back	Latin
Thailand	ID Card	บัตรประจำตัวประชาชน	Front, back	Latin
Thailand	Polycarbonate Passport	หนังสือเดินทาง	Bio-data page	Latin
Vietnam	Driving License ^{BETA}	Giấy phép lái xe	Front	Latin
Vietnam	ID Card ^{BETA}	Căn cước công dân, Giấy chứng minh nhân dân	Front, back	Latin

Supported identity documents (Europe)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Albania	Driving License	Leje drejtimi	Front	Latin
Albania	Driver Card	Karta e drejtuesit të mjetit	Front	Latin
Albania	ID Card	Letërnjoftim	Front, back	Latin
Albania	Professional DL	Certifikatë aftësimi profesionale	Front	Latin
Albania	Polycarbonate Passport	Pasaportë	Bio-data page	Latin
Austria	Driving License	Führerschein	Front	Latin
Austria	ID Card	Personalausweis	Front, back	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Austria	Paper Passport	Reisepass	Bio-data page	Latin
Austria	Residence Permit ^{BETA}	Aufenthaltstitel	Front, back	Latin
Belarus	Driving License	ВАДЗІЦЕЛЬСКАЕ ПАСВЕДЧАННЕ, ВОДИТЕЛЬСКОЕ УДОСТОВЕРЕНИЕ	Front	Latin
Belarus	Paper Passport	Пашпарт, Паспорт	Bio-data page	Latin
Belgium	Driving License	Rijbewijs, Permis de conduire, Führerschein	Front	Latin
Belgium	ID Card	Identiteitskaart, Carte d'identité, Personalausweis	Front, back	Latin
Belgium	Minors ID	Kids-ID	Front, back	Latin
Belgium	Paper Passport	Paspoort, Passeport, Reisepass	Bio-data page	Latin
Belgium	Residence Permit	Verblijfstitel, Titre de Sejour	Front, back	Latin
Belgium	Resident ID	Document de Sejour, Verblijfsdocument, Aufenthaltsdokument, E Kaart, Carte E, E Karte; E+ Kaart, Carte E+, E+ Karte; F Kaart, Carte F, F Karte; F+ Kaart, Carte F+, F+ Karte	Front, back	Latin
Belgium	Polycarbonate Passport ^{BETA}	Paspoort, Passeport, Reisepass	Bio-data page	Latin
Bosnia and Herzegovina	Driving License	Vozačka dozvola	Front	Latin
Bosnia and Herzegovina	ID Card	Lična karta, Osobna iskaznica	Front, back	Cyrillic, Latin
Bosnia and Herzegovina	Polycarbonate Passport	Pasoš, Пасош, Putovnica	Bio-data page	Latin
Bulgaria	Driving License	Свидетелство за управление на МПС	Front	Cyrillic, Latin
Bulgaria	ID Card	Лична карта	Front, back	Cyrillic, Latin
Bulgaria	Paper Passport	Паспорт	Bio-data page	Latin
Croatia	Driving License	Vozačka dozvola	Front	Latin
Croatia	ID Card	Osobna iskaznica	Front, back	Latin
Croatia	Residence Permit ^{BETA}	Boravišna iskaznica, Dozvola boravka	Front, back	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Croatia	Polycarbonate Passport	Putovnica	Bio-data page	Latin
Cyprus	Driving License	Sürüş ruhsati, Αάδεια οδήγησης	Front	Latin
Cyprus	ID Card	Kimlik kartı, Δελτίο Ταυτότητας	Front, back	Latin
Cyprus	Paper Passport	Pasaport, Διαβατήριο	Bio-data page	Latin
Cyprus	Residence Permit	ΑΔΕΙΑ ΔΙΑΜΟΝΗΣ	Front, back	Latin
Czechia	Driving License	Řidičský průkaz	Front	Latin
Czechia	ID Card	Občanský průkaz	Front, back	Latin
Czechia	Residence Permit	Povolení k pobytu	Front, back	Latin
Czechia	Polycarbonate Passport	Cestovní pas	Bio-data page	Latin
Denmark	Driving License	Kørekort	Front	Latin
Denmark	Residence Permit ^{beta}	Opholdstilladelse, Opholdskort	Front, back	Latin
Denmark	Polycarbonate Passport	Pas	Bio-data page	Latin
Estonia	Driving License	Juhiluba	Front	Latin
Estonia	ID Card	Isikutunnistus	Front, back	Latin
Estonia	Paper Passport	Pass	Bio-data page	Latin
Estonia	Residence Permit ^{BETA}	Elamisluba	Front, back	Latin
Finland	Alien ID	Ulkomaalaisen henkilökortti, Identitetskort för utlänning	Front, back	Latin
Finland	Driving License	Ajokortti, Körkort	Front	Latin
Finland	ID Card	Henkilökortti, Identitetskort	Front, back	Latin
Finland	Residence Permit	Oleskelulupa, Uppehållstillstånd	Front, back	Latin
Finland	Polycarbonate Passport	Passi, Pass	Bio-data page	Latin
France	Driving License	Permis de conduire	Front	Latin
France	ID Card	Carte d'identité	Front, back	Latin
France	Paper Passport ^{BETA}	Passeport	Bio-data page	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
France	Residence Permit ^{BETA}	Titre de séjour	Front, back	Latin
Georgia	Driving License	მართვის მოწმობა	Front	Latin
Georgia	ID Card	მოქალაქის პირადობის მოწმობა	Front, back	Latin
Georgia	Paper Passport ^{BETA}	პასპორტი	Bio-data page	Latin
Germany	Driving License	Führerschein	Front	Latin
Germany	ID Card	Personalausweis	Front, back	Latin
Germany	Minors Passport	Kinderreisepass	Bio-data page	Latin
Germany	Paper Passport	Reisepass	Bio-data page	Latin
Germany	Residence Permit	Aufenthaltstitel	Front, back	Latin
Germany	Polycarbonate Passport	Reisepass	Bio-data page	Latin
Greece	Driving License	Αάδεια οδήγησης	Front	Latin
Greece	ID Card	ΔΕΛΤΙΟ ΤΑΥΤΟΤΗΤΑΣ	Front, back	Latin
Greece	Paper Passport	Διαβατήριο	Bio-data page	Latin
Greece	Residence Permit	ΑΔΕΙΑ ΔΙΑΜΟΝΗΣ	Front, back	Latin
Hungary	Address Card ^{BETA}	Lakcímkártya, Lakcímgazolvány	Front, back	Latin
Hungary	Driving License	Vezetői engedély	Front	Latin
Hungary	ID Card	Személyazonosító igazolvány	Front, back	Latin
Hungary	Paper Passport	Útleve	Bio-data page	Latin
Hungary	Residence Permit ^{BETA}	Tartózkodási engedély	Front, back	Latin
Iceland	Driving License ^{BETA}	Ökuskírteini	Front	Latin
Iceland	Paper Passport ^{BETA}	Vegabréf	Bio-data page	Latin
Ireland	Driving License	Ceadúnas tiomána	Front	Latin
Ireland	Passport Card	Cárta Pas	Front, back	Latin
Ireland	Public Services Card	Cárta Seirbhísi Poiblí	Front, back	Latin
Ireland	Residence Permit ^{BETA}		Front, back	Latin
Ireland	Polycarbonate Passport	Pas	Bio-data page	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Italy	Driving License	Patente di guida	Front	Latin
Italy	ID Card	Carta d'identità	Front, back	Latin
Italy	Paper Passport ^{BETA}	Passaporto	Bio-data page	Latin
Italy	Residence Permit	Permesso di soggiorno	Front, back	Latin
Kosovo	Driving License	Patentë shoferi, возачка дозвола	Front	Latin
Kosovo	ID Card	Letërnjoftim, Лична карта	Front, back	Latin
Kosovo	Paper Passport	Pasaportë, Пасош	Bio-data page	Latin
Latvia	Alien ID	Nepilsoņa personas apliecība	Front, back	Latin
Latvia	Driving License	Vadītāja apliecība	Front	Latin
Latvia	ID Card	Personas apliecība	Front, back	Latin
Latvia	Residence Permit ^{BETA}	Uzturēšanās atļauja	Front, back	Latin
Latvia	Polycarbonate Alien Passport	Nepilsoņa pase	Bio-data page	Latin
Latvia	Polycarbonate Passport	Pase	Bio-data page	Latin
Liechtenstein	ID Card	Identitätskarte	Front, back	Latin
Lithuania	Driving License	Vairuotojo pažymėjimai	Front	Latin
Lithuania	ID Card	Asmens tapatybės kortelė	Front, back	Latin
Lithuania	Residence Permit ^{BETA}	Leidimas gyventi	Front, back	Latin
Lithuania	Polycarbonate Passport	Pasas	Bio-data page	Latin
Luxembourg	Driving License	Permis de conduire	Front	Latin
Luxembourg	ID Card	Carte d'Identité, Personalausweis	Front, back	Latin
Luxembourg	Residence Permit	Titre de séjour	Front, back	Latin
Luxembourg	Polycarbonate Passport	Pass, Passeport	Bio-data page	Latin
Malta	Driving License	Liċenzja tas-Sewqan	Front	Latin
Malta	ID Card	Karta tal-Identità	Front, back	Latin
Malta	Residence Permit	Permess ta' residenza, Residence documentation	Front, back	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Moldova	ID Card ^{BETA}	Buletin de identitate	Front, back	Latin
Moldova	Paper Passport ^{BETA}	Pașaport	Bio-data page	Latin
Montenegro	Driving License	Vozačka dozvola, Водачка дозвола	Front	Latin
Montenegro	ID Card	Lična karta, Лична карта	Front, back	Latin
Montenegro	Polycarbonate Passport	Pasoš, Пасош	Bio-data page	Latin
Netherlands	Driving License	Rijbewijs	Front, back	Latin
Netherlands	ID Card	Identiteitskaart (ID-kaart)	Front, back	Latin
Netherlands	Residence Permit	Verblijfstitel, Verblijfskaart	Front, back	Latin
Netherlands	Polycarbonate Passport	Paspoort	Bio-data page	Latin
North Macedonia	Driving License	возачка дозвола, Patentë shoferi	Front	Cyrillic, Latin
North Macedonia	ID Card	лична карта, Letërnjoftim	Front, back	Cyrillic, Latin
North Macedonia	Polycarbonate Passport	Пасош, Pasaportë	Bio-data page	Latin
Norway	Driving License	Fører kort, Førarkort	Front	Latin
Norway	ID Card		Front, back	Latin
Norway	Residence Permit	Oppholdstillatelse, Oppholdsløyve	Front, back	Latin
Norway	Polycarbonate Passport	Pass	Bio-data page	Latin
Poland	Driving License	Prawo jazdy	Front	Latin
Poland	ID Card	Dowód osobisty	Front, back	Latin
Poland	Paper Passport	Paszport	Bio-data page	Latin
Poland	Residence Permit ^{BETA}	Karta pobytu	Front, back	Latin
Poland	Polycarbonate Passport	Paszport	Bio-data page	Latin
Portugal	Driving License	Carta de Condução	Front	Latin
Portugal	ID Card	Cartão de Cidadão (CC)	Front, back	Latin
Portugal	Paper Passport	Passaporte	Bio-data page	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Portugal	Residence Permit ^{BETA}	Título de Residência, Cartão de Residência	Front, back	Latin
Romania	Driving License	Permis de conducere	Front	Latin
Romania	ID Card	Carte de identitate	Front	Latin
Romania	Polycarbonate Passport	Pasaport, Paşaport	Bio-data page	Latin
Russia	Driving License	Водительское удостоверение	Front	Latin
Russia	Polycarbonate Passport	(Заграничный) Паспорт	Bio-data page	Latin
Serbia	Driving License	Возачка дозвола, Vozačka dozvola	Front	Latin
Serbia	ID Card	Лична карта, Lična karta	Front, back	Cyrillic, Latin
Serbia	Polycarbonate Passport	Пасош, Pasoš	Bio-data page	Latin
Slovakia	Driving License	Vodičský preukaz	Front	Latin
Slovakia	ID Card	Občiansky preukaz	Front, back	Latin
Slovakia	Residence Permit	Povolenie na pobyt, Pobytový preukaz občana EÚ, Pobytový preukaz rodinného príslušníka občana EÚ	Front, back	Latin
Slovakia	Polycarbonate Passport	Cestovný pas	Bio-data page	Latin
Slovenia	Driving License	Vozniško dovoljenje	Front	Latin
Slovenia	ID Card	Osebna izkaznica	Front, back	Latin
Slovenia	Residence Permit	Dovoljenje za prebivanje	Front, back	Latin
Slovenia	Polycarbonate Passport	Potni list	Bio-data page	Latin
Spain	Alien ID	Tarjeta de Identidad de Extranjero (TIE)	Front, back	Latin
Spain	Driving License	Permiso de Conducción	Front	Latin
Spain	ID Card	Documento Nacional de Identidad (DNI)	Front, back	Latin
Spain	Paper Passport	Pasaporte	Bio-data page	Latin
Spain	Residence Permit	Permiso de residencia	Front, back	Latin
Sweden	Driving License	Körkort	Front	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Sweden	ID Card	Nationellt identitetskort	Front, back	Latin
Sweden	Residence Permit	Uppehållstillstånd, Uppehållskort	Front, back	Latin
Sweden	Polycarbonate Passport	Pass	Bio-data page	Latin
Sweden	Social Security Card	Identitetskort, Skatteverkets id-kort	Front	Latin
Switzerland	Driving License	Führerausweis, Permis de conduire, Licenza di condurre, Permiss da manischar	Front	Latin
Switzerland	ID Card	Identitätskarte, Carte d'identité, Carta d'identità, Carta d'identidad	Front, back	Latin
Switzerland	Paper Passport	Pass, Passeport, Passaporto, Passaport	Bio-data page	Latin
Switzerland	Residence Permit	Aufenthaltstitel, Titre de séjour, Permesso di soggiorno, Permissiun da dimora	Front, back	Latin
UK	Driving License	Trwydded yrru	Front	Latin
UK	Paper Passport		Bio-data page	Latin
UK	Proof Of Age Card	CitizenCard	Front	Latin
UK	Residence Permit		Front, back	Latin
UK	Polycarbonate Passport		Bio-data page	Latin
Ukraine	Driving License	Посвідчення водія, Водительское удостоверение	Front	Cyrillic, Latin
Ukraine	ID Card	Паспорт громадянина України	Front, back	Cyrillic, Latin
Ukraine	Residence Permit	Посвідка на постійне проживання (ППП)	Front, back	Cyrillic, Latin
Ukraine	Polycarbonate Passport	Паспорт	Bio-data page	Latin
Ukraine	Temporary Residence Permit	Посвідка на тимчасове проживання	Front, back	Cyrillic, Latin

Supported identity documents (Latin America and the Caribbean)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Antigua and Barbuda	Driving License ^{BETA}		Front	Latin
Argentina	Alien ID	DNI para extranjeros	Front, back	Latin
Argentina	Driving License ^{BETA}	Licencia de Conducir	Front	Latin
Argentina	ID Card	Documento Nacional de Identidad (DNI)	Front, back	Latin
Argentina	Paper Passport	Pasaporte	Bio-data page	Latin
Bahamas	Driving License		Front	Latin
Bahamas	ID Card ^{BETA}	NIB Smart Card	Front	Latin
Barbados	ID Card ^{BETA}		Front, back	Latin
Bolivia	Driving License	Licencia para conducir	Front	Latin
Bolivia	ID Card	Cédula de identidad	Front, back	Latin
Bolivia	Minors ID	Cédula de identidad para menores	Front, back	Latin
Brazil	Consular Passport ^{BETA}	Passaporte	Bio-data page	Latin
Brazil	Driving License	Carteira Nacional de Habilitação (CNH)	Front, back	Latin
Brazil	ID Card ^{BETA}	Cédula de identidade	Front, back	Latin
Brazil	Paper Passport ^{BETA}	Passaporte	Bio-data page	Latin
Brazil, Rio De Janeiro	ID Card	Cédula de identidade	Front, back	Latin
Brazil, Rio Grande do Sul	ID Card ^{BETA}	Cédula de identidade	Front, back	Latin
Brazil, Sao Paulo	ID Card	Cédula de identidade	Front, back	Latin
Cayman Islands	Driving License ^{BETA}	Driver's license	Front	Latin
Chile	Alien ID	Cédula de identidad para extranjeros	Front, back	Latin
Chile	Driving License	Licencia de conducir	Front	Latin
Chile	ID Card	Cédula de Identidad	Front, back	Latin
Chile	Polycarbonate Passport	Pasaporte	Bio-data page	Latin
Columbia	Alien ID	Cédula de Extranjería (CE)	Front, back	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Columbia	Driving License	Licencia de Conducción	Front, back	Latin
Columbia	ID Card	Cédula Digital Colombiana, Cédula de Ciudadanía (CC)	Front, back	Latin
Columbia	Minors ID	Tarjeta de identidad Biométrica (Azul)	Front, back	Latin
Columbia	Polycarbonate Passport	Pasaporte	Bio-data page	Latin
Costa Rica	Driving License ^{BETA}	Licencia de conducir	Front	Latin
Costa Rica	ID Card	Cédula de identidad	Front, back	Latin
Cuba	ID Card ^{BETA}	Carné de Identidad	Front, back	Latin
Cuba	Paper Passport	Pasaporte	Bio-data page	Latin
Dominican Republic	Driving License ^{BETA}	Licencia de conducir	Front, back	Latin
Dominican Republic	ID Card	Cédula de Identidad y Electoral (CIE)	Front, back	Latin
Dominican Republic	Paper Passport	Pasaporte	Bio-data page	Latin
Ecuador	Driving License	Licencia de conducir	Front	Latin
Ecuador	ID Card	Cédula de Identidad, Cédula de Identidad Electrónica	Front, back	Latin
El Salvador	Driving License ^{BETA}	Licencia de conducir	Front, back	Latin
El Salvador	ID Card	Documento Único de Identidad (DUI)	Front, back	Latin
Guatemala	Consular ID	Tarjeta de Identificación Consular (TICG)	Front, back	Latin
Guatemala	Driving License	Licencia de conducir	Front, back	Latin
Guatemala	ID Card	Documento Personal de Identificación (DPI)	Front, back	Latin
Guatemala	Paper Passport	Pasaporte	Bio-data page	Latin
Haiti	Driving License	Permis de conduire	Front	Latin
Haiti	ID Card	Carte d'identification nationale (CIN), Kat Idantifikasyon Nasyonal	Front, back	Latin
Haiti	Paper Passport	Passeport, Paspò	Bio-data page	Latin
Honduras	Driving License ^{BETA}	Licencia de conducir	Front, back	Latin
Honduras	ID Card ^{BETA}	Tarjeta de identidad	Front, back	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Honduras	Paper Passport ^{BETA}	Pasaporte	Bio-data page	Latin
Jamaica	Driving License	Motor vehicle license, MV license	Front, back	Latin
Mexico	Consular ID ^{BETA}	Matrícula consular	Front, back	Latin
Mexico	Paper Passport ^{BETA}	Pasaporte	Bio-data page	Latin
Mexico	Professional DL ^{BETA}	Licencia Federal de Conductor	Front	Latin
Mexico	Professional ID ^{BETA}	Cédula Profesional	Front, back, vertical	Latin
Mexico	Residence Permit ^{beta}	Tarjeta de Residencia Temporal y Residencia Permanente	Front, back	Latin
Mexico	Polycarbonate Passport	Pasaporte	Bio-data page	Latin
Mexico	Voter ID	Credencial para votar	Front, back	Latin
Mexico, Aguascalientes	Driving License	Licencia de Conducir	Front, back, vertical	Latin
Mexico, Baja California	Driving License	Licencia de Conducir	Front, back, vertical	Latin
Mexico, Baja California Sur	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Campeche	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Chiapas	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Chihuahua	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Ciudad de Mexico	Driving License	Licencia de Conducir	Front, vertical	Latin
Mexico, Coahuila	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Colima	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Durango	Driving License	Licencia de Conducir	Front	Latin
Mexico, Guanajuato	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Guerrero Coquila	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Guerrero Juchitan	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Hidalgo	Driving License	Licencia de Conducir	Front, back, vertical	Latin
Mexico, Jalisco	Driving License	Licencia de Conducir	Front	Latin
Mexico, Mexico	Driving License	Licencia de Conducir	Front, back	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Mexico, Michoacan	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Morelos	Driving License	Licencia de Conducir	Front	Latin
Mexico, Nayarit	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Nuevo Leon	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Oaxaca	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Puebla	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Quintana Roo Cozumel	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Quintana Roo Solidaridad	Driving License	Licencia de Conducir	Front, back, vertical,	Latin
Mexico, San Luis Potosi	Driving License	Licencia de Conducir	Front	Latin
Mexico, Sinaloa	Driving License ^{BETA}	Licencia de Conducir	Front	Latin
Mexico, Sonora	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Tabasco	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Tamaulipas	Driving License	Licencia de Conducir	Front, back, vertical,	Latin
Mexico, Tlaxcala	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Veracruz	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Yucatan	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Zacatecas	Driving License	Licencia de Conducir	Front, back	Latin
Nicaragua	ID Card	Cédula de Identidad Ciudadana	Front, back	Latin
Panama	Driving License	Licencia de Conducir	Front	Latin
Panama	ID Card	Cédula de Identidad	Front	Latin
Panama	Residence Permit	Carné de Residente Permanente	Front	Latin
Panama	Temporary Residence Permit	Carné de Residencia Provisional	Front, back	Latin
Paraguay	Driving License	Licencia de Conducir	Front, back	Latin
Paraguay	ID Card	Cédula de Identidad Civil	Front, back	Latin
Peru	Driving License	Licencia de conducir	Front, back	Latin
Peru	ID Card	Documento Nacional de Identidad (DNI)	Front, back	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Peru	Minors ID ^{BETA}	Documento Nacional de Identidad (DNI) para menores	Front, back	Latin
Peru	Paper Passport	Pasaporte	Bio-data page	Latin
Puerto Rico	Driving License	Licencia de Conducir	Front	Latin
Puerto Rico	Voter ID ^{BETA}	Tarjeta de Identificación Electoral (TIE), Electoral Identification Card	Front	Latin
Saint Lucia	ID Card ^{BETA}		Front, back	Latin
Trinidad and Tobago	Driving License		Front	Latin
Trinidad and Tobago	ID Card		Front, back	Latin
Uruguay	ID Card	Cédula de Identidad	Front, back	Latin
Venezuela	Driving License	Licencia para conducir	Front	Latin
Venezuela	ID Card	Cédula de Identidad	Front	Latin
Venezuela	Polycarbonate Passport	Pasaporte	Bio-data page	Latin

Supported identity documents (Middle East and Africa)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Algeria	Driving License	رخصة القيادة	Front, back	Latin
Algeria	ID Card	Carte nationale d'identité, بطاقة الهوية الوطنية	Front, back	Latin
Algeria	Paper Passport	جواز السفر, Passeport	Bio-data page	Latin
Bahrain	ID Card	بطاقة الهوية, CPR Card	Front, back	Latin
Botswana	ID Card	Omang	Front, back	Latin
Burkina Faso	ID Card	Carte Nationale d'Identité Burkinabè (CNIB)	Front, back	Latin
Cameroon	ID Card	Carte Nationale d'Identité (CNI)	Front, back	Latin
Democratic Republic of the Congo	Driving License ^{BETA}	Permis de conduire (CONADEP)	Front, back	Latin
Egypt	Driving License ^{BETA}	رخصة القيادة	Front, back	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Egypt	ID Card	بطاقة تحقيق الشخصيّة	Front, back	Arabic, Latin
Egypt	Paper Passport ^{BETA}	جواز سفر	Bio-data page	Latin
Eswatini	Paper Passport		Bio-data page	Latin
Ghana	Driving License		Front	Latin
Ghana	ID Card	Ghana Card	Front, back	Latin
Ghana	Paper Passport		Bio-data page	Latin
Iran	Paper Passport ^{BETA}	گذرنامه	Bio-data page	Latin
Iraq	ID Card	البطاقة الوطنية، كارتى نیشتمانى	Front, back	Latin
Iraq	Paper Passport ^{BETA}	پاسپورت، جواز سفر	Bio-data page	Latin
Israel	Driving License	רשיון נהיגה	Front	Latin
Israel	ID Card	Tehudat Zehut, بطاقة هوية، תעודת זהות	Front, back	Latin
Israel	Paper Passport ^{BETA}	דרכון	Bio-data page	Latin
Ivory Coast	Driving License	Permis de conduire	Front	Latin
Ivory Coast	ID Card	Carte Nationale d'Identité (CNI)	Front, back	Latin
Jordan	Driving License ^{BETA}	رخصة القيادة	Front	Latin
Jordan	ID Card	بطاقة شخصية	Front, back	Arabic, Latin
Jordan	Paper Passport ^{BETA}	جواز سفر	Bio-data page	Latin
Kenya	ID Card	Kitambulisho	Front, back	Latin
Kenya	Polycarbonate Passport	Passport, Pasi	Bio-data page	Latin
Kuwait	Driving License	رخصة القيادة	Front, back	Latin
Kuwait	ID Card	بطاقة المدينية	Front, back	Latin
Kuwait	Resident ID	بطاقة المدينية	Front, back	Latin
Lebanon	ID Card	بطاقة الهوية	Front, back	Latin
Libya	Polycarbonate Passport	جواز سفر	Bio-data page	Latin
Mauritius	ID Card		Front, back	Latin
Morocco	Driving License	Permis de conduire, رخصة القيادة	Front, back	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Morocco	ID Card	Carte nationale d'identité, بطاقة التعريف الوطني	Front, back	Latin
Morocco	Paper Passport ^{BETA}	Passeport, جواز سفر	Bio-data page	Latin
Mozambique	Driving License ^{BETA}	Carta de Condução	Front	Latin
Mozambique	ID Card	Bilhete de Identidade (BI)	Front, back	Latin
Nigeria	Driving License		Front, back	Latin
Nigeria	ID Card	e-ID card	Front, back	Latin
Nigeria	Paper Passport		Bio-data page	Latin
Nigeria	Polycarbonate Passport ^{BETA}		Bio-data page	Latin
Nigeria	Voter ID	Permanent Voter Card (PVC)	Front, back	Latin
Oman	Driving License ^{BETA}	رخصة قيادة مركبة	Front, back	Latin
Oman	ID Card	بطاقة الهوية	Front, back	Latin
Oman	Resident ID	بطاقة مقيم	Front, back	Latin
Qatar	Driving License	رخصة القيادة	Front	Latin
Qatar	ID Card ^{BETA}	بطاقة إثبات شخصية	Front	Latin
Qatar	Paper Passport	جواز سفر	Bio-data page	Latin
Qatar	Residence Permit	تصريح الإقامة	Front, back	Latin
Rwanda	ID Card	Indangamuntu	Front	Latin
Saudi Arabia	Driving License	رخصة قيادة	Front	Latin
Saudi Arabia	ID Card	بطاقة الأحوال المدنية	Front, back	Latin
Saudi Arabia	Paper Passport	جواز سفر	Bio-data page	Latin
Saudi Arabia	Resident ID	هوية المقيم, Iqama	Front	Latin
Senegal	ID Card	Carte d'identité biométrique CEDEAO, Carte nationale d'identité	Front, back	Latin
South Africa	Driving License	Bestuurslisensie	Front	Latin
South Africa	ID Card	Smart ID card	Front, back	Latin
South Africa	ID Card ^{BETA}	Green barcoded ID book	Front, vertical	Latin
South Africa	Polycarbonate Passport	Passeport	Bio-data page	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Sudan	Polycarbonate Passport	جواز سفر	Bio-data page	Latin
Syria	Paper Passport	جواز سفر	Bio-data page	Latin
Tanzania	Driving License	Leseni ya udereva	Front	Latin
Tanzania	ID Card ^{BETA}	Kitambulisho cha Taifa, NIDA	Front, back	Latin
Tanzania	Voter ID ^{BETA}	Kadi ya mpiga kura, Voter Card	Front	Latin
Togo	ID Card	Permis de conduire	Front, back	Latin
Tunisia	Driving License	رخصة قيادة	Front	Latin
Tunisia	ID Card	بطاقة التعريف الوطنية	Front	Latin
Tunisia	Paper Passport	جواز سفر	Bio-data page	Latin
Turkey	Driving License	Sürücü belgesi	Front	Latin
Turkey	ID Card	Kimlik Kartı	Front, back	Latin
Turkey	Paper Passport	Pasaport	Bio-data page	Latin
Turkey	Residence Permit ^{BETA}	İkamet İzni	Front, back	Latin
Turkey	Polycarbonate Passport	Pasaport	Bio-data page	Latin
UAE	Driving License	رخصة القيادة	Front, back	Latin
UAE	ID Card	بطاقة الهوية	Front, back	Arabic, Latin
UAE	Paper Passport	جواز سفر	Bio-data page	Arabic, Latin
UAE	Resident ID	بطاقة الهوية الوطنية	Front, back	Arabic, Latin
Uganda	Driving License		Front	Latin
Uganda	ID Card		Front, back	Latin
Zimbabwe	ID Card	National registration card (NRC)	Front, back	Latin
Zimbabwe	Paper Passport		Bio-data page	Latin

Supported identity documents (North America)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Bermuda	Driving License ^{BETA}		Front	Latin
Canada	Citizenship Certificate ^{BETA}	Canada citizenship card, Carte de citoyenneté canadienne	Front, back	Latin
Canada	Paper Passport	Passport, Passeport	Bio-data page	Latin
Canada	Residence Permit	Permanent residence (PR) card, Carte de résident permanent	Front, back	Latin
Canada	Social Security Card ^{BETA}	Social insurance card (SIN card), Carte d'assurance sociale (Carte de NAS)	Front	Latin
Canada	Tribal ID	Certificate of Indian Status, Certificat de statut Indien	Front, back	Latin
Canada	Weapon Permit	Possession and Acquisition License (PAL), Permis de possession et d'acquisition	Front	Latin
Canada, Alberta	Driving License		Front, back	Latin
Canada, Alberta	ID Card		Front, back	Latin
Canada, British Columbia	Driving License		Front, back	Latin
Canada, British Columbia	Driver License, Public Services Card (Combined)		Front, back	Latin
Canada, British Columbia	ID Card		Front, back	Latin
Canada, British Columbia	Minors Public Services Card		Front, back	Latin
Canada, British Columbia	Public Services Card		Front, back	Latin
Canada Manitoba	Driving License		Front, back	Latin
Canada Manitoba	ID Card		Front, back	Latin
Canada, New Brunswick	Driving License	Permis de conduire	Front, back	Latin
Canada, Newfoundland and Labrador	Driving License		Front, back	Latin
Canada, Nova Scotia	Driving License		Front, back	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Canada, Nova Scotia	ID Card ^{BETA}		Front, back	Latin
Canada, Nova Scotia	Driving License		Front, back	Latin
Canada, Nova Scotia	ID Card ^{BETA}		Front, back	Latin
Canada, Ontario	Driving License		Front, back	Latin
Canada, Ontario	ID Card	Photo card	Front, back	Latin
Canada, Quebec	Driving License	Permis de conduire	Front, back	Latin
Canada, Saskatchewan	Driving License		Front, back	Latin
Canada, Saskatchewan	ID Card ^{BETA}		Front, back	Latin
Canada, Yukon	Driving License	Permis de conduire	Front, back	Latin
USA	Border Crossing Card	BCC	Front, back	Latin
USA	Global Entry Card		Front, back	Latin
USA	Green Card	Permanent resident card	Front, back	Latin
USA	Military ID	Common Access Card (CAC)	Front, back, vertical	Latin
USA	Nexus Card ^{BETA}		Front, back	Latin
USA	Paper Passport		Bio-data page	Latin
USA	Passport Card		Front, back	Latin
USA	Polycarbonate Passport		Bio-data page	Latin
USA	Social Security Card ^{BETA}		Front	Latin
USA	Veteran ID	VIC	Front	Latin
USA	Work Permit	Employment authorization document, EAD Card	Front, back	Latin
USA, Alabama	Driving License		Front, back, vertical	Latin
USA, Alabama	ID Card		Front, back, vertical	Latin
USA, Alaska	Driving License		Front, back	Latin
USA, Alaska	ID Card		Front, back	Latin
USA, Arizona	Driving License		Front, back, vertical	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
USA, Arizona	ID Card		Front, back, vertical	Latin
USA, Arkansas	Driving License		Front, back, vertical	Latin
USA, Arkansas	ID Card		Front, back, vertical	Latin
USA, California	Driving License		Front, back, vertical	Latin
USA, California	ID Card		Front, back, vertical	Latin
USA, Colorado	Driving License		Front, back, vertical	Latin
USA, Colorado	ID Card		Front, back	Latin
USA, Connecticut	Driving License		Front, back, vertical	Latin
USA, Connecticut	ID Card		Front, back	Latin
USA, Delaware	Driving License		Front, back, vertical	Latin
USA, District of Columbia	Driving License		Front, back, vertical	Latin
USA, District of Columbia	ID Card		Front, back, vertical	Latin
USA, Florida	Driving License		Front, back, vertical	Latin
USA, Florida	ID Card		Front, back, vertical	Latin
USA, Georgia	Driving License		Front, back, vertical	Latin
USA, Georgia	ID Card		Front, back, vertical	Latin
USA, Hawaii	Driving License		Front, back, vertical	Latin
USA, Hawaii	ID Card		Front, back	Latin
USA, Idaho	Driving License		Front, back, vertical	Latin
USA, Idaho	ID Card		Front, back	Latin
USA, Illinois	Driving License		Front, back, vertical	Latin
USA, Illinois	ID Card		Front, back, vertical	Latin
USA, Indiana	Driving License		Front, back	Latin
USA, Indiana	ID Card		Front, back	Latin
USA, Iowa	Driving License		Front, back, vertical	Latin
USA, Iowa	ID Card		Front, back, vertical	Latin
USA, Kansas	Driving License		Front, back, vertical	Latin
USA, Kansas	ID Card		Front, back, vertical	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
USA, Kentucky	Driving License		Front, back, vertical	Latin
USA, Kentucky	ID Card		Front, back, vertical	Latin
USA, Louisiana	Driving License		Front, back	Latin
USA, Maine	Driving License		Front, back, vertical	Latin
USA, Maine	ID Card		Front, back	Latin
USA, Maryland	Driving License		Front, back, vertical	Latin
USA, Maryland	ID Card		Front, back, vertical	Latin
USA, Massachusetts	Driving License		Front, back, vertical	Latin
USA, Massachusetts	ID Card		Front, back, vertical	Latin
USA, Michigan	Driving License		Front, back, vertical	Latin
USA, Michigan	ID Card		Front, back, vertical	Latin
USA, Minnesota	Driving License		Front, back, vertical	Latin
USA, Minnesota	ID Card		Front, back, vertical	Latin
USA, Missouri	Driving License		Front, back, vertical	Latin
USA, Missouri	ID Card		Front, back, vertical	Latin
USA, Montana	Driving License		Front, back	Latin
USA, Montana	ID Card		Front, back	Latin
USA, Nebraska	Driving License		Front, back, vertical	Latin
USA, Nebraska	ID Card		Front, back	Latin
USA, Nevada	Driving License		Front, back, vertical	Latin
USA, Nevada	ID Card		Front, back, vertical	Latin
USA, New Hampshire	Driving License		Front, back, vertical	Latin
USA, New Hampshire	ID Card ^{BETA}		Front, back	Latin
USA, New Jersey	Driving License		Front, back, vertical	Latin
USA, New Jersey	ID Card		Front, back, vertical	Latin
USA, New Mexico	Driving License		Front, back, vertical	Latin
USA, New Mexico	ID Card		Front, back	Latin
USA, New York	Driving License		Front, back, vertical	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
USA, New York	ID Card		Front, back, vertical	Latin
USA, New York City	ID Card		Front, back	Latin
USA, North Carolina	Driving License		Front, back, vertical	Latin
USA, North Carolina	ID Card		Front, back, vertical	Latin
USA, North Dakota	Driving License		Front, back, vertical	Latin
USA, North Dakota	ID Card ^{BETA}		Front, back	Latin
USA, Ohio	Driving License		Front, back, vertical	Latin
USA, Ohio	ID Card		Front, back, vertical	Latin
USA, Oklahoma	Driving License		Front, back, vertical	Latin
USA, Oklahoma	ID Card		Front, back, vertical	Latin
USA, Oregon	Driving License		Front, back, vertical	Latin
USA, Oregon	ID Card		Front, back	Latin
USA, Pennsylvania	Driving License		Front, back, vertical	Latin
USA, Pennsylvania	ID Card		Front, back, vertical	Latin
USA, Rhode Island	Driving License		Front, back, vertical	Latin
USA, Rhode Island	ID Card		Front, back	Latin
USA, South Carolina	Driving License		Front, back, vertical	Latin
USA, South Carolina	ID Card		Front, back, vertical	Latin
USA, South Dakota	Driving License		Front, back, vertical	Latin
USA, South Dakota	ID Card ^{BETA}		Front, back	Latin
USA Tennessee	Driving License		Front, back, vertical	Latin
USA Tennessee	ID Card		Front, back, vertical	Latin
USA, Texas	Driving License		Front, back, vertical	Latin
USA, Texas	ID Card		Front, back, vertical	Latin
USA, Texas	Weapon Permit	License to Carry a Handgun (LTC)	Front	Latin
USA, Utah	Driving License		Front, back, vertical	Latin
USA, Utah	ID Card		Front, back, vertical	Latin
USA, Vermont	Driving License		Front, back	Latin
USA, Virginia	Driving License		Front, back, vertical	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
USA, Virginia	ID Card		Front, back	Latin
USA, Washington	Driving License		Front, back, vertical	Latin
USA, Washington	ID Card		Front, back, vertical	Latin
USA, West Virginia	Driving License		Front, back	Latin
USA, Wisconsin	Driving License		Front, back, vertical	Latin
USA, Wisconsin	ID Card		Front, back	Latin
USA, Wyoming	Driving License		Front, back	Latin
USA, Wyoming	ID Card		Front, back	Latin

Supported identity documents (Oceania)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Australia	Paper Passport		Bio-data page	Latin
Australia, Australian Capital Territory	Driving License		Front	Latin
Australia, New South Wales	Driving License		Front	Latin
Australia, New South Wales	ID Card		Front	Latin
Australia, Northern Territory	Driving License ^{BETA}		Front, back	Latin
Australia, Northern Territory	Proof Of Age Card	NT Evidence of age card	Front, back	Latin
Australia, Queensland	Driving License		Front, back	Latin
Australia, South Australia	Driving License		Front, back	Latin
Australia, South Australia	Proof Of Age Card		Front	Latin
Australia, Tasmania	Driving License		Front, back	Latin
Australia, Victoria	Driving License		Front, back	Latin
Australia, Victoria	Proof Of Age Card		Front	Latin
Australia, Western Australia	Driving License		Front, back	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
New Zealand	Driving License		Front	Latin
New Zealand	Polycarbonate Passport	Uruwhenua	Bio-data page	Latin

Related Topics

[About ClearID Self-Service Kiosk](#) on page 241

Troubleshooting

Visit email notifications not received by visitors

If email notifications aren't received by visitors, check that the visit event request has been approved.

Cause

Visit email notifications aren't received because the visit event request wasn't approved.

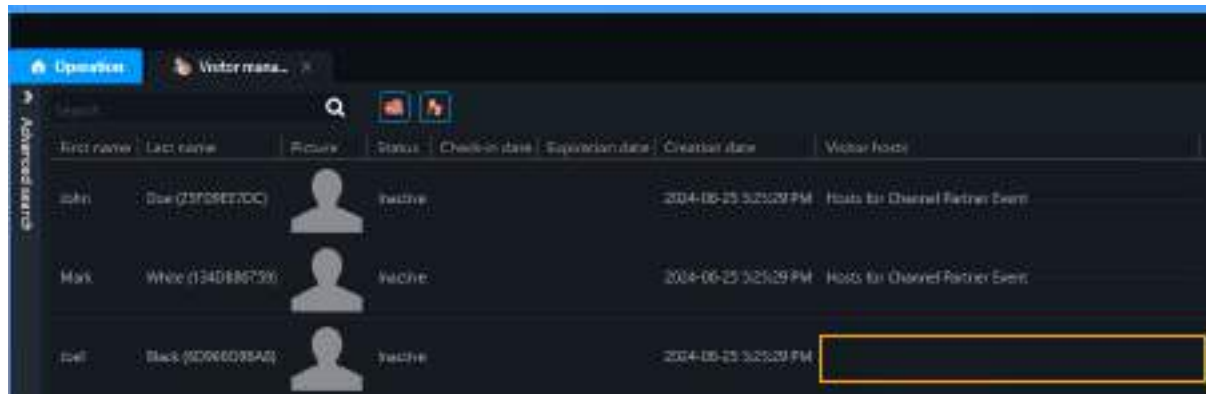
Solution

Review any visit event requests to identify the request waiting for approval:

1. Approve area access requests.
2. Approve visit events.

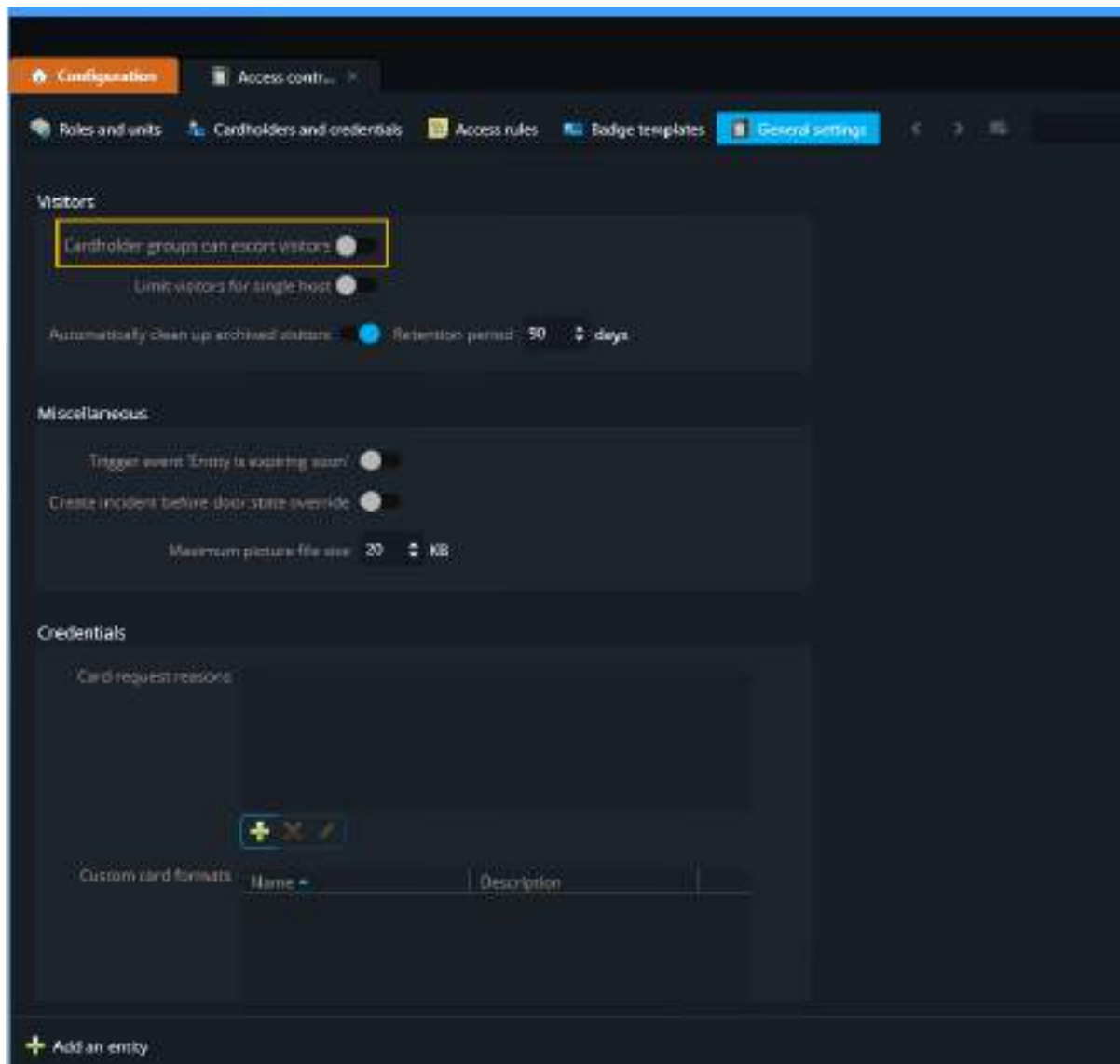
Visitor hosts fields in Genetec Operation are empty

If the **Visitor hosts** fields in Genetec™ Operation desktop are empty, then the **Cardholder groups can escort visitors** setting might not be configured correctly for Genetec ClearID™.



Cause

In the *Visitors* section of the *Access control* task, the **Cardholder groups can escort visitors** setting in Genetec™ Configuration desktop could be disabled (OFF).

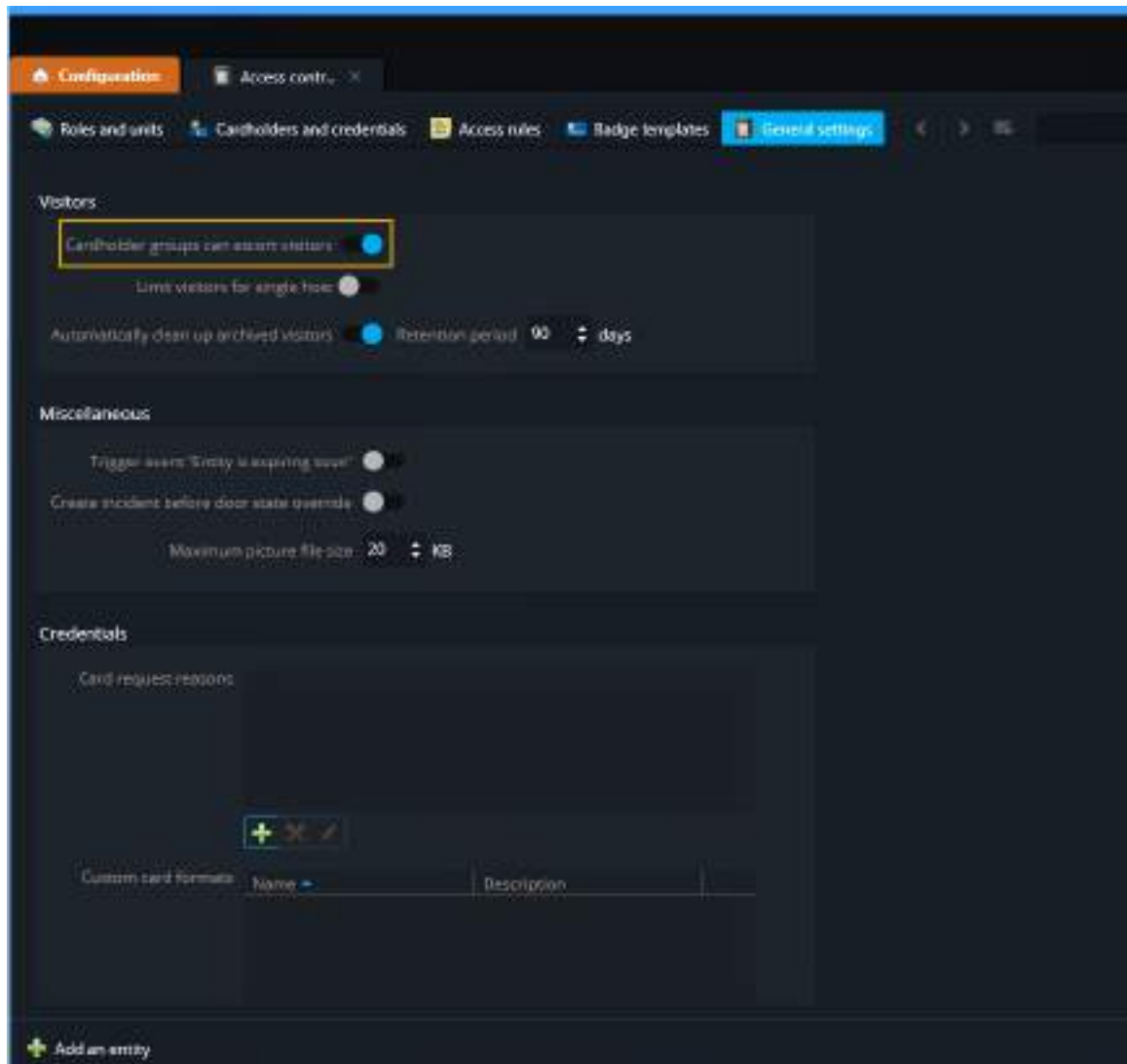


Solution

In the *Visitors* section of the *Access control* task, make sure that the **Cardholder groups can escort visitors** setting is enabled (ON).

1. From the Genetec Configuration desktop homepage, open the *Access control* task.
2. Click **General settings**.

- Click or slide the **Cardholder groups can escort visitors** option to the **ON** position.



- (Optional) In ClearID, create a new visit request to verify that the option is working as expected.
- (Optional) In Genetec Operation desktop, check that the **Visitor hosts** field contains host information.

Connectivity issues (One Identity Synchronization Tool)

If you encounter connectivity issues when using the Genetec ClearID™ One Identity Synchronization Tool, check your API integration or Azure AD application connection details.

To help you troubleshoot the issue, learn about the possible causes and their respective solutions.

Unable to connect to ClearID

Description: The synchronization tool is unable to connect to ClearID.

Solution: Review the One Identity *ConfigurationTool* logs.

1. Click , then click **Open logs folder**.

TIP: You can also open the *ConfigurationTool* logs manually here:

```
%ProgramData%\Genetec\OneIdentity\Logs\ConfigurationTool
```

2. Review the One Identity *ConfigurationTool* logs for error messages related to ClearID connectivity issues.
3. Check your API integration connection.
 - a. Click **Administration** > **Automation** and select your API integration.
 - b. Check that your API integration key and Client ID details are correct.
4. [Check your connection settings](#).

Unable to connect to Azure AD

Description: The synchronization tool is unable to connect to Azure Active Directory (Microsoft Entra ID).

Solution: Review the One Identity *ConfigurationTool* logs.

1. Click , then click **Open logs folder**.

TIP: You can also open the *ConfigurationTool* logs manually here:

```
%ProgramData%\Genetec\OneIdentity\Logs\ConfigurationTool
```

2. Review the One Identity *ConfigurationTool* logs for error messages related to Azure AD connectivity issues.
3. Check your [Azure AD application connection details](#).

Related Topics

[Synchronizing identities using One Identity](#) on page 191

Data synchronization issues (One Identity Synchronization Tool)

If you encounter connectivity issues when using the Genetec ClearID™ One Identity Synchronization Tool, check your service logs for errors. To help you troubleshoot the issue, learn about the possible causes and their respective solutions.

Missing data fields

Description: Data fields are missing.

Solution: Review the One Identity *Service* logs.

1. Click , then click **Open logs folder**.

TIP: You can also open the *ConfigurationTool* logs manually here:

```
%ProgramData%\Genetec\OneIdentity\Logs\Service
```

2. Review the One Identity *Service* logs for error messages related to missing data fields.
For more information about attribute fields, see [One Identity Synchronization Tool attribute fields](#).
3. [Check your Azure AD API permissions](#).

Missing name fields (first name, last name)

Description: Name fields (first name or last name) are missing.

Solution: Review the One Identity *Service* logs.

1. Click , then click **Open logs folder**.

TIP: You can also open the *ConfigurationTool* logs manually here:

```
%ProgramData%\Genetec\OneIdentity\Logs\Service
```

2. Review the One Identity *Service* logs for error messages related to name fields.
For more information about attribute fields, see [One Identity Synchronization Tool attribute fields](#).
3. [Check your Azure AD API permissions](#).

Missing email addresses

Description: Email address fields are missing.

Solution: Review the One Identity *Service* logs.

1. Click , then click **Open logs folder**.

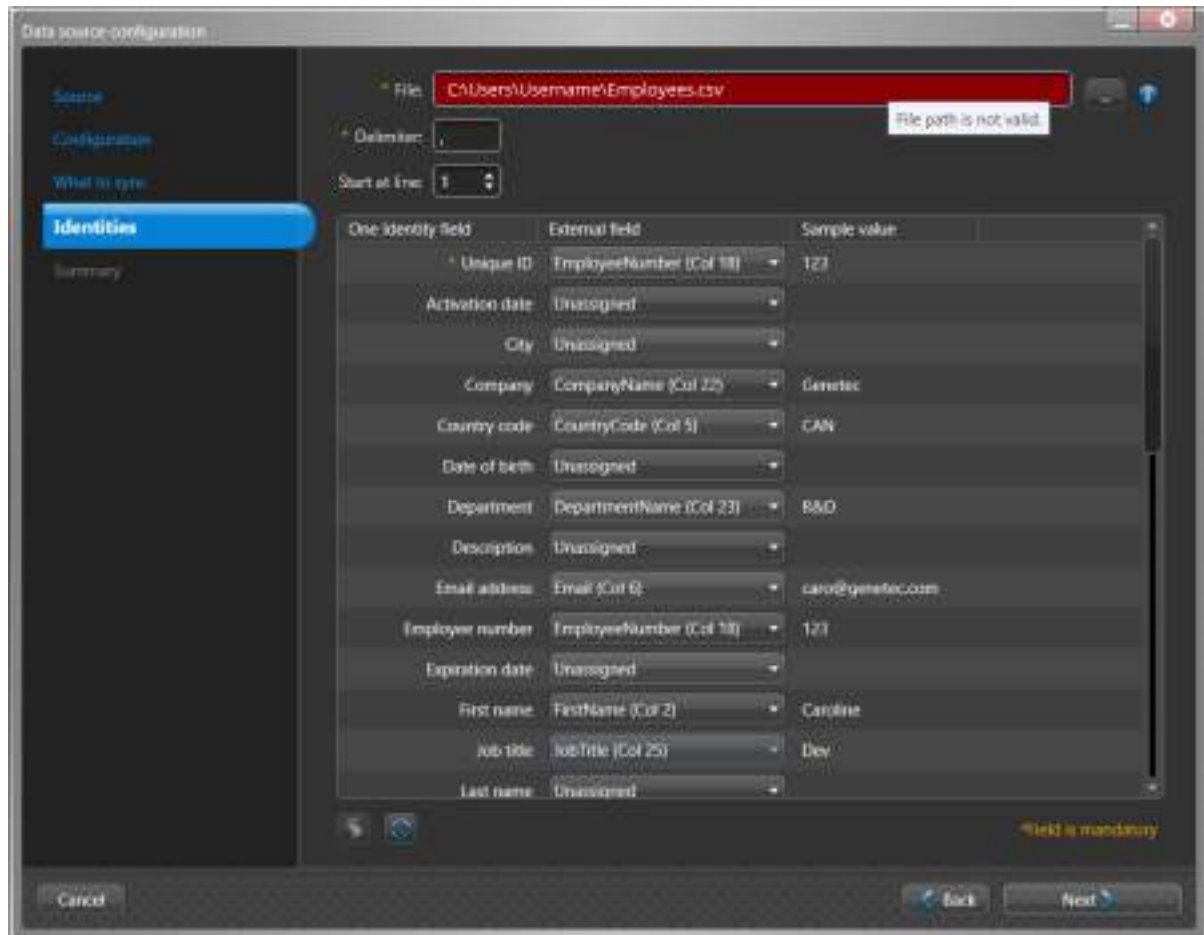
TIP: You can also open the *ConfigurationTool* logs manually here:

```
%ProgramData%\Genetec\OneIdentity\Logs\Service
```

2. Review the One Identity *Service* logs for error messages related to email address fields.
For more information about attribute fields, see [One Identity Synchronization Tool attribute fields](#).
3. [Check your Azure AD API permissions](#).

File path is not valid

Description: User permission issues encountered when using CSV files as the data source for **Identities** because the file path isn't valid.



Solution:

BEST PRACTICE: To avoid user permission issues when using CSV files with the ClearID One Identity Synchronization Tool, save your files to a C: or C:\temp folder location. Do not save your CSV files in user-controlled file or folder locations (c:\Users folders or desktop folder location) or you might encounter File path is not valid user permissions issues.

Related Topics

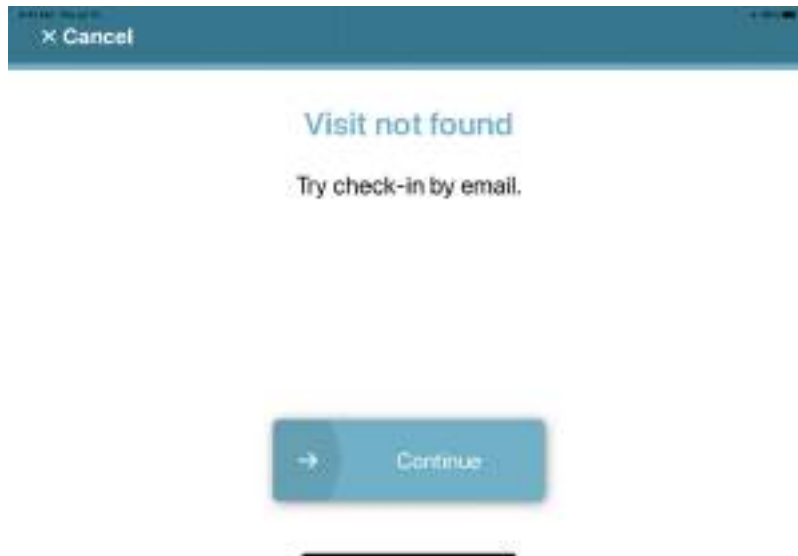
[Synchronizing identities using One Identity](#) on page 191

Self-Service Kiosk issues

If the Genetec ClearID™ Self-Service Kiosk check-in function or the kiosk doesn't work as expected, you can perform extra troubleshooting steps.

Visitor invite or visit event not found

Description: You don't see your visitor invite during check-in.



The *visit not found* issue can occur for various reasons:

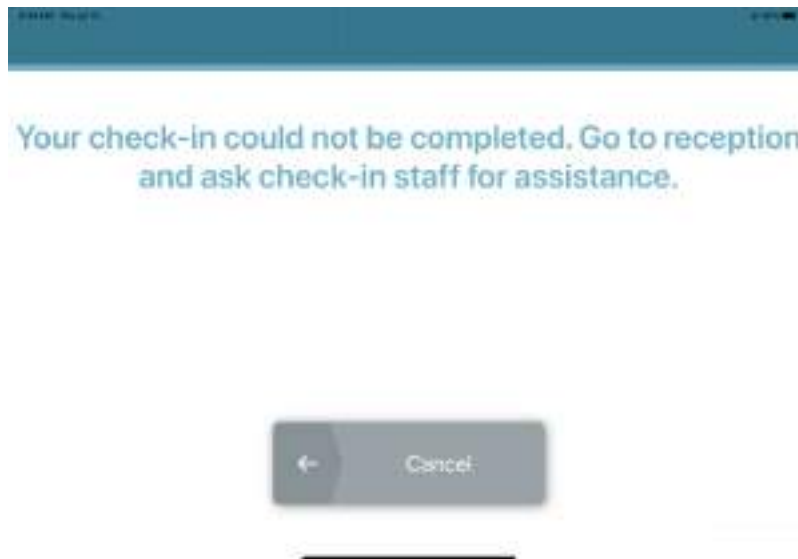
- Visitor check-in is too early (1hr+ before event start time).
- Visitor check-in is too late (1hr+ after event end time).
- Visitor isn't listed in visit event invite.
- The visitor name in the visit event invite contains a mistake or typo.

Solution:

- Check the visit event start and end times. Visitors can check in up to 1 hour before or after a visit event.
- Check visitor names listed in the visit event. Look for any visitors not listed or any mistakes in the visitor details.

Check-in could not be completed

Description: You're unable to complete your check-in.



Solution: Check your site and area settings. Self check-in can fail due to one or more of the following:

1. Visitor management isn't enabled for the site.
 - a. In Genetec ClearID™, click **Organization > Sites**.
 - b. Select your site and click **Visitor Management**.
 - c. Select **Enable visitor management for this site**.
 - d. Click **Save**.
2. Visitor management permissions for the site haven't been configured.
 - a. In ClearID, click **Organization > Sites**.
 - b. Select your site and click **Visitor Management > Permissions**.
 - c. Check identity permissions.
 - d. Modify permissions as required and click **Save**.
For example, Add role permissions or give all identities access to invite visitors.
3. Visitor management is enabled for the site but no areas are defined or there's no default area.
 - a. In ClearID, check visitor management is enabled for the area. (**Areas > Select an area > Visitor Management**).
 - b. Check the **Automatically add this area when creating visit requests** is enabled.
4. Visitor management is enabled for the site and there is at least one default area under that site. However, the host doesn't have the authority to invite visitors for that site.
 - a. Refer to [Step 2](#).
5. Site is set to approval required. Visit event approval workflow should be set to **No approval required**.
 - a. In ClearID, click **Organization > Sites** and select your site.
 - b. Click **Visitor Management**, then in *Advanced* section check **Visitor event approval workflow** is set to **No approval required**.

Camera errors

Description: The Self-Service Kiosk can occasionally encounter the following camera issues:

- Unable to initialize the front camera.
- An error was encountered while configuring the camera. Try again.

Solution: Check the following:

1. On the iPad, tap **Settings** and scroll down to the **Self-Service Kiosk** app then tap **Camera** to enable the camera.
2. On the iPad, tap **Settings** > **Privacy & Security** and check that the **Self-Service Kiosk** has access to the camera.

TIP: These settings might not be visible on your iPad if you have not used the Scan QR code function before. In this situation, you can try the following: Tap **Check-in** > **QR code**, then tap **Cancel** and try the previous solution steps again.

Self-Service Kiosk label printer issues

If the Genetec ClearID™ Self-Service Kiosk label printer isn't performing as expected, you can check the configuration, check the hardware, or perform extra troubleshooting steps.

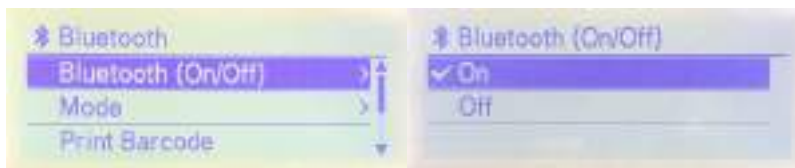
To help you troubleshoot Self-Service Kiosk label printer issues, refer to the possible causes and their respective solutions that follow.

No Bluetooth label printers detected

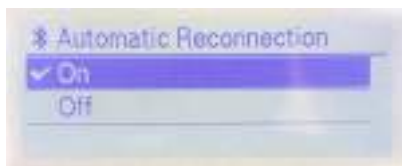
Description: No Bluetooth label printers were detected. A configuration or hardware issue can cause this situation to occur.

Solution:

1. Check that the printer is powered on and ready for use.
2. Check that Bluetooth is enabled on the label printer.
 - a. In the **Settings** menu, select **Bluetooth** > **Bluetooth (On/Off)** > **On** and press **OK**.



- b. In the **Settings** menu, select **Bluetooth** > **Automatic Reconnection (On/Off)** > **On** and press **OK**.



3. Check that Bluetooth is enabled in the ClearID Self-Service Kiosk mobile app.
4. Check that Bluetooth is enabled on the iPad.
5. Check that the printer is paired with the ClearID Self-Service Kiosk.
6. (Optional) [Perform a hard reset of the Self-Service Kiosk iPad](#).
 - a. [Configure your Self-Service Kiosk iPad](#).
 - b. Do one of the following:
 - [Configuring the Self-Service Kiosk label printer for Bluetooth mode \(Brother QL-820NWBc or QL-820NWB\)](#) on page 252.
 - [Configuring the Self-Service Kiosk label printer for Bluetooth mode \(Brother TD-4550DNWB\)](#) on page 261.
 - c. [Select a label printer](#).
 - d. [Print a test badge](#).

No Wi-Fi label printers detected

Description: No label printers were detected on the Wi-Fi network. A configuration or hardware issue can cause this situation to occur.

Solution:

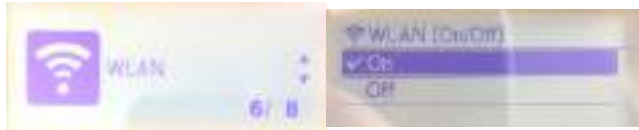
1. Check that the printer is powered on and ready for use.
2. Check that the Wi-Fi network is available.

The Wi-Fi network must be enabled for use and support the following:

- Bonjour - required for device search.
- SNMP - required to check printer status information.
- UDP or TCP Port 9100 - required to send print data.

3. Check that Wi-Fi is enabled on the label printer.

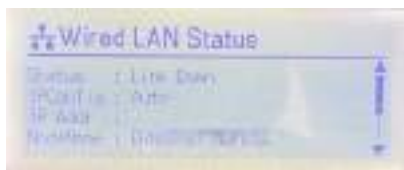
- a. In the **Settings** menu, select **WLAN > WLAN (On/Off) > On** and press **OK**.



4. Check that Wi-Fi is enabled on the iPad.
5. Check that the Self-Service Kiosk iPad and the label printer are on the same Wi-Fi network.
6. (Optional) [Perform a hard reset of the Self-Service Kiosk iPad](#).
 - a. [Configure your Self-Service Kiosk iPad](#).
 - b. Do one of the following:
 - [Configuring the Self-Service Kiosk label printer for Wi-Fi mode \(Brother QL-820NWBc, QL-820NWB, or QL-810W\)](#) on page 255.
 - [Configuring the Self-Service Kiosk label printer for Wi-Fi mode \(Brother TD-4550DNWB\)](#) on page 264.
 - c. [Select a label printer](#).
 - d. [Print a test badge](#).

No Ethernet label printers detected

Description: The label printer is showing the **Wired LAN Status** Link Down.



Solution:

1. Check that the printer is powered on and ready for use.
2. Check that the Wi-Fi function on the label printer is turned off.
 - a. From the label printer **Settings** menu, turn OFF **WLAN** (Wi-Fi).



3. Check that the Bluetooth function on the label printer is turned off.
 - a. In the **Settings** menu, select **Bluetooth > Bluetooth (On/Off) > Off** and press **OK**.



4. Check that the Ethernet network is available.
5. Check that Ethernet is enabled on the label printer.
 - a. In the **Settings** menu, select **Wired LAN > TCP/IP Settings > Auto** and press **OK**.



6. Check that the printer is connected to a LAN port and not to a WAN port (either on your router or your organizations network).
7. Verify that you're using the correct type of LAN cable.

BEST PRACTICE: Use a straight-through Category 5 (or greater) twisted-pair cable for 10BASE-T or 100BASE-TX Fast Ethernet Network.
8. (Optional) [Perform a hard reset of the Self-Service Kiosk iPad](#).
 - a. [Configure your Self-Service Kiosk iPad](#).
 - b. Do one of the following:
 - [Configuring the Self-Service Kiosk label printer for Ethernet mode \(Brother QL-820NWBc or QL-820NWB\)](#) on page 258.
 - [Configuring the Self-Service Kiosk label printer for Ethernet mode \(Brother TD-4550DNWB\)](#) on page 267.
 - c. [Select a label printer](#).
 - d. [Print a test badge](#).

Printing: A printing error has occurred. No paper in the printer.

Description: The label printer has run out of labels or has jammed.

Solution:

1. Check for the end of the label roll and replace if necessary:
 - Brother QL-820NWBc or QL-820NWB: DK Roll - 62mm Black (Brother Part No: DK-2205) or 62mm Red and Black (Brother Part No: DK-2251)
 - Brother TD-4550DNWB: RD Roll - 57mm Black (Brother Part No: RD001U1S)
2. Check the printer for a label jam or feed error.

Brother QL-820NWBc or QL-820NWB: A printing error has occurred

Description: The Brother QL-820NWBc or QL-820NWB label printer has encountered an unknown printing error.

**Solution:**

1. Check the [Label Printer Led Status indicators](#) FAQ database for possible causes.
2. Check the [Connecting to a Mobile Device](#) section for possible causes.
3. Check the FAQs & Troubleshooting [Printing](#) section for possible causes.

Brother QL-820NWBc or QL-820NWB: Printer turns off unexpectedly

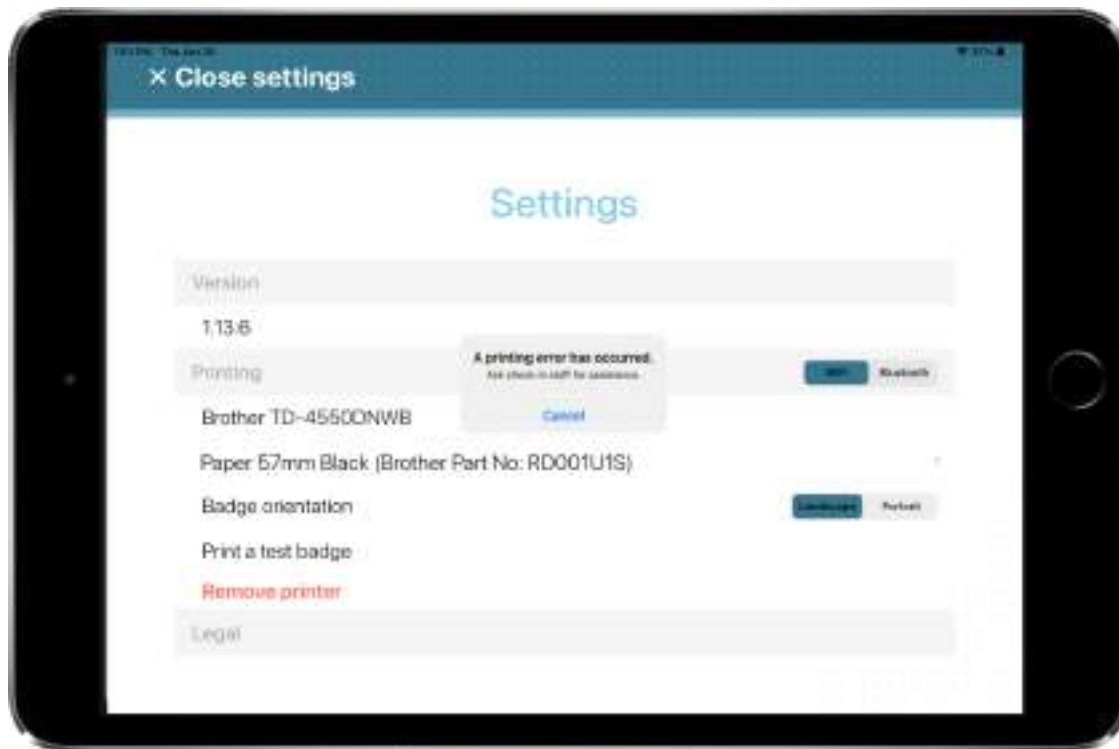
Description: The label printer turns off automatically at the same time every day.

Solution: Change the settings from the printer menu.

1. Press the **Menu** button.
2. Select **Settings** using the ▲ ▼ buttons, and then press the **OK** button.
3. Select **Auto Power Off** using the ▲ ▼ buttons, and then press the **OK** button.
4. Select **Adapter** using the ▲ ▼ buttons, and then press the **OK** button.
5. Select **Off** using the ▲ ▼ buttons, and then press the **OK** button.
6. (Optional) Also set the time to **Off** for [Li-ion battery], following the steps above.

Brother TD-4550DNWB: A printing error has occurred

Description: The Brother TD-4550DNWB label printer has encountered an unknown printing error.

**Solution:**

1. Check the [Label Printer Led Status indicators](#) FAQ database for possible causes.
2. Check the [Connecting to a Mobile Device](#) section for possible causes.
3. Check the FAQs & Troubleshooting [Printing](#) section for possible causes.

Brother TD-4550DNWB: The badge printout never arrives

Description: When printing a badge, the badges are sent to the printer but the printed badge never arrives.

Solution:

1. Check the printer LCD display to confirm you aren't in a configuration or settings menu.
NOTE: Leaving the printer in a configuration or settings menu can cause badge printing to be paused until you complete your changes.
2. If you left the printer in a configuration or settings menu, press the **Menu** button or use the printer controls to return to the homepage.

After returning to the homepage, badge printing should resume as normal.

Brother TD-4550DNWB: Badges don't print as expected

Description: The label printer prints a partial label or label orientation appears to be messed up. For example, in some situations the printer can print half a badge or print across two labels.

Solution:

1. Before printing any badges, check your label alignment and orientation.



IMPORTANT: The first label must be aligned with the front edge of the printer to ensure correct printing. Make sure that none of the labels have advanced past the front edge of the printer before printing. The printer only detects the label edges automatically after printing the first label, if the first label is misaligned badge printing issues can occur.

For more information about how to load labels or sensor positioning for different label types, see [Load the RD roll](#) and [Check the Sensor Position](#) in the Brother online printer documentation.

Related Topics

[Resetting the Self-Service Kiosk mobile app](#) on page 280

[Firewall ports](#) on page 11



Genetec ClearID™ User Guide

Date: 2025-08-12

<https://techdocs.genetec.com>
Contact Us | Privacy Policy | Terms of Use © 2013-2020 Genetec Inc.

1. About ClearID

- 1.1. What is ClearID?
- 1.2. About ClearID architecture
 - 1.2.1. ClearID subprocessors list
- 1.3. About ClearID information security
- 1.4. How is ClearID different from traditional access control systems?
- 1.5. About workflows in ClearID
- 1.6. How the ClearID plugin works with Security Center
- 1.7. Integration overview for the ClearID plugin
- 1.8. Supported features list for ClearID
- 1.9. Supported languages in ClearID
- 1.10. ClearID terminology
- 1.11. ClearID videos
- 1.12. About reports in ClearID
- 1.13. Logging on to ClearID
- 1.14. Logging off from ClearID
- 1.15. Enabling preview features in ClearID
- 1.16. Disabling preview features in ClearID
- 1.17. Customizing portal branding in ClearID
- 1.18. Customizing help menu links in ClearID

2. What's new

- 2.1. What's new in ClearID
- 2.2. Previous features and enhancements in ClearID

3. Deployment preparation

- 3.1. License options for ClearID system integration
- 3.2. Compatibility for ClearID
- 3.3. System requirements for ClearID
- 3.4. Firewall ports used in ClearID
- 3.5. Supported devices for ClearID
- 3.6. ClearID Best practices
 - 3.6.1. Best practices for setting up ClearID for a new Synergis system
 - 3.6.2. Best practices for setting up ClearID with an existing Synergis system

4. ClearID plugin

- 4.1. About ClearID plugin for Security Center
- 4.2. About cardholder and identity relationships
- 4.3. Downloading and installing the ClearID plugin
- 4.4. Creating the ClearID plugin role
- 4.5. Connecting Security Center to ClearID
 - 4.5.1. Reviewing cardholders and identities information in ClearID
 - 4.5.2. Adding a system to ClearID
 - 4.5.3. Downloading an activation file for ClearID
 - 4.5.4. Configuring connection settings for ClearID
- 4.6. Granting user privileges for the ClearID plugin
- 4.7. About ClearID system states
- 4.8. About custom fields in ClearID
 - 4.8.1. Modifying ClearID custom fields in Config Tool
 - 4.8.2. Custom fields relationships

5. Managing identities and users

- 5.1. Creating identities in ClearID
- 5.2. Identity fields in ClearID
- 5.3. About custom identity fields in ClearID
- 5.4. Creating custom identity fields in ClearID
- 5.5. Granting additional permissions for identities and roles in ClearID
- 5.6. Granting additional permissions for supervisors in ClearID
- 5.7. Viewing additional permissions in ClearID
 - 5.7.1. Modifying additional permissions in ClearID
- 5.8. Viewing identities in ClearID
- 5.9. Modifying identities in ClearID
- 5.10. Deleting identities in ClearID
- 5.11. Synchronizing ClearID identity pictures with Security Center
- 5.12. About webhooks in ClearID
- 5.13. Creating webhooks in ClearID
 - 5.13.1. Modifying webhooks in ClearID
- 5.14. Viewing webhook logs in ClearID
- 5.15. Granting access to the ClearID web portal
 - 5.15.1. Granting user access to the ClearID web portal
 - 5.15.2. Granting administrator access to the ClearID web portal

- 5.16. Viewing your profile in ClearID
 - 5.16.1. Configuring your ClearID portal theme preferences
- 5.17. Viewing your site and area access in ClearID
- 5.18. Setting request visibility for users in ClearID
- 5.19. About access request workflow in ClearID
- 5.20. Requesting access in ClearID
- 5.21. Adding supervisors manually in ClearID
- 5.22. Viewing direct reports in ClearID
- 5.23. Managing direct reports in ClearID
- 5.24. Transferring direct reports in ClearID
- 5.25. About direct reports report in ClearID
- 5.26. Resetting user passwords in ClearID
- 5.27. About email notifications in ClearID
 - 5.27.1. Customizing the email banner for sites in ClearID
 - 5.27.2. Configuring email notification preferences in ClearID (administrator)
 - 5.27.3. Configuring your ClearID email notification preferences
- 5.28. About delegation in ClearID
- 5.29. Delegating ClearID tasks to another user
- 5.30. About user activity report in ClearID
- 5.31. Viewing a user activity report in ClearID
- 5.32. User levels in ClearID
- 5.33. About identity request workflow in ClearID
- 5.34. Creating an identity template in ClearID
 - 5.34.1. Modifying an identity template in ClearID
- 5.35. Requesting identities in ClearID
 - 5.35.1. Requesting an identity in ClearID
 - 5.35.2. Requesting multiple identities using a CSV import in ClearID
- 5.36. Canceling identity requests in ClearID
- 5.37. Approving identity requests in ClearID
 - 5.37.1. Modifying an identity request in ClearID
- 5.38. About identity requests report in ClearID
- 5.39. Checking the status of identity requests in ClearID

6. Credential synchronization

- 6.1. Configuring credential replication in ClearID
- 6.2. Viewing credential synchronization logs in ClearID
- 6.3. Forcing credential synchronization in ClearID

7. Managing sites

- 7.1. About sites in ClearID
- 7.2. Creating sites in ClearID
 - 7.2.1. Adding site owners in ClearID
 - 7.2.2. Enabling visitor management for sites in ClearID
 - 7.2.2.1. Viewing sites where a user can invite visitors
- 7.3. Modifying sites in ClearID
- 7.4. Setting a maximum duration for site access in ClearID
- 7.5. Configuring access request documents for sites in ClearID
- 7.6. Customizing email notifications for sites in ClearID
 - 7.6.1. Customizing ClearID email notification branding
- 7.7. About access reviews in ClearID
- 7.8. Setting up automatic expiration for access reviews
- 7.9. Setting up area access reviews in ClearID
 - 7.9.1. Scheduling area access reviews in ClearID
- 7.10. Setting up identity access reviews in ClearID
 - 7.10.1. Scheduling identity access reviews in ClearID
- 7.11. Modifying access reviews in ClearID
- 7.12. About access reviews report in ClearID
- 7.13. Checking the status of access reviews in ClearID
- 7.14. Completing an area access review (site owner) in ClearID
- 7.15. Completing an area access review (area manager or role manager) in ClearID
- 7.16. Completing an identity access review (supervisor) in ClearID
- 7.17. Generating an access review summary in ClearID
- 7.18. About access requests report in ClearID
- 7.19. Checking the status of access requests in ClearID
- 7.20. About site activity report in ClearID
- 7.21. Viewing a site activity report in ClearID
- 7.22. About site and area owners report in ClearID
- 7.23. Viewing a site and area owners report in ClearID

8. Managing areas

- 8.1. About areas in ClearID

- 8.2. Creating areas in ClearID
 - 8.2.1. Adding doors to areas in ClearID
 - 8.2.2. Enabling visitor management for areas in ClearID
 - 8.2.3. About nested areas in Security Center
 - 8.2.4. Granting access to areas in Security Center automatically
- 8.3. Adding area owners and managers in ClearID
- 8.4. Adding schedules to an area in ClearID
- 8.5. Configuring access request documents for areas in ClearID
- 8.6. Granting access to an area in ClearID
- 8.7. Reviewing area access in ClearID
- 8.8. Approving area access requests in ClearID
- 8.9. Rejecting area access requests in ClearID
- 8.10. Creating exceptions to the access request approval workflow in ClearID

9. Managing visitors

- 9.1. About visit request workflow in ClearID
- 9.2. About visit request watchlist workflow in ClearID
- 9.3. Inviting visitors in ClearID
 - 9.3.1. Inviting visitors manually in ClearID
 - 9.3.2. Inviting visitors using a CSV import in ClearID
 - 9.3.3. SMS alerts in ClearID
- 9.4. Reviewing visit events in ClearID
- 9.5. About visit event logs in ClearID
- 9.6. Viewing visit event logs in ClearID.
- 9.7. Copying a visit event in ClearID
- 9.8. Modifying visit events in ClearID
- 9.9. Approving visit event requests in ClearID
- 9.10. Adding ClearID visit events to your calendar
- 9.11. About visitors report in ClearID
- 9.12. Viewing a visitors report in ClearID
- 9.13. QR codes as a credential for visitors in ClearID
 - 9.13.1. Importing a custom card format (QR code credential) in Synergis
 - 9.13.2. Enabling QR code credentials for visitors in ClearID
 - 9.13.3. Configuring Qscan devices for ClearID
 - 9.13.3.1. Connecting a Qscan barcode reader to a Mercury Controller for ClearID
 - 9.13.3.2. Configuring Qscan barcode reader to support 40-bit hexadecimal QR codes for ClearID
 - 9.13.4. Configuring STid devices for ClearID
 - 9.13.4.1. About STid QR code readers in ClearID
 - 9.13.4.2. Creating an STid QR code reader configuration for ClearID
 - 9.13.4.3. Transferring your reader configuration to your STid QR code reader for ClearID
 - 9.13.5. Automating visitor access and check-in using a macro in Security Center

10. Managing visitor watchlists

- 10.1. About watchlists in ClearID
- 10.2. Adding watchlist managers in ClearID
- 10.3. Adding watchlists in ClearID
 - 10.3.1. Adding an individuals watchlist entry in ClearID
 - 10.3.2. Adding a companies watchlist entry in ClearID
 - 10.3.3. Importing watchlist entries from a file in ClearID
 - 10.3.4. Exporting watchlist entries to a file in ClearID
 - 10.3.5. Testing watchlist entries in ClearID
 - 10.3.6. Deleting watchlist entries in ClearID
- 10.4. Modifying watchlists in Genetec ClearID
- 10.5. Deleting watchlists in Genetec ClearID
- 10.6. Screening visitors manually in ClearID
- 10.7. Unblocking visitors blocked by a watchlist in ClearID

11. Role-based access control

- 11.1. About role-based access control in ClearID
- 11.2. Adding roles in ClearID
- 11.3. Configuring role managers in ClearID
- 11.4. Configuring role-based access control policies in ClearID
 - 11.4.1. Scenario 1: Adding employees to an IT role in ClearID
 - 11.4.2. Scenario 2: Adding contractors to a certified contractor engineering role in ClearID
 - 11.4.3. Scenario 3: Adding employees to an ADA personnel role in ClearID
- 11.5. Adding custom provisioning attributes to an identity in ClearID
- 11.6. Adding role members in ClearID
- 11.7. About role activity report in ClearID
- 11.8. Viewing a role activity report in ClearID

12. Connecting to other systems

- 12.1. Authenticating your connection with ClearID
- 12.2. Setting up data synchronization
- 12.3. Synchronizing identities using an API in ClearID
 - 12.3.1. About the ClearID API
- 12.4. Synchronizing identities using the SCIM integration in ClearID
 - 12.4.1. About the SCIM standard in ClearID
 - 12.4.2. About Microsoft Entra ID attribute fields in Microsoft Azure

- 12.4.3. Configuring the SCIM integration in ClearID
 - 12.4.3.1. Generating a SCIM key in ClearID
 - 12.4.3.2. Creating an enterprise application in Microsoft Azure
 - 12.4.3.3. Connecting your ClearID SCIM integration to Microsoft Entra ID
 - 12.4.3.4. Disabling Microsoft Entra ID groups setting in Microsoft Azure
 - 12.4.3.5. Configuring Microsoft Entra ID user settings in Microsoft Azure
 - 12.4.3.6. Configuring the ClearID SCIM integration synchronization settings in Microsoft Azure
- 12.4.4. Resetting SCIM integration identity data in ClearID
- 12.4.5. Reviewing the SCIM integration synchronization status in Microsoft Azure

12.5. Synchronizing identities using One Identity Synchronization Tool in ClearID

- 12.5.1. About the ClearID One Identity Synchronization Tool
- 12.5.2. About ClearID One Identity Synchronization Tool attribute fields
- 12.5.3. About the Azure web app for ClearID One Identity Synchronization Tool
- 12.5.4. Installing the ClearID One Identity Synchronization Tool
 - 12.5.4.1. Uninstalling the ClearID One Identity Synchronization Tool
 - 12.5.4.2. Upgrading the ClearID One Identity Synchronization Tool
- 12.5.5. Configuring the ClearID One Identity Synchronization Tool
 - 12.5.5.1. Configuring connection settings for the ClearID One Identity Synchronization Tool
 - 12.5.5.2. Configuring the data source for Azure AD synchronization in the ClearID One Identity Synchronization Tool
 - 12.5.5.3. Configuring the data source for Database synchronization in the ClearID One Identity Synchronization Tool
 - 12.5.5.4. Configuring the data source for File synchronization in the ClearID One Identity Synchronization Tool
 - 12.5.5.5. Configuring synchronization settings in the ClearID One Identity Synchronization Tool
- 12.5.6. Reviewing synchronization status for the ClearID One Identity Synchronization Tool
- 12.5.7. About ClearID One Identity Synchronization Tool logs
- 12.5.8. Viewing the ClearID One Identity Synchronization Tool logs
- 12.5.9. Updating existing identities from an external data source using ClearID One Identity Synchronization Tool

12.6. Synchronizing identities using LDAP in ClearID

- 12.6.1. About ClearID LDAP Synchronization Agent
- 12.6.2. LDAP attributes to ClearID attribute mappings
- 12.6.3. Configuring the ClearID LDAP Synchronization Agent

13. Visitor management devices

13.1. About ClearID Self-Service Kiosk

- 13.1.1. About ClearID Self-Service Kiosk check-in
- 13.1.2. About ClearID Self-Service Kiosk Self registration

13.2. Configuring the ClearID Self-Service Kiosk iPad

- 13.2.1. Customizing the ClearID Self-Service Kiosk configuration
- 13.2.2. Customizing the ClearID Self-Service Kiosk visitor badge logo
- 13.2.3. Adding visitor compliance documents to the ClearID Self-Service Kiosk
- 13.2.4. Activating badge reprinting for the ClearID Self-Service Kiosk
- 13.2.5. Disabling visitor photo during ClearID Self-Service Kiosk check-in
- 13.2.6. Activating visitor photo retention in ClearID

13.3. About ClearID mobile operator check-in

13.4. Configuring ClearID mobile operator check-in

13.5. Configuring the ClearID Self-Service Kiosk label printer (Brother QL-820NWBc, QL-820NWB, or QL-810W)

- 13.5.1. Configuring the ClearID Self-Service Kiosk label printer for Bluetooth mode (Brother QL-820NWBc or QL-820NWB)
- 13.5.2. Configuring the ClearID Self-Service Kiosk label printer for Wi-Fi mode (Brother QL-820NWBc, QL-820NWB, or QL-810W)
- 13.5.3. Configuring the ClearID Self-Service Kiosk label printer for Ethernet mode (Brother QL-820NWBc or QL-820NWB)

13.6. Configuring the ClearID Self-Service Kiosk label printer (Brother TD-4550DNWB)

- 13.6.1. Configuring the ClearID Self-Service Kiosk label printer for Bluetooth mode (Brother TD-4550DNWB)
- 13.6.2. Configuring the ClearID Self-Service Kiosk label printer for Wi-Fi mode (Brother TD-4550DNWB)
- 13.6.3. Configuring the ClearID Self-Service Kiosk label printer for Ethernet mode (Brother TD-4550DNWB)

13.7. Selecting a ClearID Self-Service Kiosk label printer

13.8. Printing a test badge from the ClearID Self-Service Kiosk

13.9. Resetting the ClearID Self-Service Kiosk mobile app

13.10. ClearID Self-Service Kiosk options

- 13.10.1. ClearID Self-Service Kiosk floor stand
- 13.10.2. ClearID Self-Service Kiosk floor stand printer shelf
- 13.10.3. ClearID Self-Service Kiosk tabletop stand

13.11. Identity document types in ClearID

14. Troubleshooting

- 14.1. Plugin installed, but missing from Security Desk and Config Tool
- 14.2. Plugin role could not find file with certificate
- 14.3. Custom fields not displayed in Security Desk
- 14.4. No active account found for user
- 14.5. Visit email notifications not received by visitors
- 14.6. Visitor hosts fields in Security Desk are empty
- 14.7. ClearID One Identity Synchronization Tool connectivity issues
- 14.8. ClearID One Identity Synchronization Tool data synchronization issues
- 14.9. ClearID Self-Service Kiosk issues
- 14.10. ClearID Self-Service Kiosk label printer issues

1 | About ClearID

1.1 | What is ClearID?

Genetec ClearID™ is a smarter way to manage physical access using a self-service solution for Synergis™. Using ClearID, you can take control of access and compliance by using a rule-based approach through a web-based interface.

- You can access the system from any standard browser. All data and files that are imported to the system are automatically encrypted.
- The ClearID system is also integrated with Active Directory. This integration means that organizations can use their existing Active Directory service to authenticate users and manage system access.

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

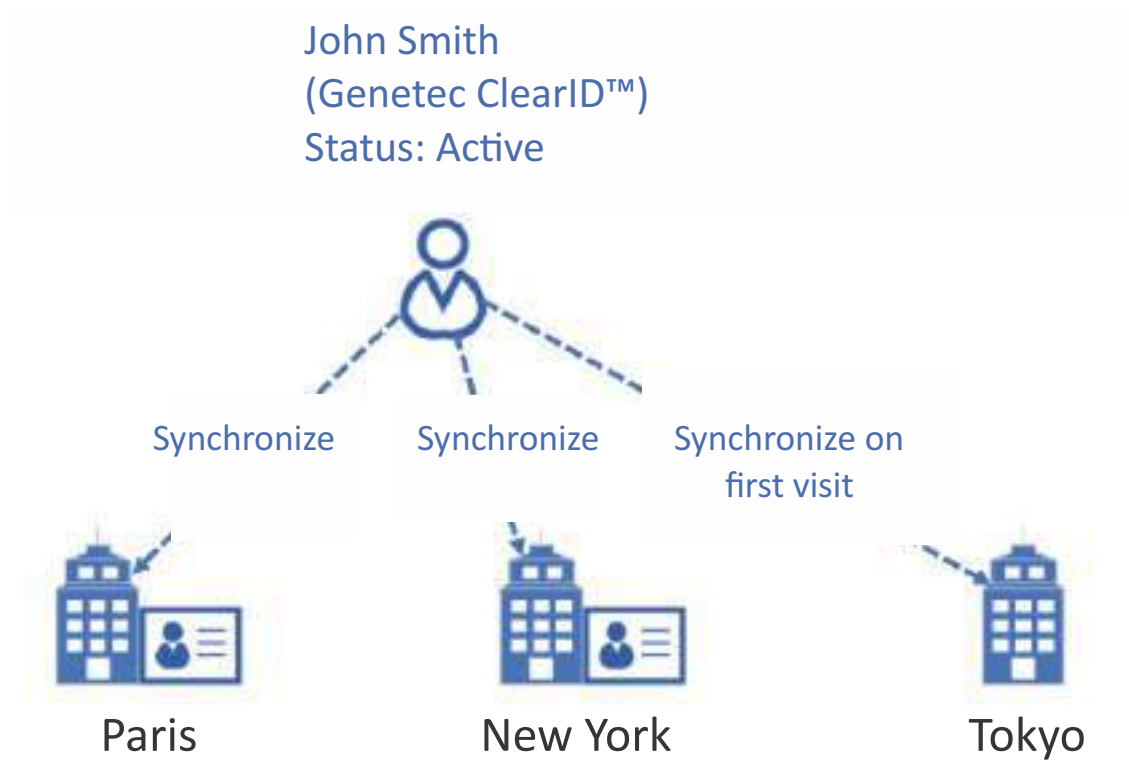
For a complete product description, visit the [ClearID](#) product page.

Advantages of the ClearID system

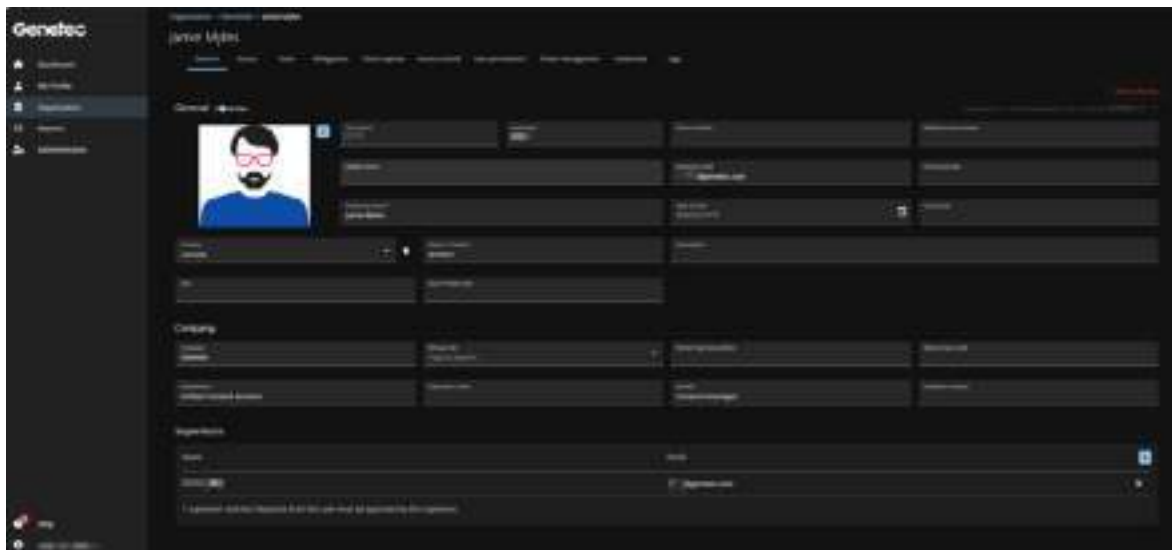
- Improve the flow of people by using the self-service solution to manage physical access.
- Reduce the risk of security breaches by simplifying access rights management.
- Standardize and automate security policies for onboarding, offboarding, access requests, and issuing credentials for multiple independent sites.
- Connect to and enhance your existing physical security system.
- Benefit from an off-the-shelf approach with faster deployment and fewer integrations to maintain.
- Maintain less infrastructure by using the distributed cloud-based approach.
- Increase efficiency and compliance with internal and external regulations, such as GDPR and export control screening.

One identity

ClearID uses one single identity to synchronize the access information for multiple independent sites managed using different instances of Synergis.



To minimize the personal information replicated in each local access control system, ClearID automatically creates the cardholder only when someone requests a site visit for the first time.



After access is granted to a new site, the system automatically synchronizes all the permanent credentials linked to the Identity. If the corporation shares the same card technology for different sites, the badge works without any manual interventions at the new site.

When an identity is deactivated in ClearID, the cardholder is deactivated. The identity is automatically synchronized to all cardholders linked to all the different areas in all sites. The credentials remain active in Security Center, but access is automatically denied because the cardholder is inactive.

Browse

- [ClearID videos](#)

Browse

- [ClearID Technical Brochure \(8 pages\)](#)
- [ClearID - Product page](#)
- [ClearID - Portfolio page](#)
- [Genetec Compliance Portal](#)

1.2 | About ClearID architecture

Genetec ClearID™ offers United States-only, European-only, Canadian-only, or Australian-only location options for data centers. Each option allows synchronization between local sites. The web application modules perform tasks or share data between the authoritative sources, ClearID, and the endpoints.

IMPORTANT: Transferring or copying a customer account from one instance to another isn't supported.

USA distributed architecture

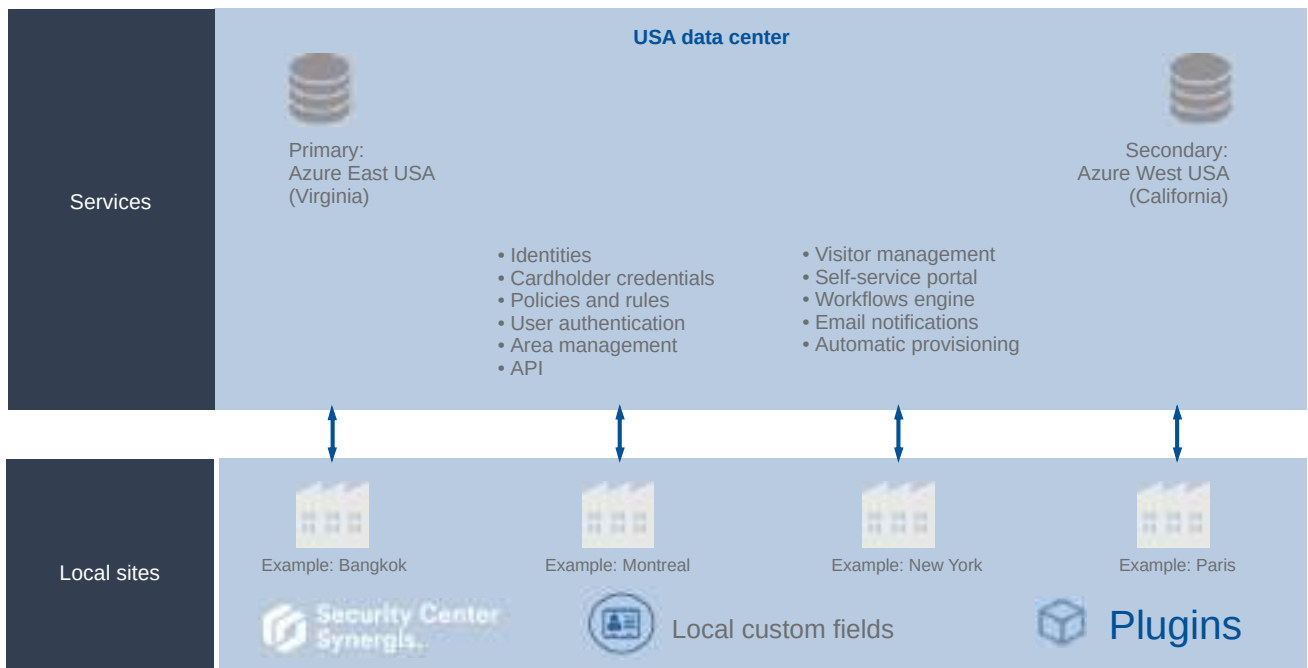
The following diagram illustrates the USA distributed solution. The diagram shows what data is stored, where data is stored, and how data flows between the local sites and the regional services.

NOTE: Regional services data is stored in the cloud.

ClearID takes advantage of the following:

- Multiple Azure data centers to minimize the risk of downtime.
- Encrypted employee data to minimize the risk of data theft.
- Geo-localized data to maintain less infrastructure and provide an optimized approach for data flow performance.

Genetec ClearID™ USA only architecture



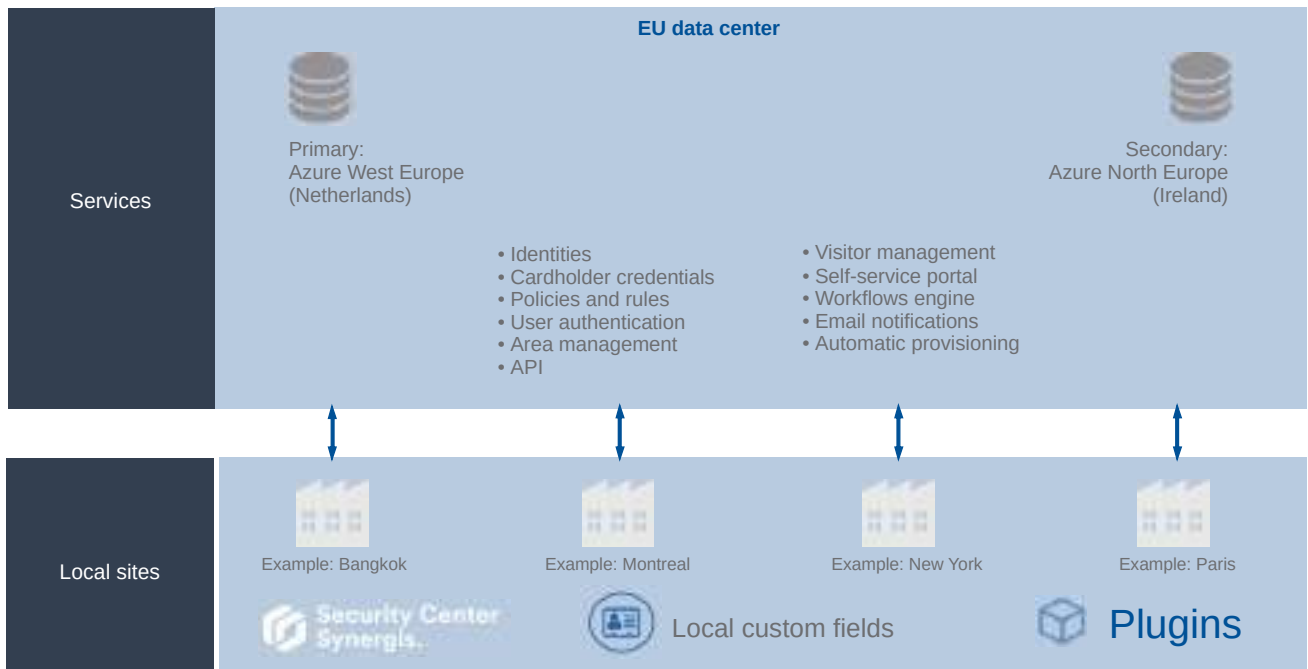
NOTE: ¹For more information about which data centers are used in the regional deployments, see the *Microsoft Corporation* entry in the ClearID section of the Genetec Subprocessors list.

For visitors, the relevant guest information is stored with the visit event information. This information is then transferred to the Security Center managing the site visited.

Europe only architecture

The following diagram illustrates the Europe-only solution where data is stored in European data centers. For example, when customers or company policies require data to be stored in European data centers.

Genetec ClearID™ Europe only architecture



NOTE: You can also choose from Canada-only and Australia-only data storage solutions.

Canadian data centers

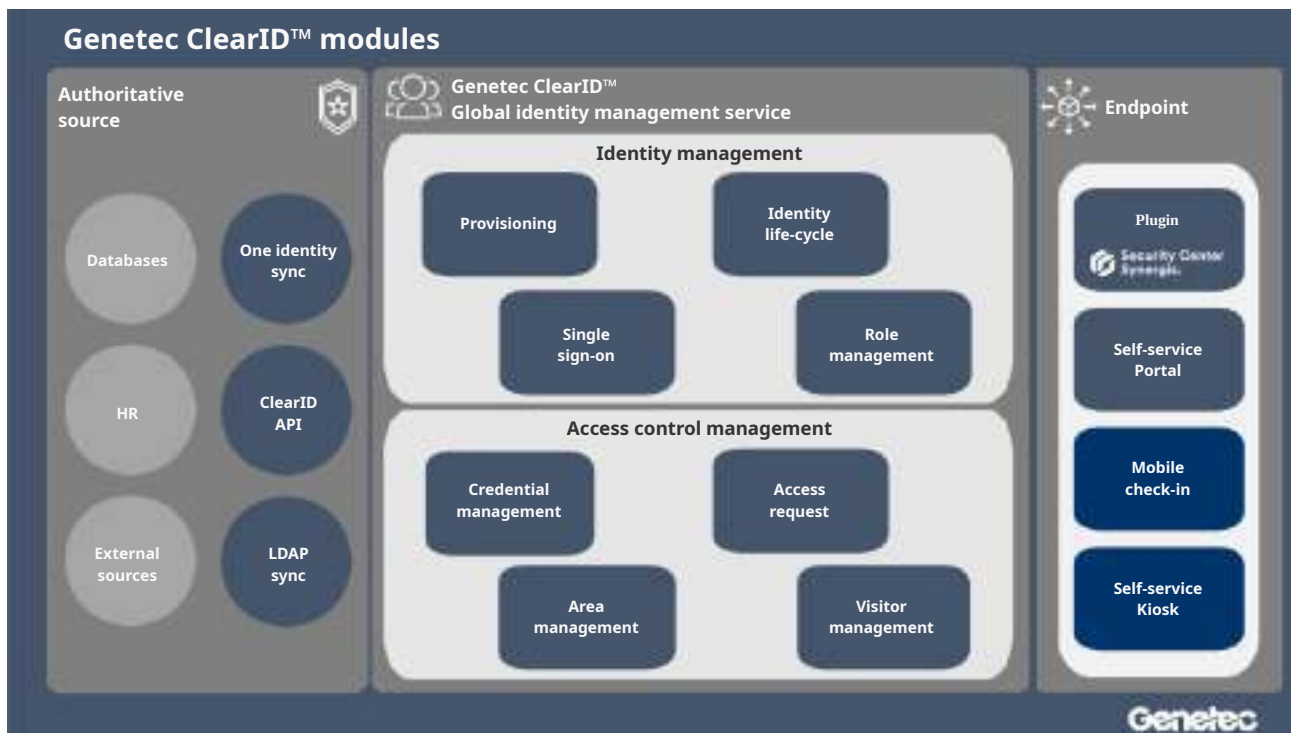
- Primary data center: Azure Central Canada (Ontario)
- Secondary data center: Azure East Canada (Quebec)

Australian data centers

- Primary data center: Azure East Australia (New South Wales)
- Secondary data center: Azure Central Australia (Canberra)

ClearID modules

The following diagram illustrates the ClearID web application modules that are available to customers:



Authoritative source

Shows the identity provisioning options that are available to customers. You can create identities in ClearID from one of the data sources (Databases, HR, External sources) by using one of the tools (Genetec ClearID™ One Identity Synchronization Tool, Genetec ClearID™ API, or the Genetec ClearID™ LDAP Synchronization Agent).

Global identity management service

Shows an overview of the features and services offered by the ClearID platform.

Endpoint

Shows the modules that customers directly interact with. These modules are where the customer enters their data or configures their system.

Cloud architecture

ClearID is deployed on the Microsoft Azure cloud platform, to take advantage of its industry-recognized security. Microsoft Azure has been audited against SOC 1, SOC 2, and SOC 3 standards. Audits are conducted in accordance with ISO SSAE 16 and ISAE 3,402 standards. Certifications are regularly updated and can be provided upon request. Azure is also compliant with ISO 27001.

The service architecture is built for High availability (HA) and scalability. Data stored in ClearID is redundant, ensuring the redundancy of critical data and mitigating the impact of hardware failure. This architecture, coupled with the robustness of the underlying Microsoft Azure cloud, means that we can provide a 99.9% SLA.

Security controls

Microsoft Azure adheres to a rigorous set of security controls that govern operations and support. Microsoft deploys a combination of preventive, defensive, and reactive controls including the following mechanisms that help to protect against unauthorized developer or administrative activity:

- Strict access controls on sensitive data, including a requirement for two-factor smart card-based authentication to perform sensitive operations.
- Combinations of controls that enhance independent detection of malicious activity.
- Multiple levels of monitoring, logging, and reporting.
- Security reports can be used to monitor access patterns and to identify and reduce potential threats proactively.
- Microsoft administrative operations, including system access, are logged to provide an audit trail if unauthorized or accidental changes are made.

High availability

Azure facilities are designed to run 24x7x365 and use various measures to help protect operations from power failures, physical intrusions, and network outages. These data centers comply with industry standards for physical security and availability. Microsoft operations personnel manage, monitor, and administer these Azure facilities.

Browse

- [Global Privacy Policy](#)
- [Product Privacy Sheet - ClearID](#)
- [Genetec Compliance Portal](#)

1.2.1 | ClearID subprocessors list

Genetec ClearID™ uses third-party vendors to assist Genetec™ in the provision of ClearID cloud services and which, as part of their responsibilities, might collect, access, store, or otherwise process customer data (including personal data).

For the latest information regarding third-party subprocessor vendors, see [List of Subprocessors](#).

Parent topic: [About ClearID architecture](#)

Browse

- [About ClearID information security](#)

1.3 | About ClearID information security

All data and files imported in Genetec ClearID™ are encrypted, and all communication with the platform is secure. These encryption and security measures ensure that sensitive data, files, and communications are only seen by users with the appropriate access.

Cryptography standards

Data encryption

All personal information managed by ClearID is automatically encrypted using Advanced Encryption Standard 256 bits (AES-256) with symmetric keys that are dynamically generated. This automatic encryption ensures that each blob of data like an identity is given a unique AES key.

For extra protection, the AES key is also encrypted with a public key unique to the account's private key. All the cryptographic keys used by ClearID are securely managed using the Azure Key Vault, which supports FIPS 140-2 Level 2 validated HSMs.

Data integrity

A digital signature (SHA 512 with RSA) is generated to detect any attempts to modify data and ensure the integrity of the data and actions in the system. Analyzing and uniquely identifying all data using a complex algorithm prevents attackers from deleting, modifying, or adding content to data stored in ClearID.

Communication encryption

Communication in the platform is secured using Hypertext Transfer Protocol Secure (HTTPS) protocol and Transport Layer Security (TLS) certificates to ensure that only trusted parties have access to data managed by ClearID. This communication encryption ensures the confidentiality of the information and reduces the possibility of malicious attempts to intercept or alter communication in transit.

Network and information security

As a trusted provider of security solutions for government agencies and high-profile public and private organizations worldwide, we take compliance with local laws seriously. This compliance includes the laws related to data security and protection of privacy in the territories where we sell our products and services.

To ensure that all customer data is stored and used appropriately and securely, ClearID is an ISO/IEC 27001 certified Information Security Management System.

Secure development and operations

Our development and operations teams have been certified ISO 27001:2013. Our dedicated security team administrates and reviews architecture and design requirements, ensuring that we meet the highest industry standards and regulations, including General Data Protection Regulation (GDPR). Every change in ClearID undergoes a strict series of automated security tests and regular penetration tests performed by industry leaders in Information Security.

Zero-trust architecture

Customer data is segmented over a series of microservices. Each microservice has one specific role in the system and the service has access only to the minimum data required to perform that task. There is no central repository of data that can be attacked. The information is distributed across siloed, independent repositories. The data center network is considered unsafe in our zero-trust architecture. All data transmitted and received between microservices is encrypted and digitally signed.

Service monitoring

We subscribe to various security threat feeds and services, including Check Point, Microsoft, Mandiant, and Hyphen. Based on the nature of evolving threats, we adapt our controls as often as necessary.

Production environments are constantly monitored using the following monitoring services:

- Perform a series of synthetic transactions every 5 minutes to emulate users from different locations in the world.
- Constantly measure a series of metrics from the servers to detect any anomalies, such as a high number of web request failures.
- Automatically raise the alarm to our development and operations team, who take immediate action to correct the issue and mitigate any impact in the production environment.

The goal is to detect transient errors, data center issues, performance degradation, and ISP outages, before users notice any impact to their system.

User authentication

By default, ClearID uses Microsoft Entra ID B2C and Entra ID B2B for user authentication. Organizations can also federate their existing Active Directory (AD) user identities through Microsoft Entra ID, or any system that supports the OpenID Connect standard, to provide a single sign-on (SSO) experience and ensure that the system meets the corporate policies requirements for user authentication.

The authentication system is based on a passive authentication model with OAuth 2.0 and OpenID Connect, which allows the identity server (AD or others) to present the connection page immediately. Identity administrators can define how users are authenticated. For example, passwords, tokens, biometrics, or a combination of these techniques.

By using Active Directory, organizations can enforce a large variety of user and password validation rules and expiration requirements. A few examples of requirements include multi-factor authentication, deactivating a user credential after several failed sign in attempts, and many other configuration options.

Browse

- [Global Privacy Policy](#)
- [Product Privacy Sheet - ClearID](#)
- [Genetec Compliance Portal](#)

1.4 | How is ClearID different from traditional access control systems?

Use the following information to help you understand how Genetec ClearID™ is different from traditional access control systems.

In traditional access control systems, security personnel are constantly involved to grant or deny access to physical locations:

- Security personnel must verify with the room owners before granting access to someone.
- When the access is no longer required, the person never goes back to security to ask to be removed from the room.
- Most sites do not track or record why access was required.

In ClearID, the self-service Web portal reduces effort and increases flexibility by using *workflows* when employees, managers, and owners of the different secure areas request and grant access.

Requests are processed as follows:

1. Separate requests and approval workflows are created for each request.

Each request includes the requester identity, time of request, reason for request, and other audit trail information.

2. Each request generates email notifications for the requester and for approvers.
3. After the request summary is confirmed, it is automatically assigned to the right individuals for approval.

4. The employee manager, area owners, and other approvers receive an email requiring them to approve, deny, or modify the submitted request.
5. After the approval process occurs, the requester receives an email notifying them whether their request was approved or rejected.

NOTE: Access, visit, or identity requests can be limited to a specific period, as opposed to the traditional method of an infinite period.

Using the self-service portal, employees can request access to specific areas in the same building or in a different site. Even when the site is managed by a different instance of Security Center.

If a person is traveling for the first time to an office managed by a different instance of Synergis™, the system automatically creates a cardholder and synchronizes all the credentials a few hours before the travelers arrive on site. On the last day of the trip, as specified in the access request, the system automatically revokes access to the secure area.

Browse

- [About workflows in ClearID](#)

1.5 | About workflows in ClearID

Genetec ClearID™ uses workflows to process, and then approve or reject, access requests, visit requests, or identity requests.

NOTE: Depending on how you configure your sites and areas, some of the workflow processes might not apply to your environment.

The following *workflows* are provided to support the different request types:

Access request workflow

An access request workflow is a series of activities performed by the system or authorized people during the life cycle of an access request. The activities can change the state and properties of access requests, affect other entities in the system, or wait for a condition to be met.

Visit request workflow

A visit request workflow is a series of activities performed by the system or authorized people during the life cycle of a visit request. The activities can change the state and properties of visit requests, affect other entities in the system, or wait for conditions to be met.

Visit request watchlist workflow

A watchlist workflow is a series of activities performed by the system or authorized people during the life cycle of a visit request if watchlists are enabled. The activities can change the state and properties of watchlists, affect other entities in the system, or wait for conditions to be met.

Identity request workflow

An identity request workflow is a series of activities performed by the system or authorized people during the life cycle of an identity request. The activities can create an individual identity, or multiple identities using a CSV import, and add each new identity to a role to inherit relevant access for a specified period.

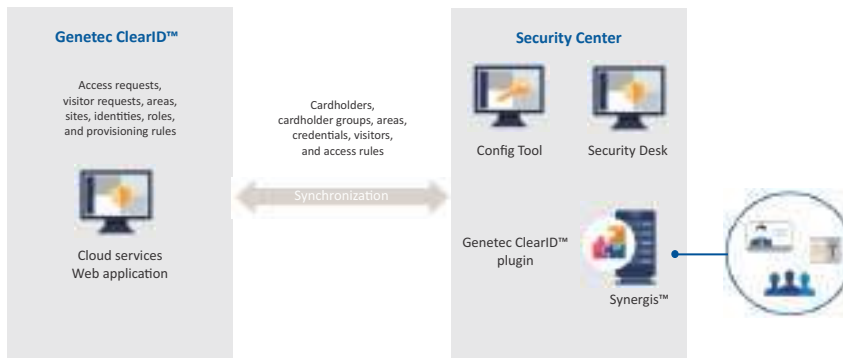
Browse

- [About access request workflow in ClearID](#)
- [About visit request workflow in ClearID](#)
- [About visit request watchlist workflow in ClearID](#)
- [About identity request workflow in ClearID](#)
- [Creating exceptions to the access request approval workflow in ClearID](#)

1.6 | How the ClearID plugin works with Security Center

The Genetec ClearID™ plugin is required to synchronize data between the Genetec ClearID™ web application and Security Center.

The components of the ClearID plugin integration



ClearID

Genetec ClearID™ is a smarter way to manage physical access using a self-service solution for Synergis™.

ClearID plugin

The ClearID plugin is installed on a Security Center server and runs as a plugin role.

The Genetec ClearID™ Plugin integrates Genetec ClearID™ with Security Center and connects Synergis™ and ClearID cloud services. Any actions performed in ClearID are automatically synchronized with Synergis.

Security Center

Security Center is a truly unified platform that blends IP video surveillance, access control, automatic license plate recognition, intrusion detection, and communications within one intuitive and modular solution. By taking advantage of a unified approach to security, your organization becomes more efficient, makes better decisions, and responds to situations and threats with greater confidence.

The ClearID plugin is installed on a Security Center server. The plugin can be installed on the Directory or an expansion server.

Config Tool

The ClearID plugin is also installed on a Config Tool workstation. The Security Center administrator uses Config Tool to create and configure the plugin role, configure database settings, and connection settings for ClearID. You can also configure a proxy connection if required. For example, when servers do not have internet access.

Security Desk

Security Desk operators can create credentials, check in visitors, or assign and print badges.

Synergis

Security Center Synergis™ is the IP access control system (ACS) that heightens your organization's physical security and increases your readiness to respond to threats. Synergis™ supports an ever-growing portfolio of third-party door control hardware and electronic locks. Using Synergis™, you can leverage your existing investment in network and security equipment.

The following information is extracted from Synergis for use by ClearID:

- Access rules
- Areas
- Cardholders
- Cardholder groups
- Credentials
- Schedules
- Visitors

NOTE: In Config Tool and Security Desk, entities managed by ClearID are highlighted with a blue dot in the bottom-right corner of the entity icon as follows:

- Access rules (🟡)
- Areas (🏠)
- Cardholders (👤)
- Cardholder groups (👥)
- Credentials (🔑)
- ClearID partitions (🌐)
- Visitors (👤)

Browse

- [Downloading and installing the ClearID plugin](#)

1.7 | Integration overview for the ClearID plugin

You can integrate the Genetec ClearID™ web application with Security Center by installing and configuring the ClearID plugin and following a sequence of steps.

Genetec ClearID®; User Guide

Displayed in the header

The following table lists the tasks required for the integration with Security Center, and how to verify that the integration is successful.

Step	Task	Where to find more information
Understand the prerequisites and key issues before deploying		
1	Learn about what you can do using ClearID.	- What is ClearID?. - How is ClearID different from traditional access control systems?. - About workflows in ClearID. - Supported features list for ClearID. - Supported languages in ClearID.
2	Before installing the plugin, read the release notes to learn about the new features.	What's new in ClearID.
3	Familiarize yourself with the common terms and their equivalents in Security Center.	ClearID terminology.
4	Learn about the different components and how they connect.	- How the ClearID plugin works with Security Center. - About ClearID architecture. - ClearID subprocessors list. - About ClearID information security.
5	Learn about key features and understand the product.	ClearID videos.
Deployment Preparation		
1	Ensure that the plugin is installed on a server that meets the recommended system requirements and is running a compatible version of Security Center.	- Compatibility for ClearID. - System requirements for ClearID. - Firewall ports used in ClearID.
2	Learn about the devices that are supported for use with ClearID.	Supported devices for ClearID.
3	Familiarize yourself with deployment best practices.	- ClearID Best practices. - Best practices for setting up ClearID for a new Synergis system. - Best practices for setting up ClearID with an existing Synergis system.
Prepare Security Center		
1	Verify that the Security Center license has a valid certificate for the plugin. Go to the Config Tool homepage, click About > Certificates, and confirm that the ClearID plugin is in the list.	- Your license information is included in the license update email that we sent you. This email includes links to the download package and other license information. - To acquire a license, see License options.
2	To manage visitors in ClearID, verify that the Synergis™ visitor management module is enabled. Go to the Config Tool homepage, click About > Synergis™, and confirm that Visitors is in the list.	- Your license information is included in the license update email that we sent you. This email includes links to the download package and other license information. - To acquire a license, see License options.
Deploy the plugin		
1	On a Security Center server, download and install the plugin.	Downloading and installing the ClearID plugin.

Genetec ClearID®; User Guide

Displayed in the header

Step	Task	Where to find more information
2	Create the plugin role. IMPORTANT: Each plugin role can only connect to or communicate with one unique ClearID system name at a time. For environments with multiple systems, you must create a plugin role for each system.	Creating the ClearID plugin role.
3	Connect Security Center to ClearID. NOTE: For environments with multiple systems, repeat these tasks for each system.	- Connecting Security Center to ClearID. - Reviewing cardholders and identities information in ClearID. - Adding a system to ClearID. - Downloading an activation file for ClearID. - Configuring connection settings for ClearID.
4	Grant users the privileges they require to use the plugin. NOTE: Security Desk operators do not need special privileges to use this plugin.	- Granting user privileges for the ClearID plugin. - Assigning privileges to users . - For a list of all available privileges, refer to the Security Center privileges spreadsheet for your version.
5	Learn about system states.	About ClearID system states.
6	Learn about identity fields.	Identity fields in ClearID.
7	Learn about custom fields.	- About custom fields in ClearID. - Modifying ClearID custom fields in Config Tool. - Custom fields relationships.
Manage identities and users		
1	Create, view, or modify your identities.	- Creating identities in ClearID. - Viewing identities in ClearID. - Modifying identities in ClearID. - Granting additional permissions for identities and roles in ClearID. - Granting additional permissions for supervisors in ClearID. - Viewing additional permissions in ClearID. - Modifying additional permissions in ClearID. - Deleting identities in ClearID
2	Grant users or administrators access to the web portal.	- Granting user access to the ClearID web portal. - Granting administrator access to the ClearID web portal.
3	View your profile.	Viewing your profile in ClearID.
4	View your site and area access.	Viewing your site and area access in ClearID.
5	Learn about and submit access requests.	- About access request workflow in ClearID. - Requesting access in ClearID.
6	Add your supervisors.	Adding supervisors manually in ClearID.
7	View and manage direct reports.	- Viewing direct reports in ClearID. - Managing direct reports in ClearID. - Transferring direct reports in ClearID.

Genetec ClearID®; User Guide

Displayed in the header

Step	Task	Where to find more information
8	Learn how to reset user passwords.	Resetting user passwords in ClearID.
9	Learn about email notifications sent by ClearID.	- About email notifications in ClearID. - Customizing the email banner for sites in ClearID.
10	Learn about delegation.	- About delegation in ClearID. - Delegating ClearID tasks to another user.
11	Understand the different user levels and what they can do.	User levels in ClearID.
12	Learn about and submit identity requests.	- About identity request workflow in ClearID. - Creating an identity template in ClearID. - Requesting identities in ClearID. - Requesting an identity in ClearID. - Requesting multiple identities using a CSV import in ClearID. - Canceling identity requests in ClearID - Approving identity requests in ClearID - About identity requests report in ClearID - Checking the status of identity requests in ClearID
Credential replication		
1	Configure credentials replication.	Configuring credential replication in ClearID
2	Review the credentials logs	Viewing credential synchronization logs in ClearID
3	Force a credentials synchronization	Forcing credential synchronization in ClearID
Manage your sites		
1	Learn about sites.	About sites in ClearID.
2	Create your sites in ClearID.	Creating sites in ClearID.
3	Enable visitor management for sites.	- Enabling visitor management for sites in ClearID. - Viewing sites where a user can invite visitors.
4	Grant users permission to access ClearID.	Granting access to the ClearID web portal.
5	Learn about access reviews.	About access reviews in ClearID.
6	Set up access reviews.	- Setting up area access reviews in ClearID. - Scheduling area access reviews in ClearID. - Setting up identity access reviews in ClearID. - Scheduling identity access reviews in ClearID.
7	Learn about access reviews report.	About access reviews report in ClearID.

Genetec ClearID®; User Guide

Displayed in the header

Step	Task	Where to find more information
8	Check the status of access reviews.	Checking the status of access reviews in ClearID.
9	Complete an access review.	- Completing an area access review (site owner) in ClearID. - Completing an area access review (area manager or role manager) in ClearID. - Completing an identity access review (supervisor) in ClearID.
10	Generate an access reviews report.	Generating an access review summary in ClearID.
11	Learn about access requests report.	About access requests report in ClearID.
12	Check the status of your access requests.	Checking the status of access requests in ClearID.
13	Learn about site activity report.	About site activity report in ClearID.
14	Learn about and manage webhook integrations.	- About webhooks in ClearID. - Creating webhooks in ClearID. - Modifying webhooks in ClearID. - Viewing webhook logs in ClearID.
Manage your areas		
1	Learn about areas.	About areas in ClearID.
2	Create your areas in ClearID.	Creating areas in ClearID.
3	Add doors to areas.	Adding doors to areas in ClearID.
4	Enable visitor management for your areas.	Enabling visitor management for areas in ClearID.
5	Learn about nested areas and access rules	- About nested areas in Security Center - Granting access to areas in Security Center automatically
6	Add your area owners and managers.	Adding area owners and managers in ClearID.
7	Add your area schedules.	Adding schedules to an area in ClearID.
8	Grant people access to an area.	Granting access to an area in ClearID.
9	Review who has access to your area.	Reviewing area access in ClearID.
10	Approve requests for access to your area.	Approving area access requests in ClearID.
11	Reject requests for access to your area.	Rejecting area access requests in ClearID.
Manage your visitors		

Genetec ClearID®; User Guide

Displayed in the header

Step	Task	Where to find more information
1	Learn about visit request workflows.	- About visit request workflow in ClearID. - About visit request watchlist workflow in ClearID.
2	Invite visitors.	- Inviting visitors in ClearID. - Inviting visitors manually in ClearID. - Inviting visitors using a CSV import in ClearID.
3	Review visit events.	Reviewing visit events in ClearID.
4	Copy a visit event.	Copying a visit event in ClearID.
5	Modify a visit event	Modifying visit events in ClearID.
6	Learn about visitors report.	About visitors report in ClearID.
7	View a visitors report.	Viewing a visitors report in ClearID.
8	Learn about QR codes as a credential for visitors.	QR codes as a credential for visitors in ClearID.
9	Import the custom card format (QR code credential).	Importing a custom card format (QR code credential) in Synergis.
10	Enable QR code credentials for visitors.	Enabling QR code credentials for visitors in ClearID.
11	Configure Qscan barcode readers for ClearID.	- Configuring Qscan devices for ClearID. - Connecting a Qscan barcode reader to a Mercury Controller for ClearID. - Configuring Qscan barcode reader to support 40-bit hexadecimal QR codes for ClearID.
12	Configure STid devices for ClearID.	- Configuring STid devices for ClearID. - About STid QR code readers in ClearID. - Creating an STid QR code reader configuration for ClearID. - Transferring your reader configuration to your STid QR code reader for ClearID.
13	Configure macro for automatic check-in and access to a parking entrance or gated facility.	Automating visitor access and check-in using a macro in Security Center.
Managing visitor watchlists		
1	Learn about watchlists.	About watchlists in ClearID.
2	Add your watchlist managers.	Adding watchlist managers in ClearID.

Genetec ClearID®; User Guide

Displayed in the header

Step	Task	Where to find more information
3	Add your watchlists.	- Adding watchlists in ClearID. - Adding an individuals watchlist entry in ClearID. - Adding a companies watchlist entry in ClearID. - Importing watchlist entries from a file in ClearID. - Exporting watchlist entries to a file in ClearID. - Testing watchlist entries in ClearID.
4	Screen your visitors manually	Screening visitors manually in ClearID.
5	Unblock visitors blocked by a watchlist.	Unblocking visitors blocked by a watchlist in ClearID.
Managing role-based access control		
1	Learn about role-based access control.	About role-based access control in ClearID.
2	Add your roles.	Adding roles in ClearID.
3	Add your role managers.	Configuring role managers in ClearID.
4	Configure your role-based access control policies.	Configuring role-based access control policies in ClearID.
5	Add custom provisioning attributes to an identity.	Adding custom provisioning attributes to an identity in ClearID.
6	Add your role members.	Adding role members in ClearID.
Connecting other systems		
1	Learn how to authenticate non-user system connections.	Authenticating your connection with ClearID.
2	Synchronize identity attributes using LDAP.	- Synchronizing identities using LDAP in ClearID. - About ClearID LDAP Synchronization Agent. - LDAP attributes to ClearID attribute mappings. - Configuring the ClearID LDAP Synchronization Agent.
3	Synchronize identity attributes using an API.	- Synchronizing identities using an API in ClearID. - About the ClearID API.
4	Synchronizing identity attributes using One Identity.	- Synchronizing identities using One Identity Synchronization Tool in ClearID. - About the ClearID One Identity Synchronization Tool. - About ClearID One Identity Synchronization Tool attribute fields. - Installing the ClearID One Identity Synchronization Tool. - Configuring the ClearID One Identity Synchronization Tool. - Reviewing synchronization status for the ClearID One Identity Synchronization Tool. - About ClearID One Identity Synchronization Tool logs. - Viewing the ClearID One Identity Synchronization Tool logs. - Updating existing identities from an external data source using ClearID One Identity Synchronization Tool.
Visitors self-service check-in		

Genetec ClearID™; User Guide

Displayed in the header

Step	Task	Where to find more information
1	Learn about Genetec ClearID™ Self-Service Kiosk.	- About ClearID Self-Service Kiosk. - About ClearID Self-Service Kiosk check-in. - About ClearID Self-Service Kiosk Self registration.
2	Learn about the different ClearID Self-Service Kiosk options that are available.	- ClearID Self-Service Kiosk options. - ClearID Self-Service Kiosk floor stand. - ClearID Self-Service Kiosk floor stand printer shelf. - ClearID Self-Service Kiosk tabletop stand.
3	Learn about the Identity Document (ID) types that the ClearID Self-Service Kiosk ID scanning function supports.	Identity document types in ClearID.
4	Configure your ClearID Self-Service Kiosk.	- Configuring the ClearID Self-Service Kiosk iPad. - Customizing the ClearID Self-Service Kiosk configuration. - Customizing the ClearID Self-Service Kiosk visitor badge logo. - Configuring the ClearID Self-Service Kiosk label printer (Brother QL-820NWBc, QL-820NWB, or QL-810W). - Configuring the ClearID Self-Service Kiosk label printer (Brother TD-4550DNWB). - Selecting a ClearID Self-Service Kiosk label printer. NOTE: The Brother TD-4550DNWB printer is no longer available for purchase through Genetec. We now support and sell the Brother QL820NWBc (CD-KIOSK-PRINTER-NA-KIT).
5	Test your visitor badge printing.	Printing a test badge from the ClearID Self-Service Kiosk.
6	Reset the ClearID Self-Service Kiosk mobile app (If required).	Resetting the ClearID Self-Service Kiosk mobile app.
Troubleshooting		
1	Learn how to troubleshoot issues that might occur.	- Plugin installed, but missing from Security Desk and Config Tool. - Plugin role could not find file with certificate. - Custom fields not displayed in Security Desk. - No active account found for user. - Visit email notifications not received by visitors. - Visitor hosts fields in Security Desk are empty. - ClearID One Identity Synchronization Tool connectivity issues. - ClearID One Identity Synchronization Tool data synchronization issues. - ClearID Self-Service Kiosk issues. - ClearID Self-Service Kiosk label printer issues. - Viewing webhook logs in ClearID.

Browse

- License options for ClearID system integration

1.8 | Supported features list for ClearID

Discover the Genetec ClearID™ supported features.

The following table lists the features that are available in ClearID.

Feature
Identity management

Feature
Supervisor management of direct reports.
Transfer of direct reports
Configuration for supervisors to have elevated management permission for their direct reports. - Update profile information fields. - Update access control settings.
Identity request workflow and approval for onboarding: - One identity at a time. - Many identities at a time (CSV import).
Permissions for identities or roles to view and edit identities.
Area management
Delegate the management of controlled areas to one or more area owners.
Area owner or area manager can view, add, and remove people from Areas.
Area owner or area manager can view, add, and remove roles from Areas.
Area owner or area manager can grant temporary access to a role.
A permanent cardholder can request temporary access to an area (built-in workflow).
Actions in workflow are captured and available in the workflow history.
Area managers can approve or deny access requests.
Area managers can perform area access reviews.
Employee supervisor can be required to approve employee access request.
Email notifications when an access request is submitted.
Email notifications when an access request is approved or denied.
Role management
Delegate the management roles or cardholder group to one or more role owners.
Role managers can add or remove people from their groups.
Automatic provisioning and synchronization of cardholder groups for multiple sites
Role owners can request access to an area for their entire group.
Role managers can perform role access reviews.
Multi-site management
Global management of cardholders for multiple Synergis™ systems
Time zone support (built-in)
Automatic synchronization of permanent credentials when someone travels between sites.
Synchronization of cardholders only happens when cardholders are changed, if the cardholder has access on that Synergis system. This approach minimizes the number of cardholders synchronized to each Synergis system.
Synchronization of cardholder groups only happens when cardholder groups are changed, if the cardholder group has access on that Synergis system. This approach minimizes the amount of cardholder groups synchronized to each Synergis system.
Site owners can configure access review schedules or manually trigger access reviews.

Genetec ClearID®; User Guide

Displayed in the header

Feature
Site owners can generate an access reviews report.
Visitor management
Preregister visitors using a web portal
The visitor approval workflow can be customized based on the area selected.
Automatic provisioning of visitors with the required areas automatically assigned
Visitor check-in using Security Desk
Paper badges and temporary credentials - Paper badges are typically used for large volumes of visitors who require temporary access, for example: - Hosting a conference or trade show for business partners. - To identify people visiting an area, temporary visitor badges can also be stuck on visitors' clothing. - Security or reception issue temporary credentials after visitors check-in. These temporary credentials are returned to security or reception when leaving the <i>site</i> or <i>area</i>.
Visitor escort with multiple visitor hosts
Email notifications when a visitor is approved.
Capture and report the visit reason. Security staff can use the visit reason information to help track who enters or exits a building and the reason for the visit.
Email invitation sent to visitor with a meeting invite, site details, and optional file attachments
Send SMS notifications to the host when a visitor checks in. These SMS notifications can be sent to any valid phone number.
Send email notifications to the watchlist manager when visitor details match a person of interest or company of interest on an individuals or companies block or notify watchlist.
Visitor entry is blocked when visitor details match a person of interest or company of interest on an individuals or companies block watchlist.
Configurable Genetec ClearID™ Self-Service Kiosk options. For example, customizing the welcome screen QR code, ID, check-in, check-out, and self-registration option combinations that are displayed.
Configurable options to capture extra visitor information during the creation process for a visit event. For example, delivery ID, vehicle, passenger name, ID number, or license plate.
Configurable automatic visitor check-out (grace period).
Reports
Reports including CSV downloads (where applicable). Workflow request reports: - Access requests report - Access reviews report - Visitors report Audit trail reports: - Role activity report - Site activity report - Site and area owners report - User activity report
Platform
Corporate logo for Portal and email notifications

Feature
Cloud platform ClearID is a cloud service. A dedicated server is not required. However, a communications connection to the Synergis servers is required. This connection is provided by the ClearID plugin.
HTML5 web interface with mobile support Users can use their mobile devices to navigate the ClearID portal.
REST API available to automate any functions available in the Web portal. • Create or edit an identity in the system. • Disable access for a person. • Add a person to a role. • Remove a person from a role. • Create a visitor event. • Acknowledge an access request.
Synchronize identity using Microsoft SQL Server.
Synchronize identity from custom source using Identity REST API.
Security and authentication
Support multi-factor authentications for users using OpenID connect
Single sign-on using Microsoft Office 365
Single sign-on using Microsoft Entra ID
ISO 27001 certification For more information, see Cybersecurity resources.
AES-256 encryption with RSA Personal data managed by ClearID is always encrypted.

Browse

- [Genetec Compliance Portal](#)

1.9 | Supported languages in ClearID

Genetec ClearID™ is available in the following languages.

ClearID web portal

- English
- French
- Spanish
- Dutch
- German
- Italian
- Portugese
- Japanese

NOTE: The language that is displayed in the web portal user interface is determined by your web browser language settings.

ClearID plugin

- English

Genetec ClearID™ One Identity Synchronization Tool

- English

Genetec ClearID™ LDAP Synchronization Agent

- English

Genetec ClearID™ Self-Service Kiosk mobile app

- English
- French
- Spanish
- Dutch
- German
- Italian
- Portuguese
- Japanese

Documentation

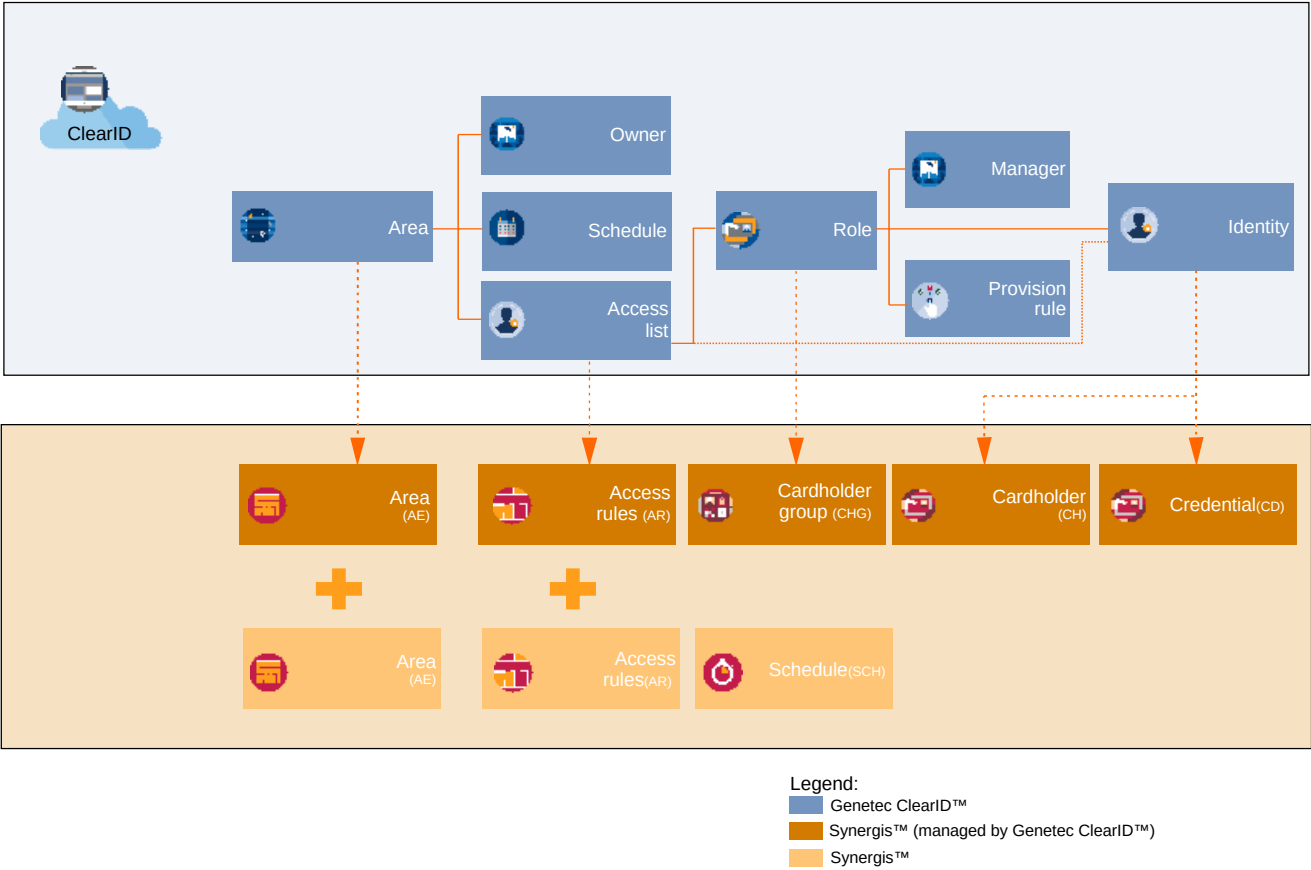
- ClearID User Guide (English)
- ClearID User Guide (French)
- ClearID User Guide (Spanish)

IMPORTANT: Translation of documentation is ongoing. Documentation in languages other than English might not be complete at the time of release.

1.10 | ClearID terminology

Genetec ClearID™ uses specific terms. Here are the definitions of some common terms and their equivalents in Security Center.

The following diagram shows ClearID terms and their equivalents in Security Center:



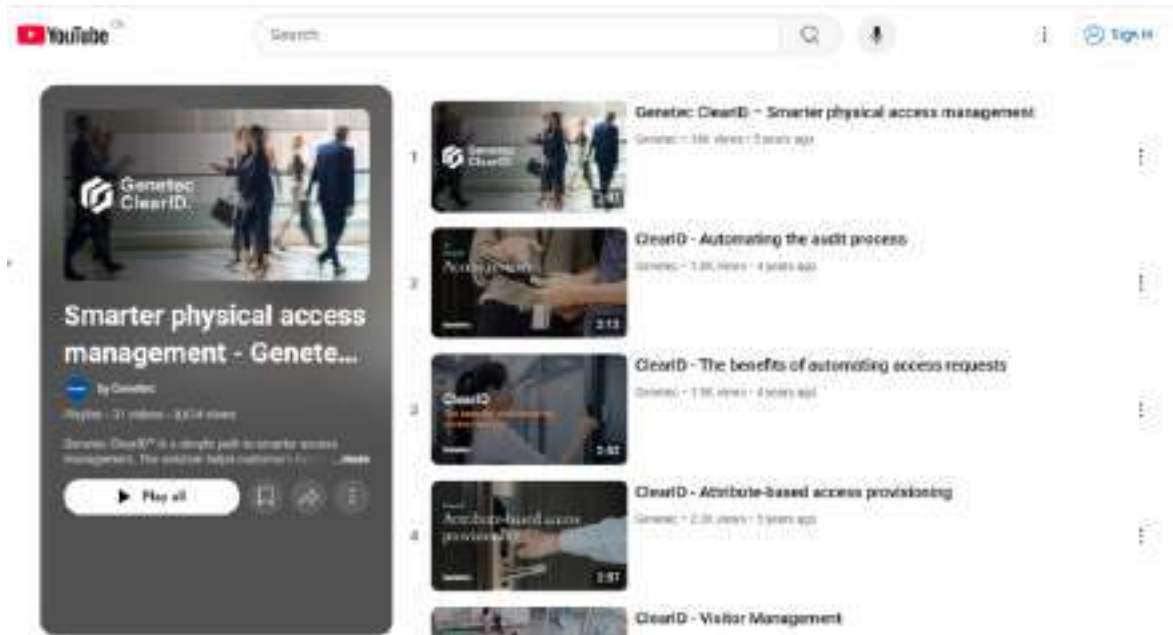
The following table lists ClearID terms and their equivalents in Security Center:

ClearID	Security Center
Identity	Cardholder
Area	Area

ClearID	Security Center
Role	Cardholder group
Schedule (defined in Security Center) and access list (defined in ClearID)	Access rules

1.11 | ClearID videos

Use the Genetec ClearID™ videos to help you learn about key features and understand the product. You can access all the videos in one place, the [ClearID videos playlist](#).



Click the image to access the ClearID videos playlist.

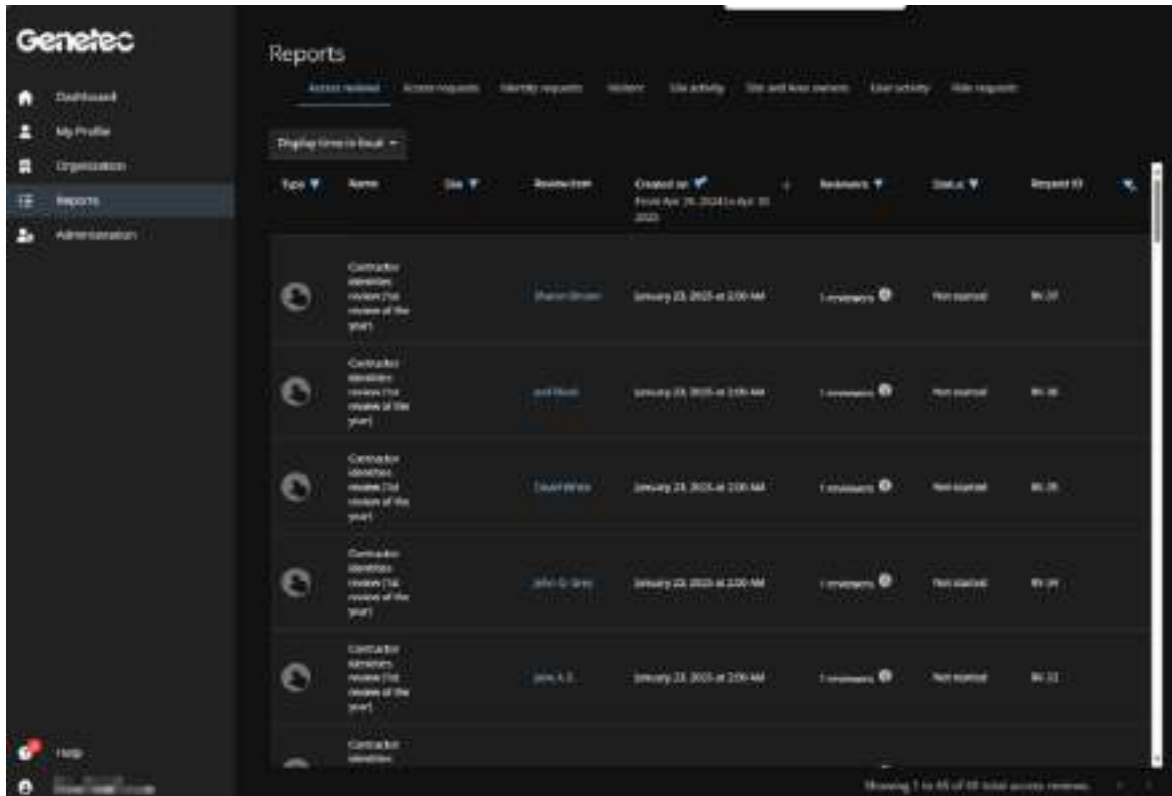
Videos can also be launched individually from relevant topics or the documentation homepage.

Browse

- [What is ClearID?](#)

1.12 | About reports in ClearID

Genetec ClearID™ provides several reports to manage your site and various activities. The reports can help you understand the status of access requests, access reviews, and current or upcoming visit events. Reports can also be used to review audit trail information about roles, sites, site and area owners, and users.



You can use the following reports to check the status of the following:

- Access reviews report
- Access requests report
- Identity requests report
- Direct reports report
- Site and area owners report
- Visitors report

You can use the following reports to review audit trail information about the following:

- Role activity report
- Site activity report
- User activity report

1.13 | Logging on to ClearID

Log on to your Genetec ClearID™ account to submit visitor or access requests.

Before you begin

- Enable cookies in the web browser that you are using
- If you are not using a corporate Active Directory system, activate your ClearID account by clicking the activation link in your email.

Procedure

1. In your web browser, enter or select the required host as detailed in your account activation email.

For example:

- United States: <https://portal.clearid.io/>
- Australia: <https://portal.au.clearid.io/>
- Canada: <https://portal.ca.clearid.io/>
- Europe: <https://portal.eu.clearid.io/>

NOTE: If a corporate log on (single sign-on using Microsoft Office 365 or similar) is used, the account is automatically activated and no activation email is received.

2. On the logon page, enter your *username* and click Logon.

You are redirected to your user account's logon page.

3. (Optional) Select an account.

- The account ID is shown in the URL of every page.

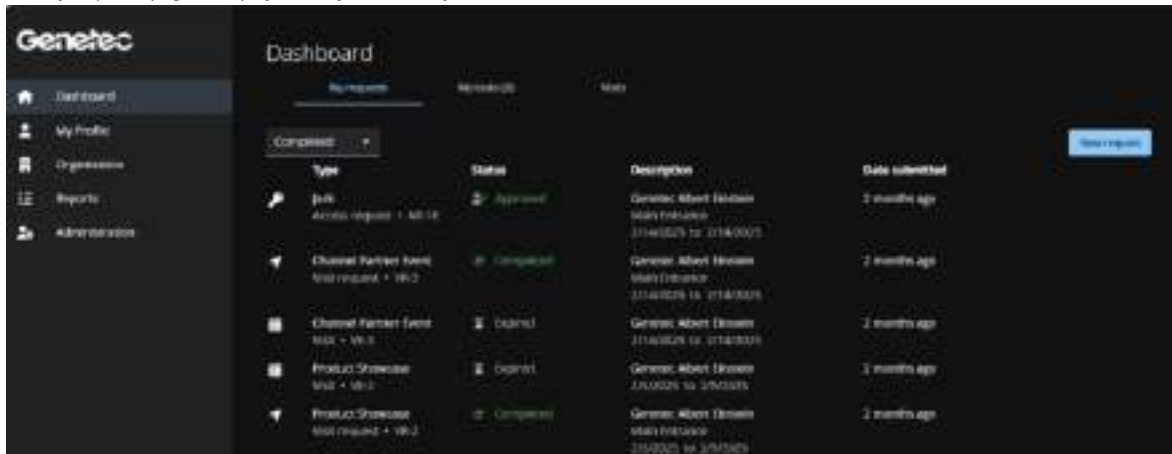
For example, <https://hostname/accountid/currentpage>.

- The account ID can change depending on the user account that is logged on.

Tip: If you have more than one account, you can switch accounts at any time by clicking Change account from the account options under the user ID.

Results

The My requests page is displayed and you are ready to use ClearID.



Browse

- Creating identities in ClearID
- Authenticating your connection with ClearID

1.14 | Logging off from ClearID

To exit from Genetec ClearID™, you can log off from your user account.

What you should know

You are logged off from the system automatically after a specified period of inactivity. The inactivity period varies depending on your environment configuration. The default is 30 minutes.

Procedure

At the top of the page, click your name, and then click Log off.

Tip: After you log off from of your account, close all browser windows that were used for ClearID.

1.15 | Enabling preview features in ClearID

When available, users can enable one or more preview features in Genetec ClearID™ to get early access to evaluate new functions before they are released.

Before you begin

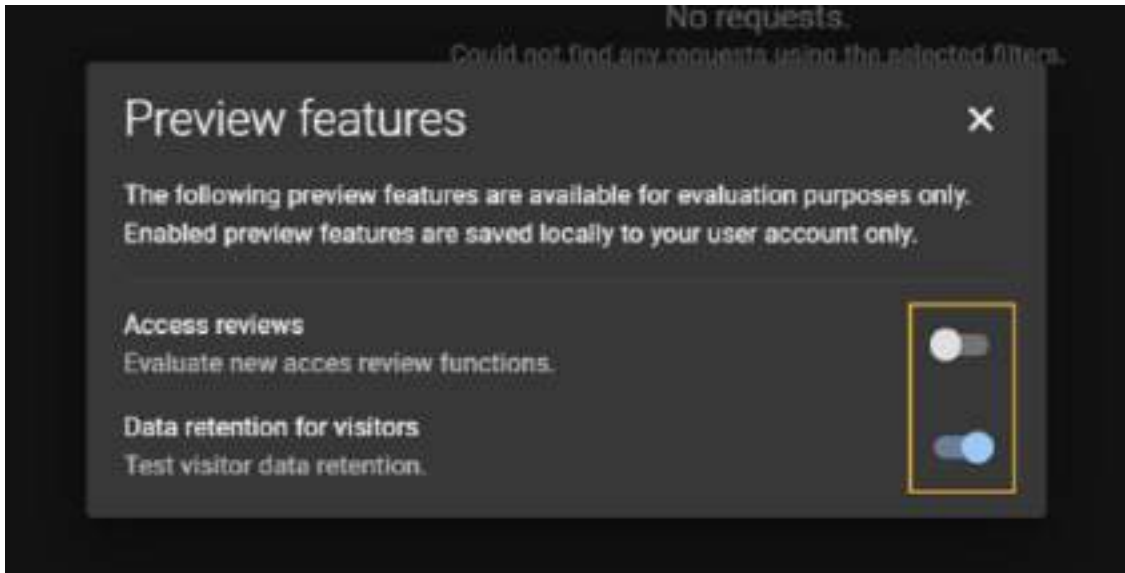
The Preview features function must be enabled for your organization.

What you should know

- Preview features are for evaluation purposes only.
- Enabled preview features are saved locally to your user account only.

Procedure

1. In the ClearID web portal, click your user name.
2. Click Preview features.
3. In the Preview features dialog, use the preview features slider controls to enable the features you want to evaluate.



4. Click  to close the dialog.

1.16 | Disabling preview features in ClearID

Users can disable one or more preview features in Genetec ClearID™ if they no longer want to use or see the new preview features.

Before you begin

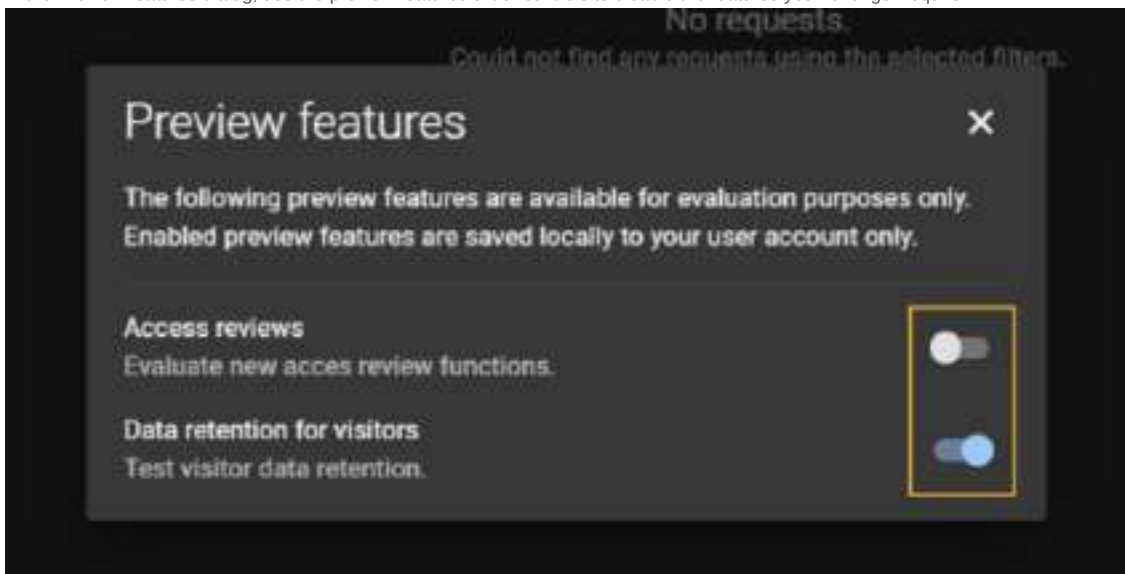
The Preview features function must be enabled for your organization.

What you should know

- Preview features are for evaluation purposes only.
- Enabled preview features are saved locally to your user account only.

Procedure

1. In the ClearID web portal, click your user name.
2. Click Preview features.
3. In the Preview features dialog, use the preview features slider controls to disable the features you no longer require.



4. Click  to close the dialog.

1.17 | Customizing portal branding in ClearID

As an account administrator, you can customize the Genetec ClearID™ portal logo and accent color to align with your company's branding.

Before you begin

You must be an *Account administrator* to customize the ClearID portal branding.

What you should know

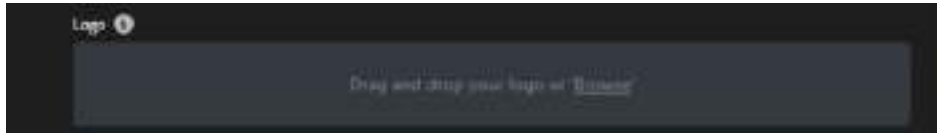
- You can set different branding options for light and dark themes in ClearID.

Procedure

- In the ClearID web portal, click Administration > Account configuration.
- In the Branding section, choose either light theme or dark theme.
 - Select the logo and accent color.

Logo

Click Browse or drag and drop an image from your file browser to upload your logo. The image must have a resolution within the range of 20x20 and 2000x500 pixels.



Accent color

Use the color picker to select a color and adjust the opacity, or type the hexadecimal code of the color in the Accent color field.



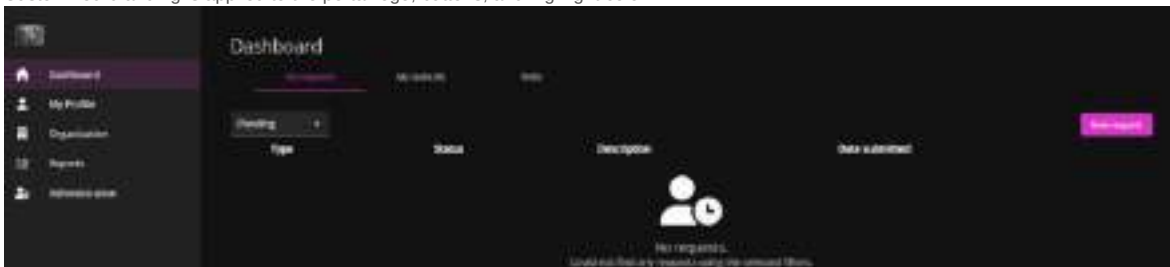
(Optional)

Click Restore default theme to restore the portal branding to default.

- Click Save.
- (Optional) Repeat steps 2 - 3 for other themes as required.

Example

Customized branding is applied to the portal logo, buttons, and highlight color.



1.18 | Customizing help menu links in ClearID

As an *Account administrator*, you can customize the Genetec ClearID™ Help menu links, directing portal users to your company's support resources and pages.

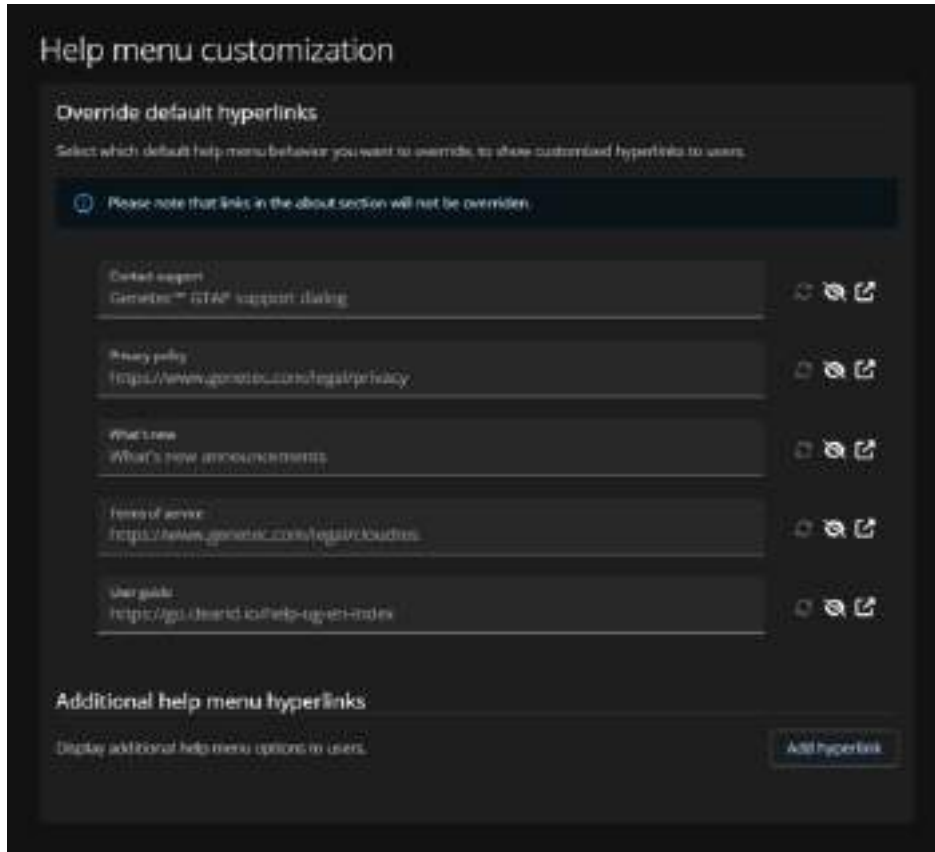
Before you begin

You must be an *Account administrator* to customize the links in the ClearID Help menu.

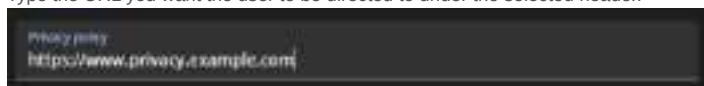
Procedure

1. In the ClearID web portal, click Administration > Account configuration.
2. In the Override default hyperlinks section, modify the default Help menu links.

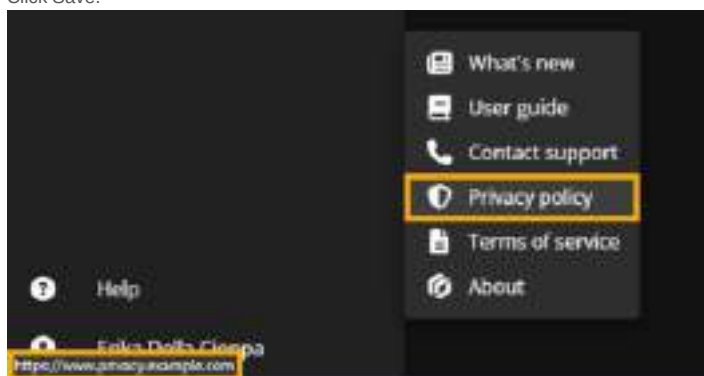
NOTE: You can't override the About link.



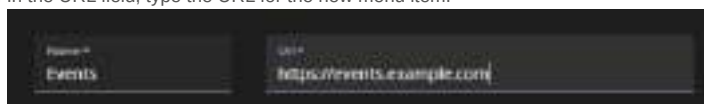
- a. Select the Help menu item you want to modify.
- b. Type the URL you want the user to be directed to under the selected header.



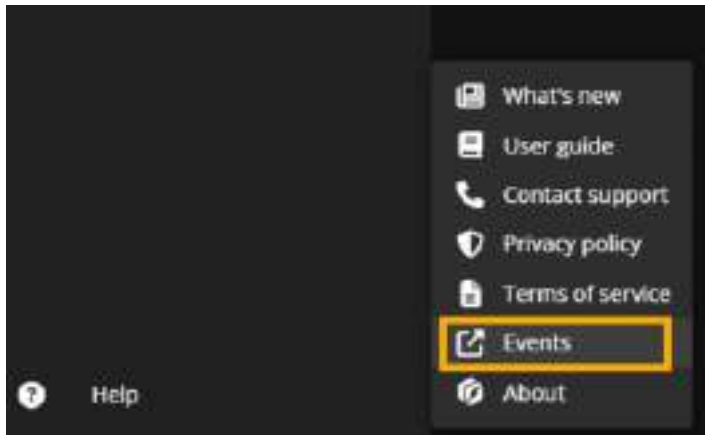
- c. Click Save.



3. (Optional) In the Additional help menu hyperlinks subsection, add more links to the menu.
 - a. Click Add hyperlink to add a new menu item.
 - b. In the Name field, type a name for your new menu item.
 - c. In the URL field, type the URL for the new menu item.



- d. Click Save.
The new link is added to the menu below the default portal links.



4. (Optional) Use the icons beside each link to reset, hide, or view menu items.

- Click Revert to default (🔄) to revert the customized link to the portal default.
- Click Hide (🔒) to hide the link from the menu.
- Click Show (👁️) to show a previously hidden link.
- Click Go to URL (🔗) to go to the linked page.
- Click Delete (🗑️) to delete the custom link.

2 | What's new

2.1 | What's new in ClearID

Check out what's new in the latest update to Genetec ClearID™.

What's New: July 2025

Updated part numbers

Genetec™ has updated and simplified ClearID part numbers to support changes in pricing for ClearID systems. There are now fewer part numbers required to build your system.

For more information, see [License options for ClearID system integration](#) and [ClearID Self-Service Kiosk options](#).

Create custom identity fields

As an *Account administrator*, you can now create and manage custom fields for identities directly in the ClearID web portal. With custom identity fields, you can store extra information like vehicle profiles, employee types, worker schedules, and more for all identities.



For more information, see [About custom identity fields in ClearID](#) and [Creating custom identity fields in ClearID](#).

Skip access request approval workflow

You can now exclude users and roles from the access request approval workflow for an area. For example, you can decide to bypass the workflow and automatically approve access requests for people who belong to a specific role, like Upper Management.

For more information, see [Creating exceptions to the access request approval workflow in ClearID](#).

Save visitor photos

You can now save photos of visitors taken during check-in to the Genetec ClearID™ web portal. You can access saved photos for incident management and auditing purposes by going to [Reports > Visitors](#).

For more information, see [Activating visitor photo retention in ClearID](#).

For a complete list of all prior announcements, see [Previous features and enhancements](#).

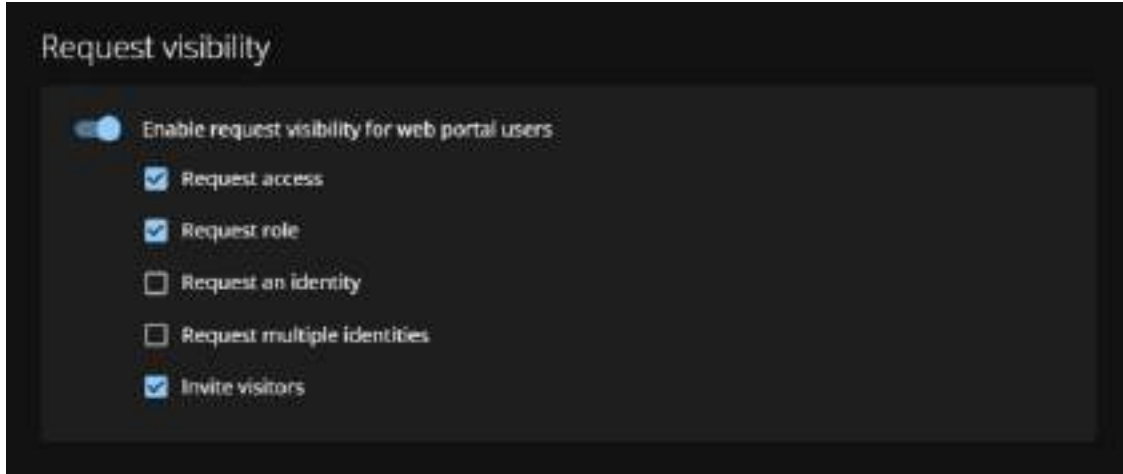
2.2 | Previous features and enhancements in ClearID

The Genetec ClearID™ solution includes the following features and enhancements.

What's New: June 2025

Change visible request types

As an *Account administrator*, you can configure permitted request types for users, limiting the types of requests users can make in the ClearID web portal.

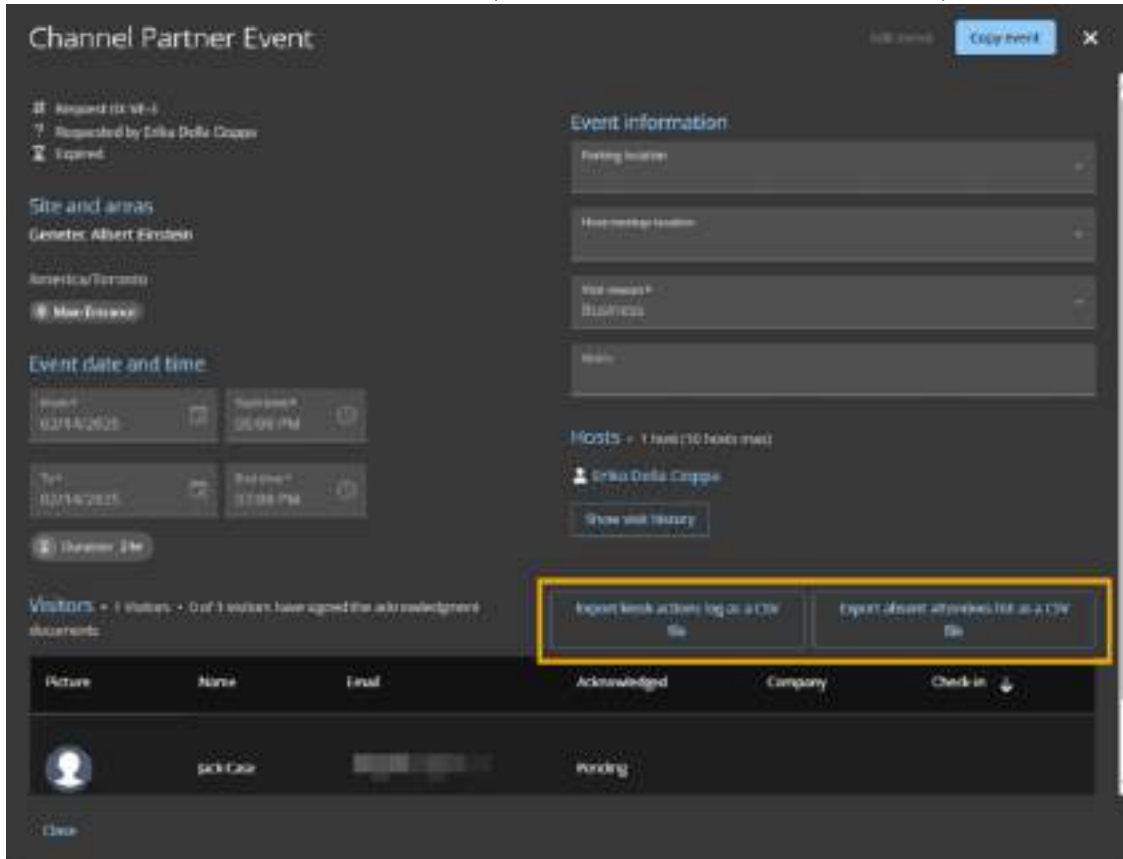


For more information, see [Setting request visibility for users in ClearID](#).

What's New: May 2025

Visit event logs

Account administrators, *Site owners*, and *hosts* can track operator and visitor actions on check-in devices and export lists of invited visitors who didn't check in.



For more information, see [About visit event logs in ClearID](#) and [Viewing visit event logs in ClearID](#).

Account-level notification preferences

Account administrators can manage the default email notification preferences for all ClearID portal users and decide which stakeholders receive notifications. You can also configure whether users can opt out of certain email notifications in their personal email notification preferences.



For more information, see [Configuring email notification preferences in ClearID \(administrator\)](#).

Add visit events to your calendar

Hosts and guests can now keep track of events by adding visits to their digital calendars using the ICS files attached to visit confirmation emails.

For more information, see [Adding ClearID visit events to your calendar](#).

What's New: January 2025

Check visitors in using ClearID mobile operator check-in

Previously, visitors could only check in to events using the Self-Service Kiosk iPad. Now, receptionists, security guards, and attendants at hosted events can quickly check visitors in using the ClearID Self Service Kiosk app on an iPhone. Mobile operator check-in uses the iPhone to scan QR codes and look up visit information.

For more information, see [About ClearID mobile operator check-in](#) and [Configuring ClearID mobile operator check-in](#).

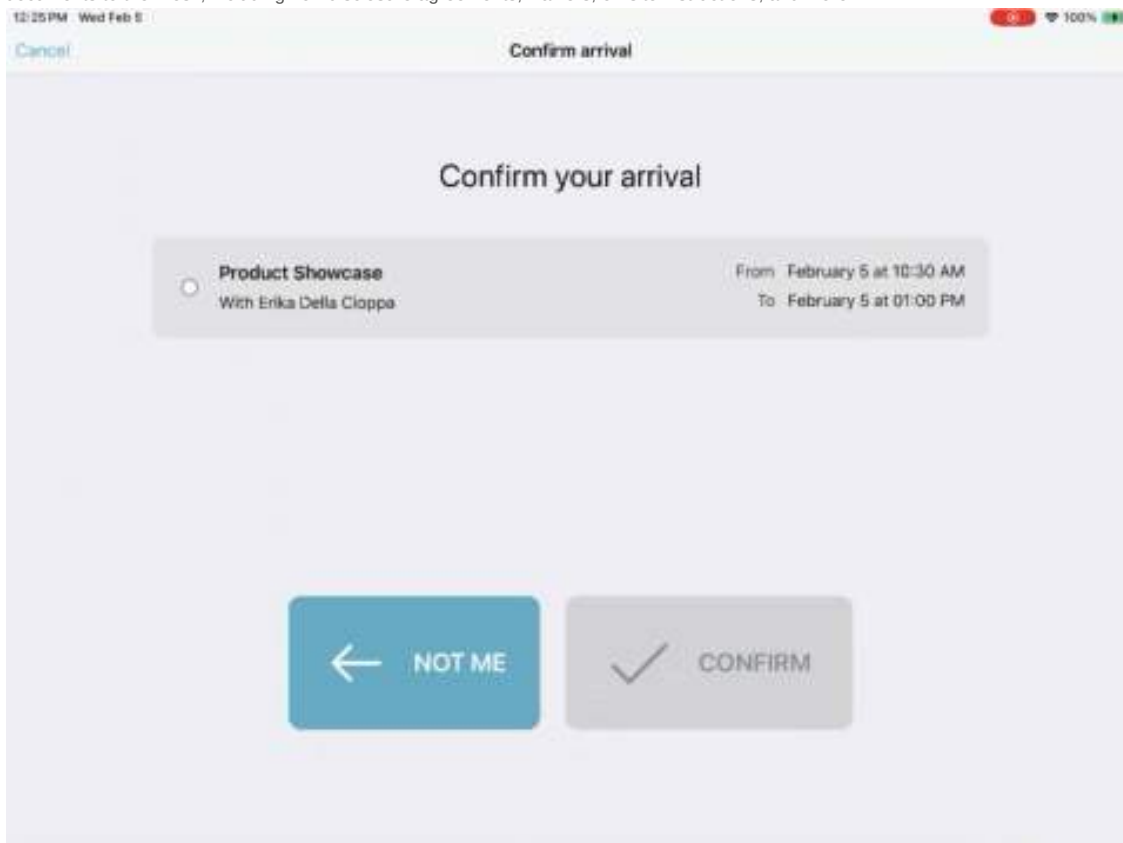
Make informed decisions when granting employees access

You can now specify that employees upload supporting documents when submitting access requests for secure areas where specialized certifications are required to gain access. *Site owners* and *Area approvers* can review submitted documents to ensure that employees requiring access comply with industry regulations and company policies before granting them access.

For more information, see [Configuring access request documents for sites in ClearID](#) and [Configuring access request documents for areas in ClearID](#).

Ensure visitors comply with site requirements

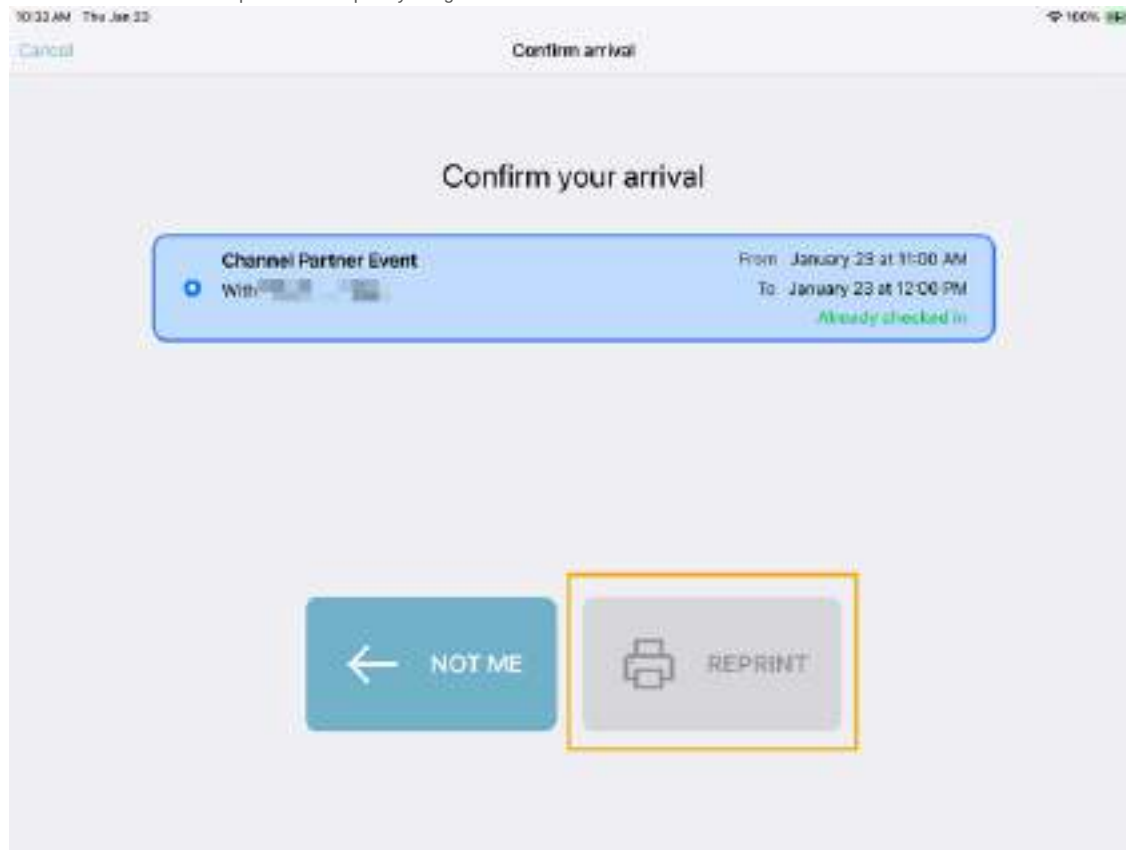
You can now specify that visitors read and sign required compliance documents during a Self-Service Kiosk check-in. *Account administrators* can add up to five documents to the Kiosk, including non-disclosure agreements, waivers, on-site instructions, and more.



For more information, see [Adding PDF acknowledgment documents to the Self-Service Kiosk](#).

Visitors can reprint badges

Visitors can now reprint lost or damaged badges directly from the Self-Service Kiosk. As a *Site owner*, you can activate the Re-print badge option so that visitors can return to the Kiosk to reprint their temporary badge.



For more information, see [Activating badge reprints](#).

Protect visitor privacy

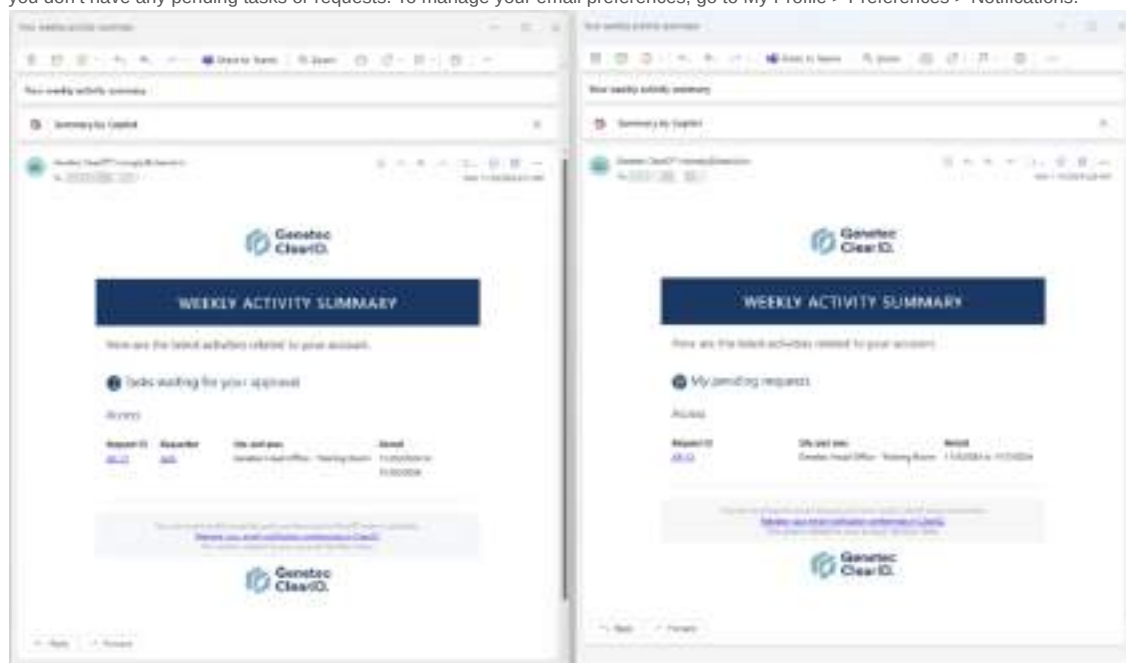
Site owners can now deactivate photo-taking during visitor check-in at the Self-Service Kiosk.

For more information, see [Disabling visitor photo during check-in](#).

What's New: December 2024

Keep track of your pending tasks

You can now receive Weekly Activity Summary emails every Monday detailing pending tasks or requests that require approval. You won't receive these emails if you don't have any pending tasks or requests. To manage your email preferences, go to [My Profile > Preferences > Notifications](#).



For more information, see [About email notifications](#) and [Configuring your email notification preferences](#).

What's New: October 2024

Synchronize ClearID identity pictures with Security Center

Account administrators can now set ClearID as the preferred data source for all cardholder pictures in Security Center. You can activate identity picture synchronization to automatically replace cardholder pictures in Security Center with ClearID identity pictures.

NOTE: ClearID identity pictures have a maximum size of 5 megabytes.

For more information, see [Synchronizing identity pictures with Security Center](#).

Personalize notification email header and footer text

Account administrators and *Site owners* can now customize the header and footer text of email notifications. Use the custom text fields to communicate information to visitors such as equipment or documentation requirements for their visit or steps to complete before arrival.



For more information, see [Customizing email notifications for sites in ClearID](#).

ClearID Self-Service Kiosk mobile app version 2.2 is now available

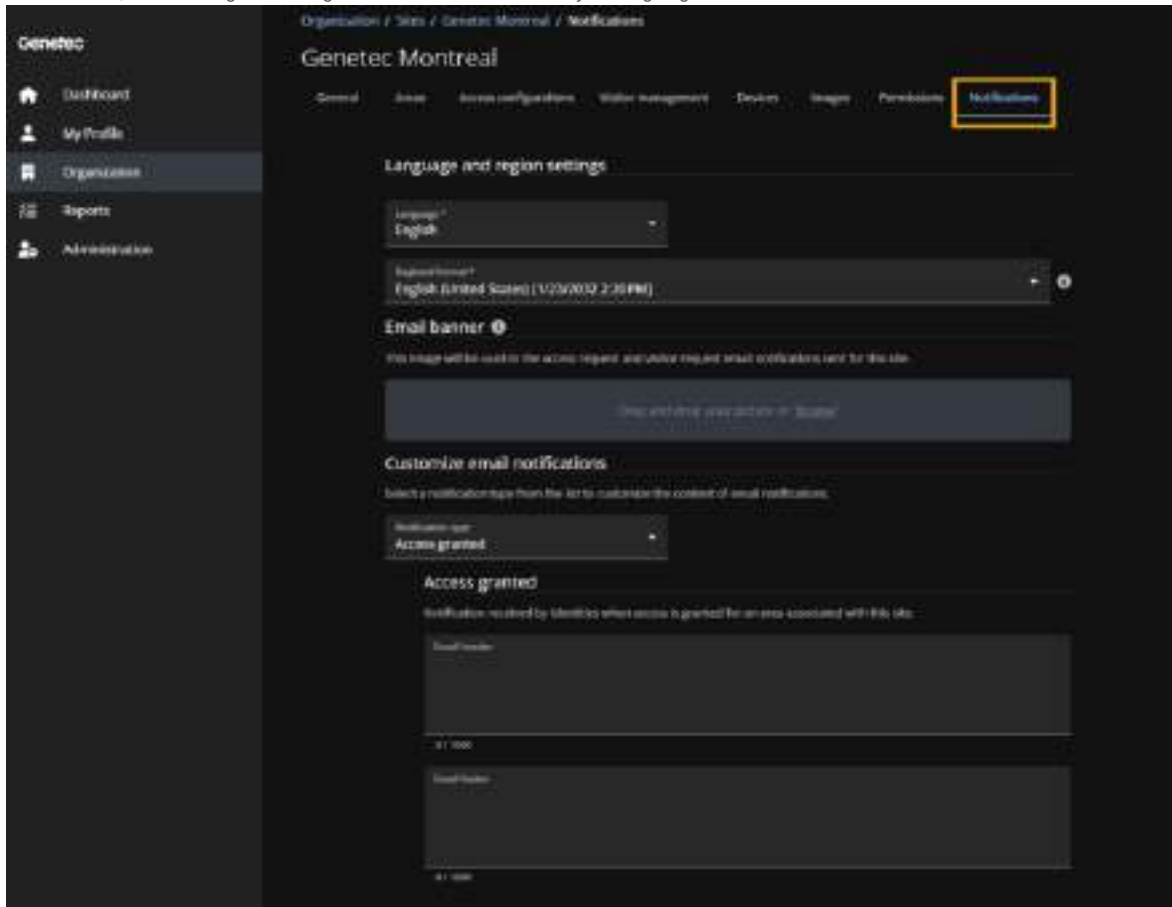
The latest update includes bug fixes and improved diagnostics for visit events. Core functionality of the kiosk remains the same.

To download the ClearID Self-Service Kiosk mobile app, visit the [App Store](#).

IMPORTANT: User interface changes

Language and region settings and notification settings have moved

Previously language and region settings and notification settings were configured by *Account administrators* or *Site owners* by clicking Organization > Sites > General. Now, these settings are configured in the Notifications tab by clicking Organization > Sites > Notifications.



For more information, see [Creating sites in ClearID](#) and [Modifying sites in ClearID](#).

What's New: September 2024

Cardholder credential synchronization

ClearID accounts connecting to multiple Security Center systems now have a new configuration setting. Administrators can now specify the Security Center system that is the source of credentials synchronized to other systems. This option makes credential synchronization automatic and predictable and can give employees access to multiple sites with a single access card.

For more information, see [Configuring credential replication in ClearID](#).

Simplified identity management

You can now use the System for Cross-domain Identity Management (SCIM) integration to synchronize system attributes from an external data source into ClearID. These identity attributes can then be used in ClearID to assign people to roles and automate role-based access control.

For more information, see [Synchronizing identities using the SCIM integration](#).

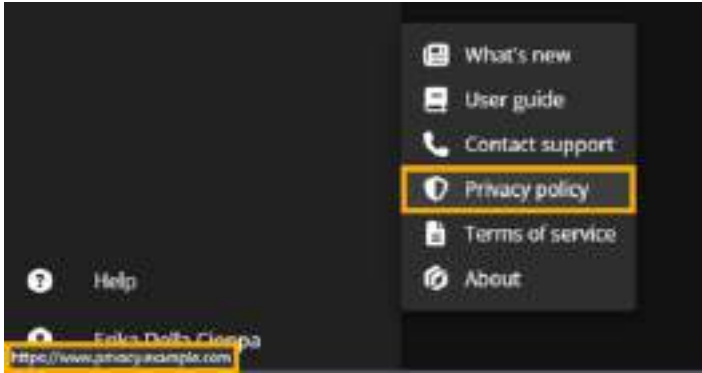
ClearID Self-Service Kiosk mobile app version 2.1.2 is now available

The latest update includes performance and scalability improvements, bug fixes, and some minor changes to the user interface. Core functionality of the kiosk remains the same.

To download the ClearID Self-Service Kiosk mobile app, visit the [App Store](#).

Help menu link customization

Account administrators can now customize the ClearID Help menu links, directing portal users to your company's support pages and resources.

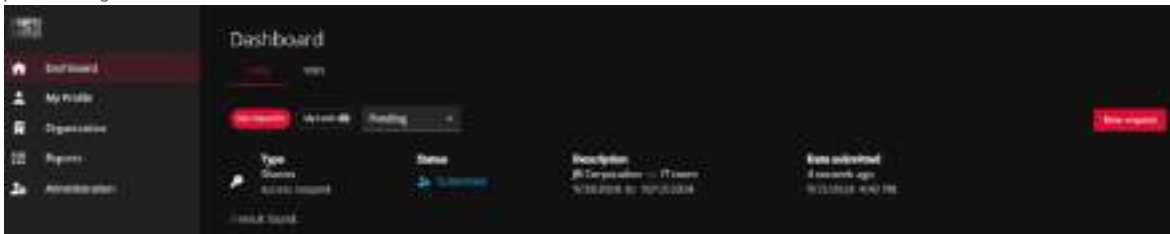


For more information, see [Customizing help menu links](#).

What's New: June 2024

Portal branding customization

Account administrators can now customize the ClearID portal logo and accent color to align with your company's branding. Portal users can choose to view the portal in a light or dark theme.



For more information, see [Customizing portal branding in ClearID](#).

Geo-specific data centers

You can now store your data in a region that applies to the geographical location of your system or where you want data stored. You can choose between more regional data center options to meet regulatory requirements or other geo-specific data storage needs.

Canadian data centers

All data is stored in data centers located within Canada.

- Primary data center: Azure Central Canada (Ontario)
- Secondary data center: Azure East Canada (Quebec)

Australian data centers

All data is stored in data centers located within Australia.

- Primary data center: Azure East Australia (New South Wales)
- Secondary data center: Azure Central Australia (Canberra)

For more information, see [About ClearID architecture](#).

User activity report

Account administrators can now review activity related to identities and supervisors in the User activity report. It's now possible to filter results in the Activity type column to display activities for these action types:

- Supervisor added or removed
- Identity created, updated, or deleted

For more information, see [About user activity report](#) and [Viewing a user activity report](#).

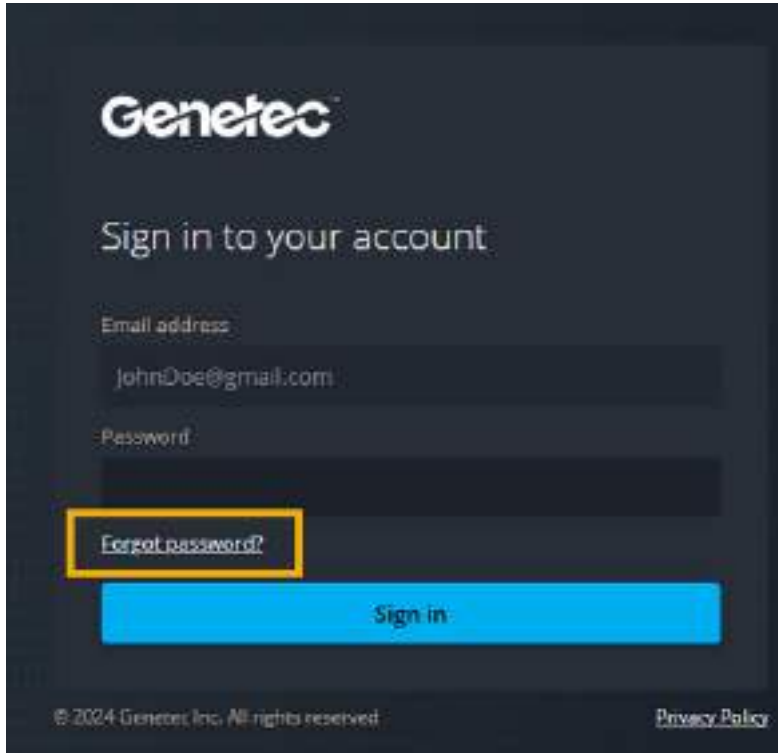
What's New: April 2024

Updates to the ClearID sign in system

An update has been made to the ClearID sign in system that might affect your organization. Users who don't use a single sign-on (SSO) integration might need to reset their passwords the first time they sign in to ClearID. As part of the transition:

- Multifactor authentication (MFA) is mandatory for all users that sign into Genetec™ applications.
- A code is sent to the email address associated with the user's account to act as a second factor for authentication.

NOTE: This change doesn't affect users in organizations that integrate their corporate identity system with ClearID. These users can continue to use the SSO functionality that their organization provides.



For more information, see [Resetting user passwords](#).

What's New: February 2024

Tracking entities managed by ClearID in Synergis™

You can now track entities managed by ClearID in Config Tool and Security Desk. These entities are highlighted with a blue dot in the bottom-right corner of the entity icon. For example:

Access rules ()

For more information, see [How the ClearID plugin works with Security Center](#).

Zebra DS 9300 QR code scanner support

ClearID now supports the Zebra DS 9300 QR code scanner.

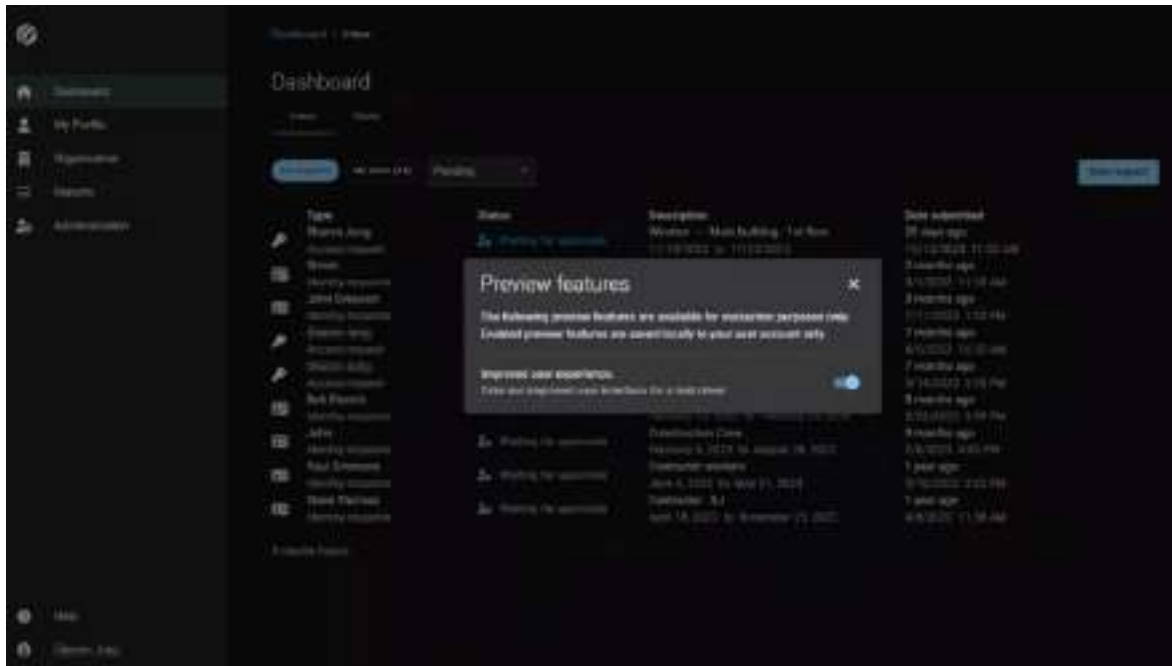


For more information, see [Supported devices for ClearID](#), [Enabling visitor management for sites in ClearID](#), or refer to the manufacturer documentation.

What's New: December 2023

Preview features

ClearID now includes a preview features option. Users can enable one or more preview features (when available) to get early access to new functions before they are released.

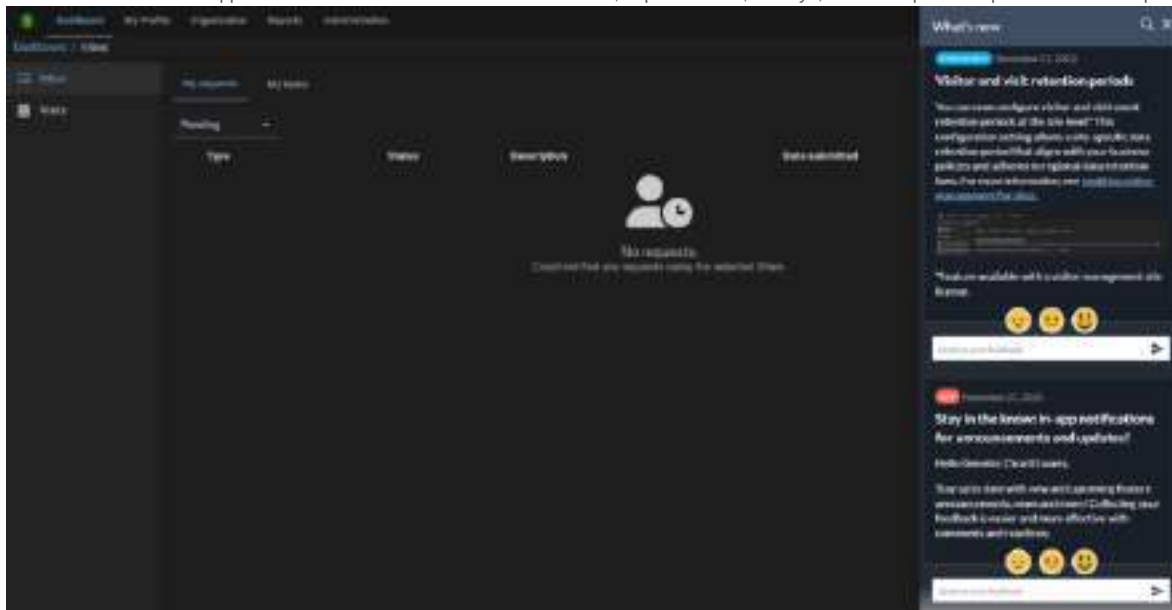


NOTE: Preview features are for evaluation purposes only. Enabled preview features are saved locally to your user account only.

For more information, see [Enabling preview features in ClearID](#) and [Disabling preview features in ClearID](#).

In-app notifications

ClearID now includes in-app notifications for new feature announcements, improvements, surveys, and other product updates in the web portal.



Stay up to date with new and upcoming feature announcements, news, and more. Collecting your feedback is now even easier. You can submit emoji reactions or send feedback for each announcement or notification directly to the product team.

ClearID architecture update

Identity data processing has changed.

For more information about which data centers are used in the Global deployment, see the *Microsoft Corporation* entry in the ClearID section of the [Genetec Subprocessors](#) list.

Genetec ClearID™ Self-Service Kiosk 1.13.9

ClearID Self-Service Kiosk mobile app version 1.13.9 is now available.

This maintenance update includes the following:

- Performance improvements
- iOS 17.1.1 compatibility update

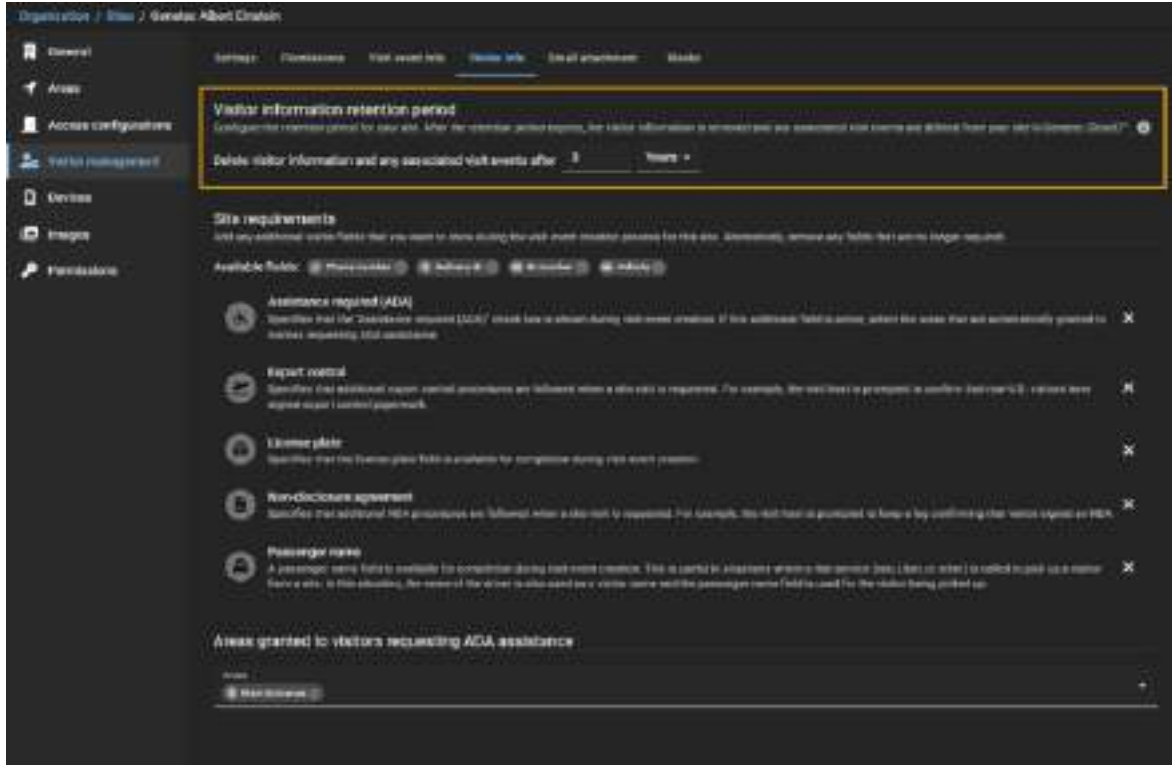
To download the ClearID Self-Service Kiosk mobile app, visit the [App Store](#).

What's New: November 2023

Data retention for visitors

You can now configure a retention period for visitor information. After the retention period expires, the visitor information is removed and any associated visit events are deleted from your site in ClearID.

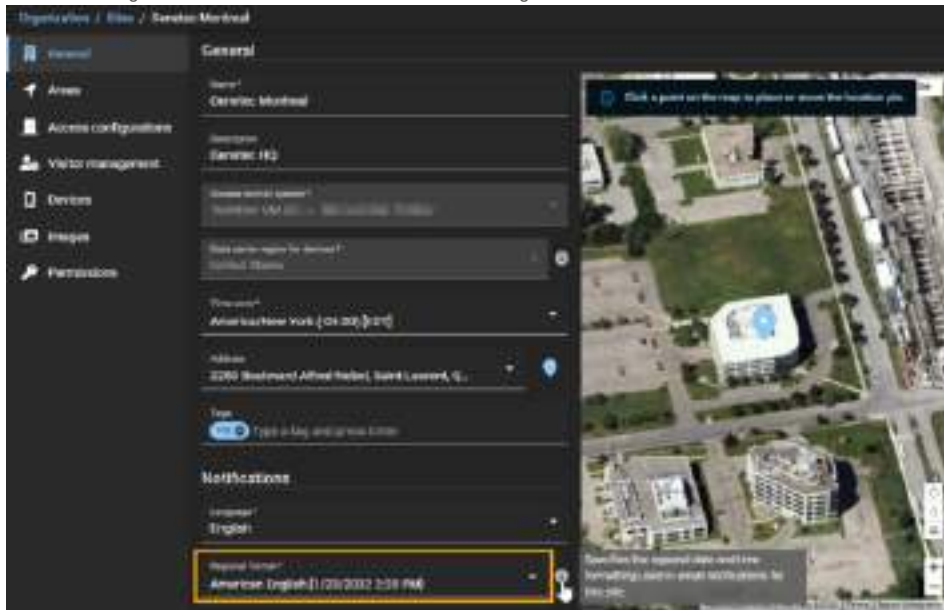
NOTE: The retention period is configurable by site to comply with the different data laws that might apply in your region.



For more information, see [Enabling visitor management for sites in ClearID](#).

Email notifications

You can now configure your email notifications to specify a Regional format that is relevant for your sites. The email notifications display the date and time using the selected regional format that is the local standard in the region where the site is located.

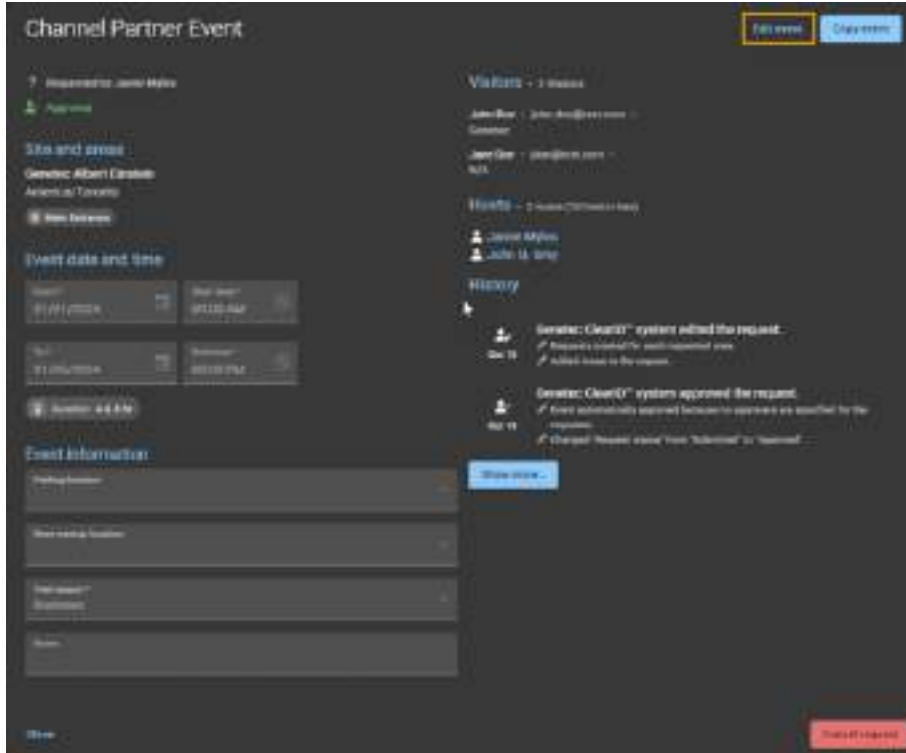


For more information, see [Creating sites in ClearID](#) and [Modifying sites in ClearID](#).

Updating scheduled visit events

You can now modify visit events to change the event details, or to add or remove visitors or hosts. Updating the visit event details ensures that your visitors are always kept up to date following any changes to an upcoming event.

NOTE: Events can only be modified before the start of the visit event.



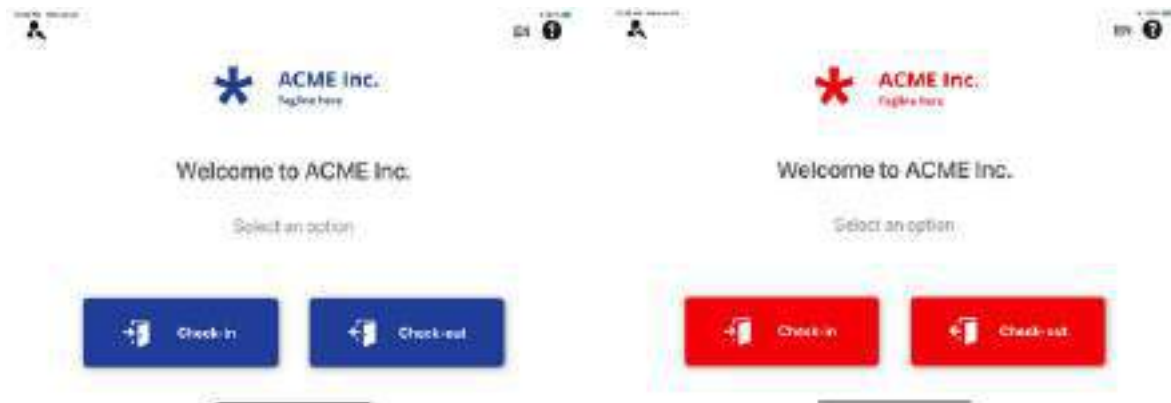
For more information, see [Modifying visit events in ClearID](#).

What's New: October 2023

Kiosk customization

The Genetec ClearID™ Self-Service Kiosk has been enhanced to include kiosk theme customization.

The following examples show the white kiosk theme with an accent color.



You can choose a white kiosk theme. When you choose the white kiosk theme, you can also choose one of ten accent colors. Alternatively you can enter a specific HEX color code value to align with your corporate branding.



For more information, see [Customizing the ClearID Self-Service Kiosk configuration](#) or [Enabling visitor management for sites in ClearID](#).

Genetec ClearID® User Guide
Displayed in the header

Genetec ClearID Self-Service Kiosk 1.13.8

ClearID Self-Service Kiosk mobile app version 1.13.8 is now available.

The Kiosk mobile app now supports the following:

- Kiosk Theme customization
- Translation updates for check-in, check-out, and welcome screen or assistance messages.

For more information, see [Customizing the ClearID Self-Service Kiosk configuration](#) or [Enabling visitor management for sites in ClearID](#).

To download the Genetec ClearID™ Self-Service Kiosk mobile app, visit the [App Store](#).

What's New: August 2023

Reports

ClearID now includes two more reports for audit trail and activity tracking purposes:

Identity requests report

Account administrators can now use the Identity requests report to review all activities related to identity requests.

Identity requests report					
Request date 		Requested by 	Name 	Identity template 	Status 
From Aug 15, 2022 to Aug 22, 2022					Reviewers 
February 2, 2023 at 9:07 AM		Supervisor1	Anna Smith	Toronto A	Completed  1 reviewers 
November 30, 2022 at 8:10 AM		Supervisor1	Charlie Brown	Toronto	Completed  1 reviewers 
November 11, 2022 at 6:03 AM		Contractor Manager	Devin Jones	Toronto	Completed  1 reviewers 

For more information, see [About reports in ClearID](#), [About identity requests report in ClearID](#), and [Checking the status of identity requests in ClearID](#).

Direct reports report

Supervisors or account administrators can now use the Direct reports report to check their direct reports access control status and general identity information.

[illegible]

For more information, see [About reports in ClearID](#), [About direct reports report in ClearID](#), and [Viewing direct reports in ClearID](#).

Kiosk kit update

The ClearID Self-Service Kiosk kits now include and support the 10th generation 10.9 inch Apple iPad.

For more information, see [ClearID Self-Service Kiosk options](#) and [Supported devices for ClearID](#).

What's New: July 2023

One Identity Synchronization Tool

The Genetec ClearID™ One Identity Synchronization Tool has been updated to simplify synchronization and also to resolve the End of Life (EOL) of the Microsoft Azure AD Graph.

IMPORTANT: The Microsoft Graph library replaces the now End of Life (EOL) Azure Active Directory Graph library (EOL since June 30, 2023 - [Azure AD Graph API end of life](#)). The new library supports all previous mappings.

Who is affected? ClearID customers who are using Azure AD as the data source to synchronize their identities in ClearID with the One Identity Synchronization Tool.

For more information, see the official documentation from Microsoft: [Migrate your apps from Azure AD Graph to Microsoft Graph](#).

Next steps? Get in touch with your ClearID team deployment contact to upgrade the One Identity Synchronization Tool.

NOTE: If you are not using Azure AD as a data source, these events do not affect you and you do not require an upgrade.

For more information about the synchronization tool, see [Synchronizing identities using One Identity Synchronization Tool in ClearID](#).

For more information about Azure AD API permissions, see [About the Azure web app for ClearID One Identity Synchronization Tool](#).

What's New: June 2023

Genetec ClearID Self-Service Kiosk 1.13.7

ClearID Self-Service Kiosk mobile app version 1.13.7 is now available.

The Kiosk mobile app now supports the following:

- Brother QL-820NWbc label printer
- iOS 16
- 135 new or updated Identity Document (ID) types

For more information, see [Supported devices for ClearID](#), [ClearID Self-Service Kiosk options](#), [Configuring the ClearID Self-Service Kiosk label printer \(Brother QL-820NWBc, QL-820NWB, or QL-810W\)](#), and [Identity document types in ClearID](#).

To download the Genetec ClearID™ Self-Service Kiosk mobile app, visit the [App Store](#).

What's New: May 2023

Custom fields updates

ClearID custom fields information has been updated to help you understand the relationship between ClearID identity field names and Security Center entity type fields.

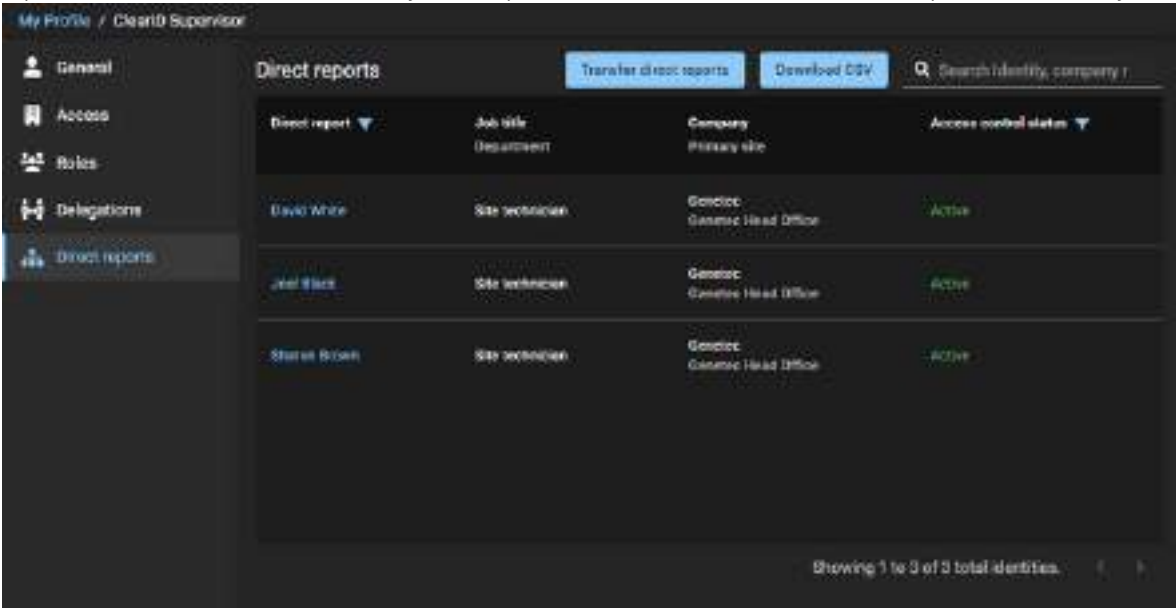
[illegible]

For more information, see [About custom fields in ClearID](#), [Modifying ClearID custom fields in Config Tool](#), and [Custom fields relationships](#).

What's New: March 2023

Transfer direct reports

Supervisors, account administrators, or an identity with write permissions for identities can now transfer direct reports to another identity.



IMPORTANT: This function is intended for identities that are locally managed in ClearID. If identities are managed using an external data source, the transfer of direct reports will be overwritten.

For more information, see [Transferring direct reports](#).

Synergis™ licensing changes

Synergis licensing has changed. For Security Center 5.11 or later (Synergis Base Enterprise or Synergis Base Professional) the Synergis visitor management module is now included by default.

NOTE: The Synergis visitor management module is required if the ClearID customer has the CD-SITE-VM-1Y ClearID license.

For more information, see [License options for ClearID system integration](#).

What's New: February 2023

Genetec ClearID Self-Service Kiosk 1.13.6

Genetec ClearID Self-Service Kiosk mobile app version 1.13.6 is now available.

The Genetec ClearID Self-Service Kiosk mobile app version 1.13.6 now supports the following:

- Brother TD-4550DNWB thermal printer (with pre-cut labels).

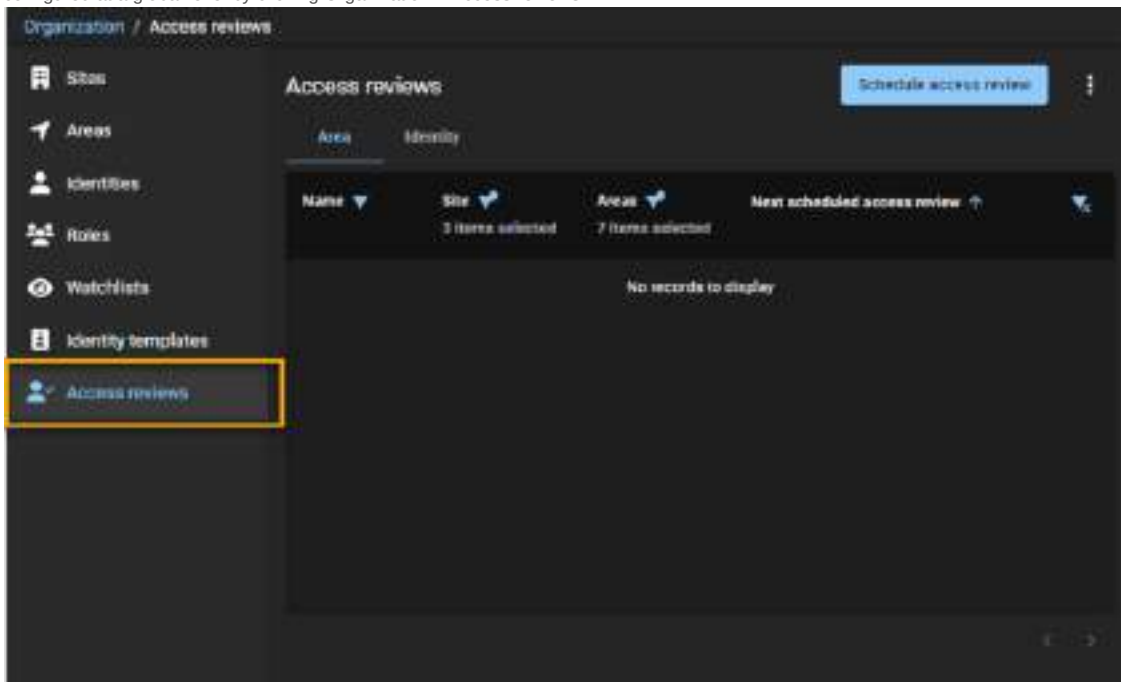
For more information, see [Supported devices for ClearID](#), [ClearID Self-Service Kiosk options](#), and [Configuring the ClearID Self-Service Kiosk label printer \(Brother TD-4550DNWB\)](#).

To download the Genetec ClearID™ Self-Service Kiosk mobile app, visit the [App Store](#).

IMPORTANT: User interface changes

Access reviews have moved

Previously access reviews were created and scheduled at a site level by clicking Organization > Sites > Access reviews. Access reviews settings are now configured at a global level by clicking Organization > Access reviews.

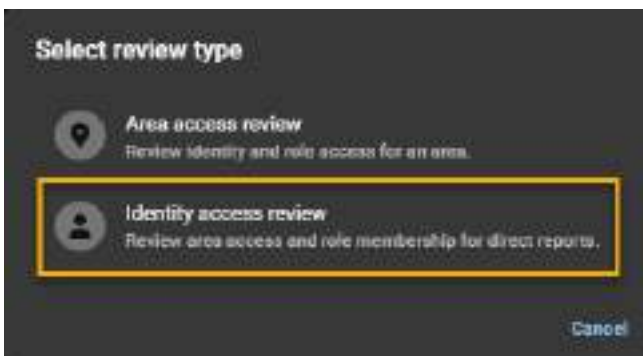


Access reviews enhancements

Access reviews

Access reviews now include a new Identity access review option.

An identity access review is the process where a supervisor reviews their direct reports access. This review includes confirming or updating area access, access control date range, or role membership for their direct reports to ensure security compliance and audit readiness.

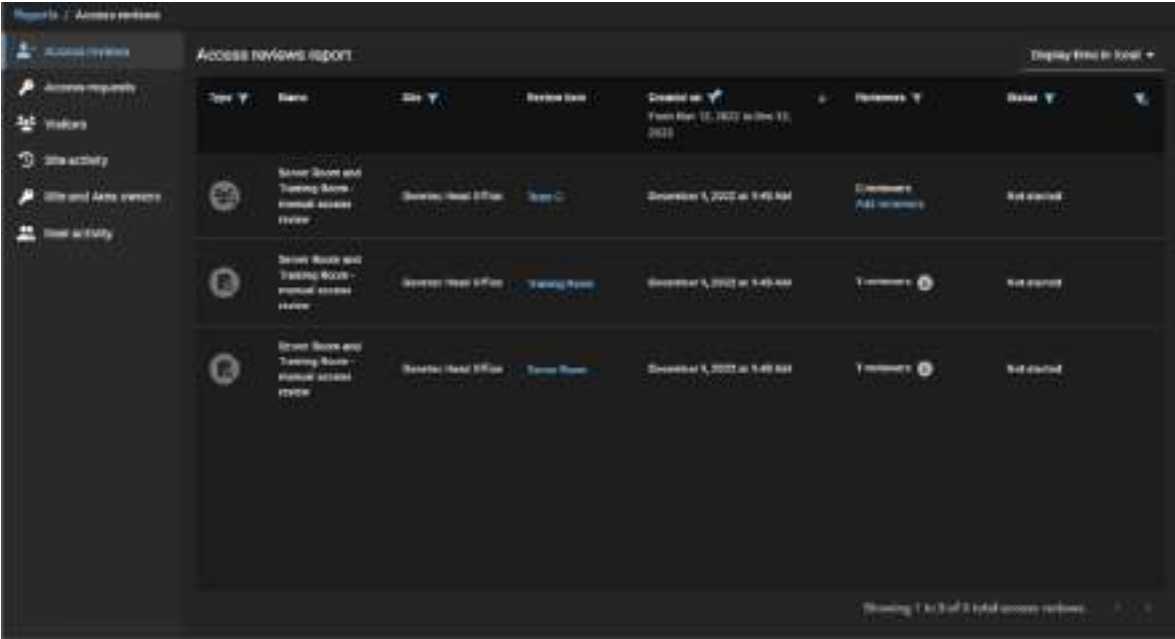


Access reviews also include updates to the Site access review schedule dialog.

For more information, see [Setting up area access reviews in ClearID](#) and [Setting up identity access reviews in ClearID](#).

Access reviews report updates

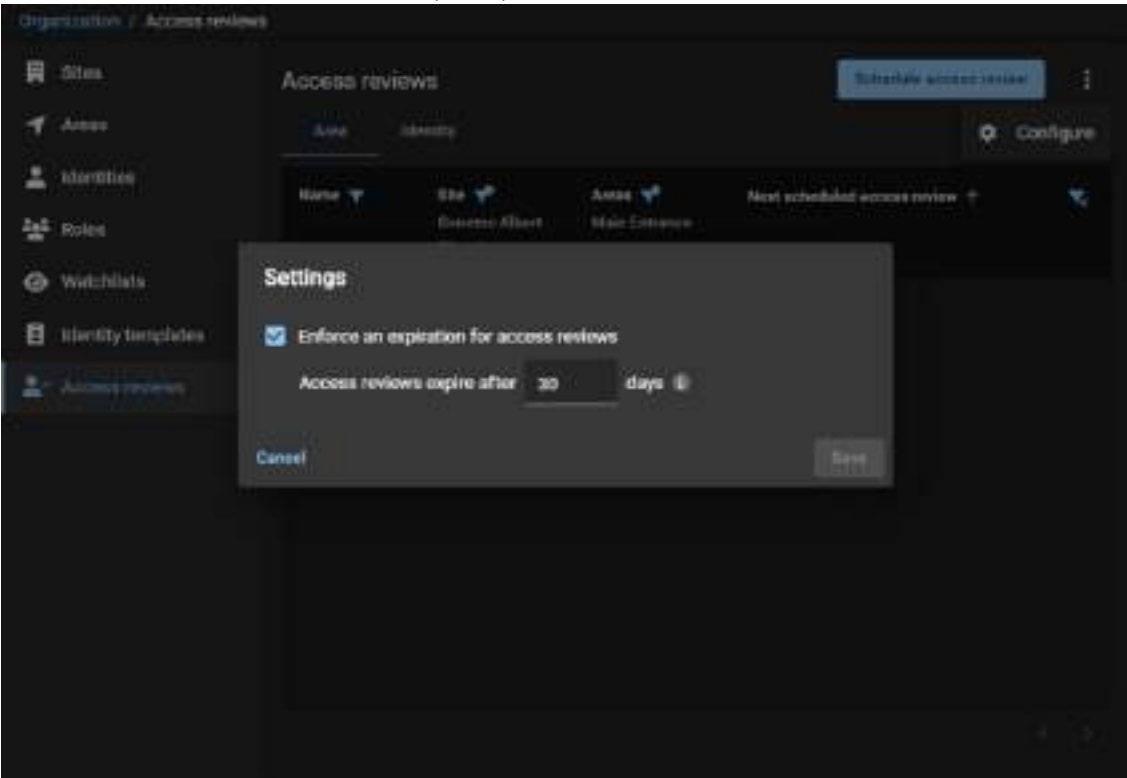
Access reviews report now includes updates to report data and filtering.



For more information, see [About access reviews report in ClearID](#) and [Checking the status of access reviews in ClearID](#).

Automatic expiration for access reviews

Account administrators can now set an automatic expiration period for all access reviews.



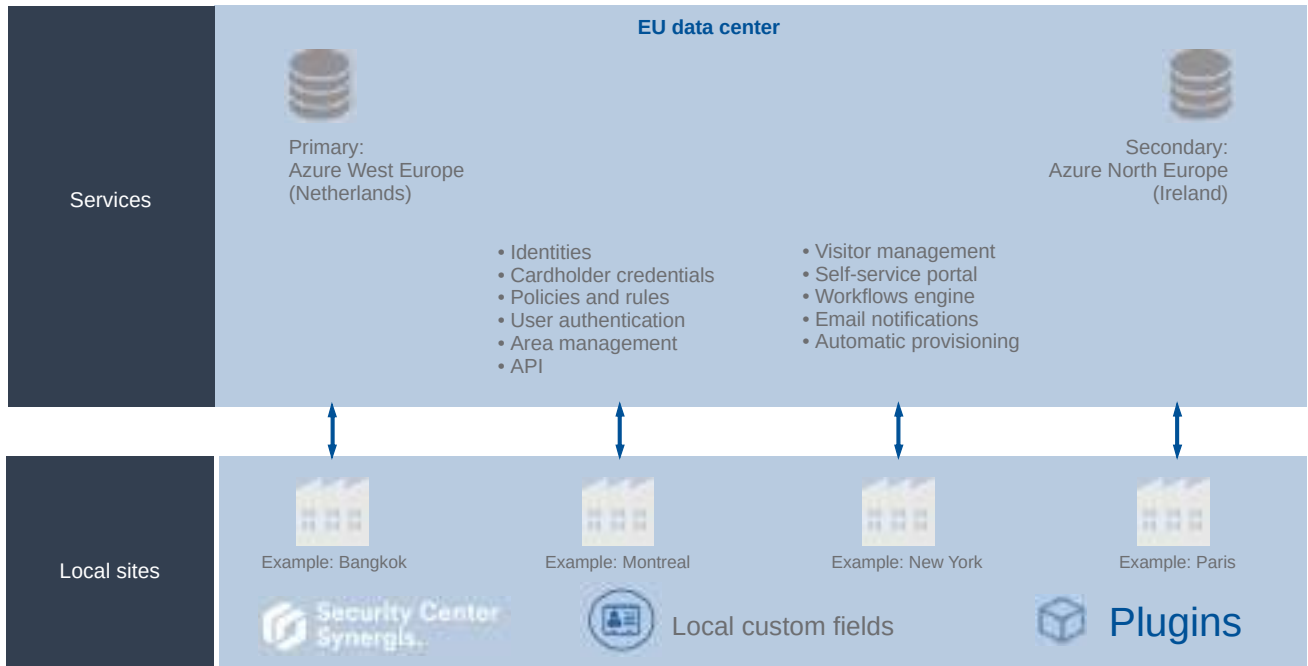
For more information, see [Setting up automatic expiration for access reviews](#).

What's New: January 2023

Europe only architecture (NOW AVAILABLE)

ClearID now includes a Europe only solution for customers who require all their data to be stored in Europe.

Genetec ClearID™ Europe only architecture



For more information, see [About ClearID architecture](#).

What's New: November 2022

Supervisor permissions enhanced

Administrators can now grant supervisors more control to manage their direct reports. Supervisors can now modify General identity information fields and Access control settings.



This option is useful for any organization that wants to decentralize some administration functions by allowing supervisors to manage their direct reports.

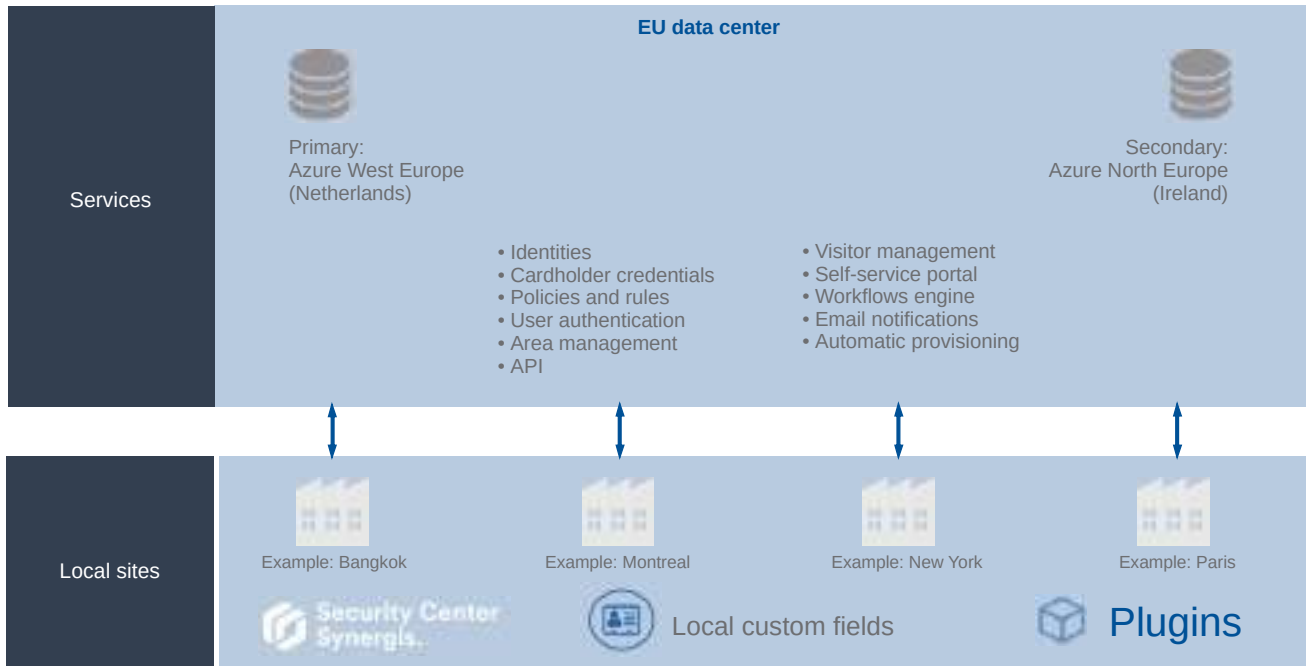
For more information, see [Managing direct reports in ClearID](#).

What's New: Coming soon

Europe only architecture (coming soon)

ClearID now includes a Europe only solution for customers who require all their data to be stored in Europe.

Genetec ClearID™ Europe only architecture



For more information, see About ClearID architecture.

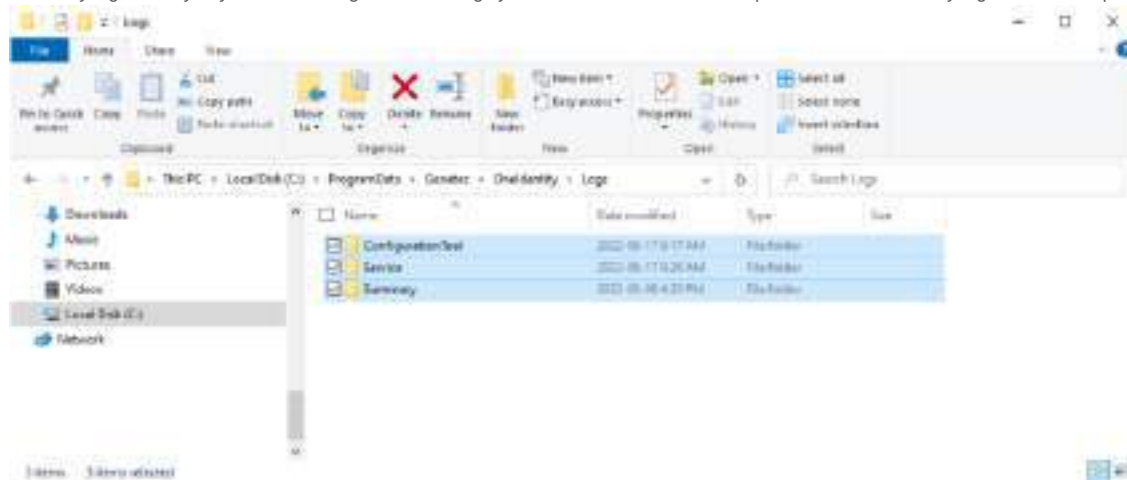
What's New: September 2022

Genetec ClearID One Identity Synchronization Tool

The Genetec ClearID One Identity Synchronization Tool has been updated and now supports the following:

Improved logging

Summary logs identify any issues that might occur during synchronization. Read the Recap.txt file in the Summary logs folder for a quick synchronization overview.



For more information, see Viewing the ClearID One Identity Synchronization Tool logs.

Microsoft Graph library replaces Azure Active Directory Graph library

The Microsoft Graph library replaces the now deprecated Azure Active Directory Graph library. The new library supports all previous mappings.

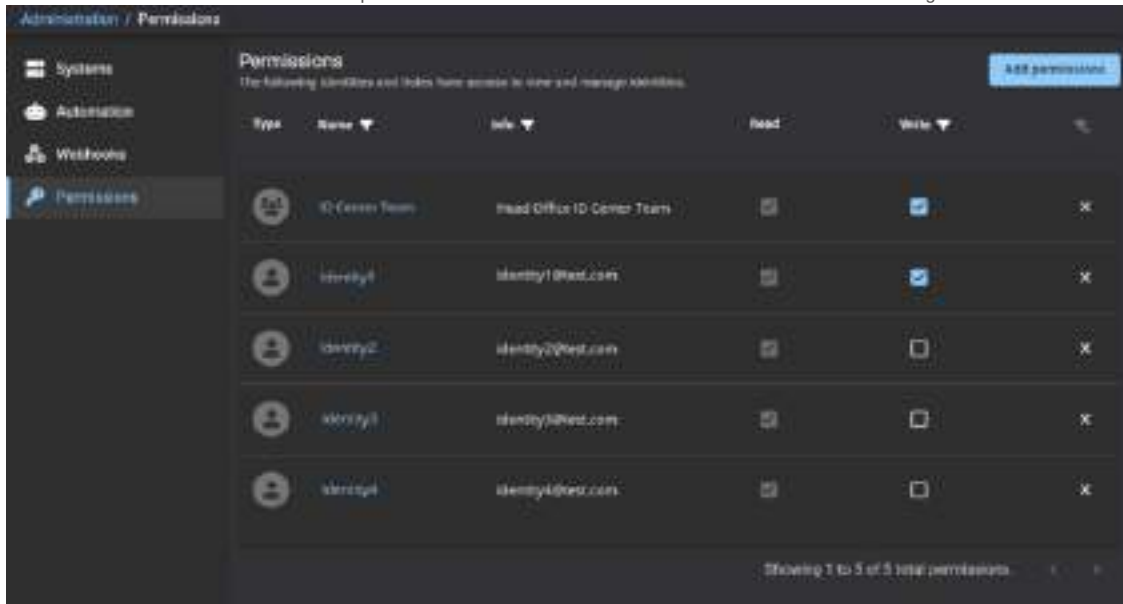
For more information, see About the Azure web app for ClearID One Identity Synchronization Tool.

For more information about the synchronization tool, see Synchronizing identities using One Identity Synchronization Tool in ClearID.

What's New: August 2022

Identity permissions

Account administrators can now add extra permissions to identities or roles so that the users can view or manage identities.



For more information, see [Granting additional permissions](#).

What's New: July 2022

Genetec ClearID Self-Service Kiosk 1.13.3

Genetec ClearID Self-Service Kiosk mobile app version 1.13.3 is now available.

The Genetec ClearID Self-Service Kiosk mobile app version 1.13.3 now supports the following Identity Document (ID) types:

- UAE - Driving License
- UAE - ID card
- UAE - Resident ID

For more information, see [Identity document types in ClearID](#).

To download the Genetec ClearID™ Self-Service Kiosk mobile app, visit the [App Store](#).

What's New: May 2022

ClearID best practices

ClearID User Guide now includes best practices information for the following:

- Setting up ClearID for a new Synergis system.
- Setting up ClearID with an existing Synergis system.

You can use the best practices to help plan your ClearID system deployments.

For more information, see [ClearID Best practices](#).

Requesting identities

An identity request wizard is now available to submit either an individual identity request or multiple identities request (CSV import) for different types of employees or contractors. Individual identity requests or multiple identities requests can be repeated using a template for specific employees who require the same access to a specific site, area, or building.

The following example shows an individual identity request:

The screenshot shows the 'identity request' wizard in the 'General information' step. The progress bar at the top indicates four steps: 1. Identity template (completed), 2. General information (current), 3. Work details, and 4. Review. The 'General information' section contains several input fields: 'First name' with the value 'John', 'Last name' with 'Doe', 'Email' with 'johndoe@test.com', 'Middle name' (empty), 'Mobile phone number' with '123-456-7899', 'Preferred name*' with 'John Doe', and 'External ID' (empty). Below this is a 'Web portal access' section with a toggle for 'Grant user access to the web portal' set to 'N/A'. At the bottom, there is a 'Save as draft' button, a 'Back' button, and a 'Next' button.

The following example shows an identities request (CSV import):

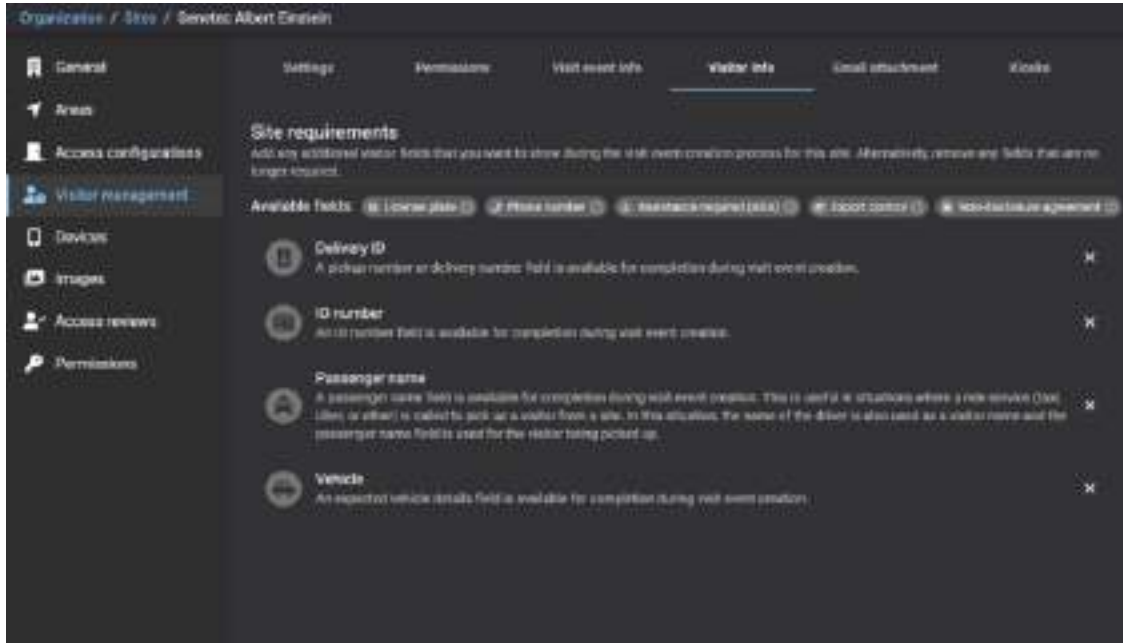
The screenshot shows the 'Request identities' wizard in the 'Import' step. The progress bar at the top indicates three steps: 1. Basic information (completed), 2. Import (current), and 3. Review. The 'Import identities' section contains a text block explaining the import process: 'Import your identities for this request below. If any data errors are encountered during the identities import, fix the issues in the CSV file then import the file again. CAUTION: Importing the file again overwrites any data already imported into the grid.' Below this text is a large 'Import from CSV' button. Underneath the button, it says 'No records to display' above an empty table grid. At the bottom right, it says '0 total results'. At the bottom left is a 'Cancel' button, and at the bottom right are 'Back' and 'Next' buttons.

For more information, see About workflows in ClearID, Creating an identity template in ClearID, Requesting an identity in ClearID, and Requesting multiple identities using a CSV import in ClearID.

Visitor management enhancements

Visitor management for sites now includes more optional visitor information fields for the following:

- Delivery ID
- ID number
- Passenger name
- Vehicle



For more information, see the Visitor info tab in [Enabling visitor management for sites in ClearID](#).

What's New: March 2022

Genetec ClearID Self-Service Kiosk 1.13.1

Genetec ClearID Self-Service Kiosk mobile app version 1.13.1 is now available.

The ClearID Self-Service Kiosk mobile app version 1.13.1 now supports 78 additional Identity Document (ID) types and includes some additional countries.

For more information, see [Identity document types in ClearID](#).

To download the Genetec ClearID™ Self-Service Kiosk mobile app, visit the [App Store](#).

What's New: January 2022

Reports

ClearID now provides three more reports for audit trail and activity tracking purposes:

Genetec ClearID[®] User Guide
Displayed in the header

Site and area owners report

Account Administrators can now use the Site and area owners report to get a global view of all identities and their permissions. When the report is used by a site owner, only information about their own sites is shown.

Genetec

Dashboard

My Profile

Organization

Plans & Billing

Administration

Reports

[Access Events](#)
[Access Requests](#)
[Visitor Records](#)
[Video](#)
[Get a Quote](#)
[Get a Demo](#)
[Admin Panel](#)

Day 1

Day 2

Day 3

Accesses 1

Accesses 2

Accesses 3

Accesses 4

Accesses 5

Accesses 1							
Accesses 2							
Accesses 3							
Accesses 4							
Accesses 5							
Accesses 6							
Accesses 7							
Accesses 8							
Accesses 9							
Accesses 10							
Accesses 11							
Accesses 12							
Accesses 13							
Accesses 14							
Accesses 15							
Accesses 16							
Accesses 17							
Accesses 18							
Accesses 19							
Accesses 20							

For more information, see [About reports in ClearID](#) and [Viewing a site and area owners report in ClearID](#).

User activity report

Account administrators can now use the User activity report to review all activities related to users.

The screenshot displays the 'Reports' section of a system, specifically the 'Total activity' tab. It shows a table of user activities with the following columns: Time stamp, Activity type, Performed by, and Details. The data is filtered for the period from Feb 03, 2020 to May 23, 2020. The activities listed include adding and removing area managers, adding and removing members, and adding and removing coordinators, all performed by Erikka Della Cappa.

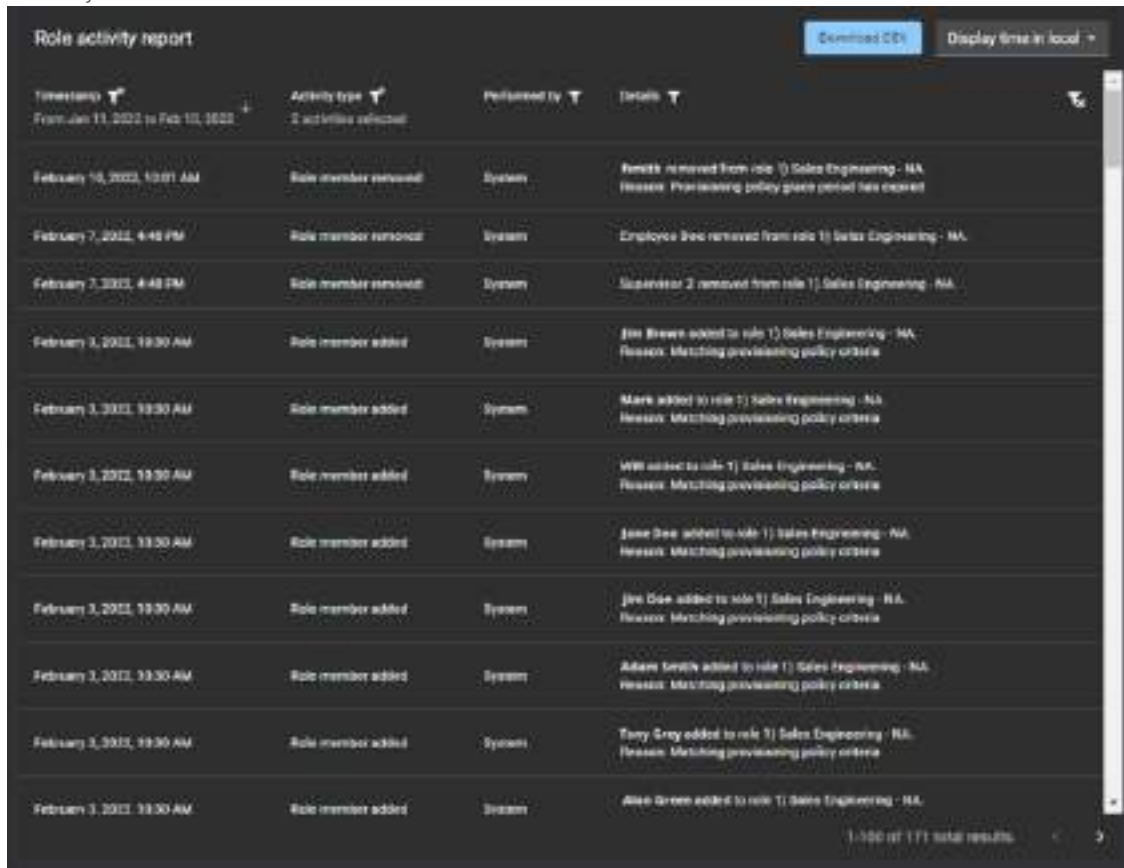
Time stamp	Activity type	Performed by	Details
April 2, 2020 at 1:52 PM	Area manager added	Erikka Della Cappa	Erikka Della Cappa added as area approver for Main Endowment
April 2, 2020 at 11:16 AM	Area member added	jack	Erikka Della Cappa added as area member for Main Endowment
April 2, 2020 at 11:16 AM	Area manager removed	jack	Erikka Della Cappa removed as area approver from Main Endowment
April 2, 2020 at 11:06 AM	Role member added	Erikka Della Cappa	Erikka Della Cappa added to user Identity Requests Decision: Unable to approve Identity Requests
April 2, 2020 at 11:07 AM	Role member added	Erikka Della Cappa	Erikka Della Cappa added to role Coordinator Manager Decision: Erikka Della Cappa Coordinator Manager
April 2, 2020 at 11:07 AM	Role member added	Erikka Della Cappa	Erikka Della Cappa added to role Certified Decision: Erikka Della Cappa Certified

Showing 1 to 5 of 13 total user activities.

For more information, see [About reports in ClearID](#) and [Viewing a user activity report in ClearID](#).

Role activity report

Account administrators can now use the Role activity report to review all activities related to roles. When the report is used by role managers or role owners, only the activity for their roles is shown.



Timestamp	Activity type	Performed by	Details
From Jan 11, 2022, to Feb 10, 2022	2 activities selected		
February 10, 2022, 10:01 AM	Role member removed	System	Remita removed from role 1) Sales Engineering - NA. Reason: Provisioning policy grace period has expired
February 7, 2022, 4:48 PM	Role member removed	System	Employee Dev removed from role 1) Sales Engineering - NA.
February 7, 2022, 4:48 PM	Role member removed	System	Supervisor 2 removed from role 1) Sales Engineering - NA.
February 3, 2022, 10:30 AM	Role member added	System	Joe Brown added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Mark added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Will added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Jane Doe added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Jim Doe added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Adam Smith added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Tony Grey added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Alice Green added to role 1) Sales Engineering - NA.

1-100 of 171 total results

For more information, see [About reports in ClearID](#) and [Viewing a role activity report in ClearID](#).

ClearID plugin

The ClearID plugin is a new integration for Security Center 5.7 SR6 or later.

3 | Deployment preparation

3.1 | License options for ClearID system integration

Use the following information to understand the licenses that are available for Genetec ClearID™ or the Genetec ClearID™ Self-Service Kiosk. To update your license, contact us and provide the part numbers listed in this topic.

ClearID license options

Part number	Description	Requirements
CID-DELIVERY	Remote support services for initial account setup of ClearID cloud-based service. These services include a block of eight hours of support. Services are rendered during local business days and normal business hours.	All services must be used within twelve months of your first support call. At the end of this twelve-month period, the full service fee is billed, and any unused support hours expire.
- CID-IDENTITY-1Y - CID-IDENTITY-3Y - CID-IDENTITY-5Y	One ClearID Identity license for one, three, or five years. An identity is a unique individual that is managed, governed, or authenticated by the system. The license includes two hours of ClearID deployment consultation.	This part is mandatory to use ClearID.
- CID-MULTI-SYSTEM-1Y - CID-MULTI-SYSTEM-3Y - CID-MULTI-SYSTEM-5Y	One ClearID multi-system license for one, three, or five years. Enables management and synchronization across multiple systems.	This part is mandatory to connect ClearID to two or more Security Center systems. NOTE: Only one system is required to support a ClearID account.

Part number	Description	Requirements
- CID-KIOSK-LIC-1Y - CID-KIOSK-LIC-3Y - CID-KIOSK-LIC-5Y	One ClearID kiosk license for one, three, or five year.	Each kiosk must be licensed. NOTE: The ClearID Self Service Kiosk app on an iPhone doesn't need to be licensed.

Synergis license options

To synchronize data between ClearID and Synergis™, one of the following part numbers is required:

NOTE: The following Synergis license options all include the CD-SC-PLUGIN by default. This package provides a license for one connection to ClearID cloud services. You need one license per Directory.

Part number	Description	Requirements
GSC-BASE-E 5.11 or later	The Synergis Base Enterprise package. NOTE: The base package includes the Synergis visitor management module by default.	
GSC-BASE-P 5.11 or later	The Synergis Base Professional package. NOTE: The base package includes the Synergis visitor management module by default.	
SCS-Base	Security Center SaaS Edition (Classic) - Base Package NOTE: The base package includes the Synergis visitor management module by default.	

Does your Security Center license include all the options you need?

In addition to a certificate for your plugin, ensure that your Security Center license includes all the options you expect to use in Security Center. For example, if you've integrated a system that has visitors, you need the Visitors option in Security Center. If an option is missing, an error message is displayed when the server tries to create or modify the entity related to that option.

For a list of available license options, see [License options in Security Center](#).

Browse

- Integration overview for the ClearID plugin
- ClearID Self-Service Kiosk options

3.2 | Compatibility for ClearID

The Genetec ClearID™ web portal and the ClearID plugin are compatible with Security Center 5.11 or later.

The web portal and plugin support Security Center versions for a maximum of 3 years after the first GA release date.

Supported Security Center versionsUse the following information to help you understand when each Security Center version will no longer be supported for use with ClearID:

Security Center version	Security Center first GA release date	Security Center end of support in ClearID
5.11	September 2022	September 2025
5.12	December 2023	December 2026
5.13	December 2024	December 2027

IMPORTANT: You must have Synergis™ Professional or Enterprise to use ClearID. For more information, see [License options for ClearID system integration](#).

3.3 | System requirements for ClearID

For the Genetec ClearID™ system to run efficiently in your web browser, the computer or mobile device that you use must meet certain software and hardware requirements.

The requirements for ClearID web application are as follows:

Desktop requirements

- Cookies and JavaScript are enabled in your web browser.

The ClearID web application is compatible with the following web browsers:

- Google Chrome (latest version)
- Microsoft® Edge (latest version)

ClearID plugin requirements

The following system requirements must be met to run the ClearID plugin:

Synergis Professional or Omnicast Professional is required for plugins support in Security Center.

Hardware

The ClearID plugin must be installed on a server that meets the recommended specifications, as described in the [Security Center system requirements](#).

Networking

The server that the plugin is installed on requires internet access to communicate between Synergis™ and ClearID cloud services. All communications use TCP port 443.

IMPORTANT: All data uploaded to the ClearID web application remains encrypted in transit and at rest.

3.4 | Firewall ports used in ClearID

To ensure that Genetec ClearID™ works as designed, the following ports, URLs, and network requirements must be met.

ClearID web portal

The following network configuration is required for the web portal:

- TCP Port 443 outbound
- *.clearid.io - Allow all outbound traffic for this domain
- *.core.windows.net - Allow all outbound traffic for this domain
- *.launchdarkly.com - Allow all outbound traffic for this domain

ClearID plugin

The following network configuration is required for the plugin:

- TCP Port 443 outbound
- *.clearid.io - Allow all outbound traffic for this domain
- *.servicebus.windows.net - Allow all outbound traffic for this domain
- *.core.windows.net - Allow all outbound traffic for this domain

NOTE: The server that the plugin is installed on requires internet access to communicate between Synergis™ and ClearID cloud services.

Genetec ClearID™ One Identity Synchronization Tool

The following network configuration is required for the One Identity Synchronization Tool:

- TCP Port 443 outbound
- *.clearid.io - Allow all outbound traffic for this domain

Genetec ClearID™ LDAP Synchronization Agent

The following network configuration is required for the LDAP Synchronization Agent:

- TCP Port 443 outbound
- *.clearid.io - Allow all outbound traffic for this domain

Genetec ClearID™ Self-Service Kiosk

The following features or network configuration are required for the Self-Service Kiosk:

- TCP Port 443 outbound
- *.clearid.io - Allow all outbound traffic for this domain
- Label Printer (Wi-Fi mode only) Bonjour - used for device search
- Label Printer (Wi-Fi mode only) SNMP - used for checking printer status information
- Label Printer (Wi-Fi mode only) UDP or TCP Port 9100 - used for sending print data

Other requirements

The following resources are used by ClearID to enhance the user experience, but they are not mandatory.

Google Maps:

- <https://www.google.com/>
- <https://maps.googleapis.com>
- <https://fonts.googleapis.com/>
- <https://maps.gstatic.com/>

Microsoft Application Insights:

- <https://dc.services.visualstudio.com/>
- <https://dc.applicationinsights.azure.com/>
- <https://dc.applicationinsights.microsoft.com/>

NOTE: These resources do not prevent you from using the ClearID portal, but some elements of the user interface might not format correctly unless these resources are available.

3.5 | Supported devices for ClearID

To help you understand the hardware devices that are supported for use with Genetec ClearID™ or the Genetec ClearID™ Self-Service Kiosk, use this supported devices list.

For each device, the corresponding firmware and certification level is listed.

Certified

Genetec Inc. has tested and validated the device.

Supported by design

The device has the same design characteristics as a certified device, but Genetec Inc. has not tested or validated the device.

Kiosk devices

The following iPad devices are supported for use with the ClearID Self-Service Kiosk.

Manufacturer	Model	Device type ¹	Version
Apple	Not applicable	• iPad 11.0 inches • iPad 10.9 inches • iPad 10.2 inches	Certified: iOS 16.1 or later

NOTE:

- ¹ Other iPad devices might also be supported (without kiosk stand) if they are running the Minimum iOS version required for the Kiosk mobile app. For example, the iPad Pro could be used. However, due to the iPad Pro physical dimensions it is not compatible with the Kiosk stand. For information about iPad power adapter requirements, see *ClearID Self-Service Kiosk options*.

Kiosk label printer

The following label printer devices are supported for use with the ClearID Self-Service Kiosk.

Manufacturer	Model	Device type	Version
Brother	QL-820NWBc (Network, Wi-Fi, Bluetooth) NOTE: Only DK-2205 or DK2251 (62mm Black or Red and Black) labels are supported for this printer.	Thermal Label Printer	Supported by design
Brother	QL-820NWB (Network, Wi-Fi, Bluetooth)	Thermal Label Printer	Supported by design (DEPRECATED) NOTE: The QL-820NWBc replaces the discontinued QL-820NWB printer.
Brother	QL-810W	Thermal Label Printer	Supported by design

Genetec ClearID®; User Guide

Displayed in the header

Manufacturer	Model	Device type	Version
	(Wi-Fi only)		
Brother	TD-4550DNWB (Network, Wi-Fi, Bluetooth) NOTE: Only RD001U1S (57mm Black) labels are supported for this printer.	Thermal Label Printer	Supported by design

QR code (2d barcode reader) devices

The following devices are supported for use with ClearID when using QR codes as a credential for visitors.

Manufacturer	Series	Model	Device type	Version
IBC	Qscan	Qscan (for parking lots)	Barcode scanner	Supported by design: Firmware qswie26m.bin
IBC	Qscan	QscanT (for turnstiles)	Barcode scanner	Supported by design
IBC	Qscan	QscanI (indoor version)	Barcode scanner	Supported by design
Zebra	DS9300	DS9308	Barcode scanner	Supported by design

STid OSDP devices

The following STid OSDP devices are supported for use with ClearID when using QR codes as a credential for visitors.

Manufacturer	Series	Model	Part Number	Device type	Version
STid	Architect®	ARC-AQ	SY-ARC-W33-AQPH5-7OS1	QR code reader - Classic Reader - QR Code Module	Supported by design All STid readers Firmware version 10 or later ¹
STid	Architect®	ARC-BQ	SY-ARC-W33-BQPH5-7OS1	QR code reader - Keypad Reader - QR module	Supported by design All STid readers Firmware version 10 or later ¹
STid	Architect® Blue	ARCS-AQ/BT	SY-ARCS-W33-AQBT1-7OS1	QR code reader - Classic reader - Crypto processor - QR Code module - Bluetooth	Supported by design All STid readers Firmware version 10 or later ¹
STid	Architect® Blue	ARCS-BQ/BT	SY-ARCS-W33-BQBT1-7OS1	QR code reader - Keypad reader - Crypto processor - QR Code module - Bluetooth	Supported by design All STid readers Firmware version 10 or later ¹

Manufacturer	Series	Model	Part Number	Device type	Version
STid	SECard ² - High security programming kit (Configuration software for the QR code reader)	Not applicable	KIT-SECARD-BT-V3.X	• STid ARC-G USB encoder • USB key containing SECard software	Supported by design Software version 3.5 or later.

STid model codes explained:

- ARCS = Crypto Processor
- AQ = reader + QR code
- BQ = Keypad reader + QR code
- BT = Bluetooth

¹ If you are re-using existing readers, refer to *STid documentation* about how to upgrade your reader to firmware version 10 or later.

IMPORTANT: ² Genetec Inc. does not provide support for the STid SECard solution. Customers require the stand-alone STid SECard software to configure the STid OSDP readers to work with the ClearID ACS panel solution.

Browse

- [ClearID Self-Service Kiosk options](#)
- [System requirements for ClearID](#)

3.6 | ClearID Best practices

Use the provided best practices to help you successfully plan, design, and configure your Genetec ClearID™ system deployments.

This information is intended for end users, integrators, or deployment contacts who are responsible for planning, designing, and configuring a ClearID system.

Review the following best practices before planning your deployments:

- [Best practices for setting up ClearID for a new Synergis system](#)
- [Best practices for setting up ClearID with an existing Synergis system](#)

3.6.1 | Best practices for setting up ClearID for a new Synergis system

Consider the following best practices when building a new Synergis™ system to align with Genetec ClearID™ for an eventual ClearID implementation.

This information is intended for end users, integrators, or deployment contacts who are responsible for planning, designing, and configuring a ClearID system.

IMPORTANT: Because every system has different requirements, these best practices alone cannot be used to deploy your system. The deployment steps vary depending on your organizations architecture and current setup.

- Use this information as a starting point only for basic planning purposes.
- If you require help with your deployment, contact your deployment contact.

Best Practice: Ensure that you always test your new deployment implementation in a demo environment before applying to your production environment.

Pre-ClearID deployment tasks

1. Plan your Sites and Areas to suit your access requirements.

Tip: Think about meaningful names that relate to the sites or areas that end users will request.

- a. Plan out the *Sites* and *Areas* that require access control.
 - Example sites: Main building, Satellite office 1, Satellite office 2 and so on.
 - Example areas: 1st floor, 2nd floor, server room, auditorium, and so on.

NOTE: A site is typically one physical building or a cluster of buildings in close proximity. The site configuration applies to the entire site so it should be controlled by the same sets of policies (access configurations and visitor management configurations).

- b. Plan out the *Roles* that you require for your access and identity grouping.
 - Example roles: Sales, Marketing, Executives, Faculty, Students, Production crew, Contractors, All permanent employees, All part-time employees.

- c. (Optional) Consider [attribute-based provisioning to automate role memberships](#).

NOTE: Make a note of these sites, areas, and roles for use during the deployment tasks (steps 3 and 4) detailed later in this procedure.

2. (Optional) Test your setup and configuration in a ClearID demo environment.

- a. Connect your ClearID demo account to a Synergis demo system.
- b. Contact your Genetec Inc. representative to request a ClearID DEMO account and a Synergis demo system.

IMPORTANT: The configuration performed in a demo environment cannot be migrated to a production system.

Deployment tasks

1. Connect your new production Synergis system with your ClearID production account.
 - a. Install the ClearID plugin.
 - b. Connect Security Center to ClearID.
2. Synchronize identities with your data source.

Depending on your specific requirements, do one of the following:

 - o Synchronize your identities using the Genetec ClearID™ One Identity Synchronization Tool.
 - o Synchronize your identities using the API.
3. In the ClearID web portal, create the sites and areas that you planned earlier.
 - a. Create your sites.
 - b. Create your areas.
4. In the ClearID web portal, create the roles and attribute provisioning policies that you planned earlier.
 - a. Create your roles.
 - b. (Optional) Create attribute-based provisioning policies to automate role memberships.

Parent topic: ClearID Best practices

Browse

- About cardholder and identity relationships
- About custom fields in ClearID
- About ClearID One Identity Synchronization Tool attribute fields

3.6.2 | Best practices for setting up ClearID with an existing Synergis system

Consider the following best practices when setting up Genetec ClearID™ with an existing Synergis™ system.

This information is intended for end users, integrators, or deployment contacts who are responsible for planning, designing, and configuring a ClearID system.

IMPORTANT: Because every system has different requirements, these best practices alone cannot be used to deploy your system. The deployment steps vary depending on your organizations architecture and current setup.

- Use this information as a starting point only for basic planning purposes.
- If you require help with your deployment, contact your deployment contact.

Best Practice: Ensure that you always test your new deployment implementation in a demo environment before applying to your production environment.

Pre-ClearID deployment tasks

1. Prepare your cardholder information.
 - a. In Security Center, make sure that the existing cardholders have the required information to link with ClearID identities.

IMPORTANT: Cardholder Email field or External ID custom field must be populated.

 - This check ensures that existing identities and future identities are linked with pre-existing cardholders.
 - Future cardholders created by ClearID will already be linked correctly.
2. Plan your Sites and Areas to suit your access requirements.

Tip: Refer to your existing Synergis system when planning out your requirements. Think about meaningful names that relate to the sites or areas that end users will request.

 - a. Plan out the *Sites* and *Areas* that require access control.
 - Example sites: Main building, Satellite office 1, Satellite office 2 and so on.
 - Example areas: 1st floor, 2nd floor, server room, auditorium, and so on.

NOTE: A site is typically one physical building or a cluster of buildings in close proximity. The site configuration applies to the entire site so it should be controlled by the same sets of policies (access configurations and visitor management configurations).
 - b. Plan out the *Roles* that you require for your access and identity grouping.
 - c. (Optional) Consider attribute-based provisioning to automate role memberships.

NOTE: Make a note of these sites, areas, and roles for use during the deployment tasks (steps 3 and 4) detailed later in this procedure.
3. (Optional) Test your setup and configuration in a ClearID demo environment.
 - a. Connect your ClearID demo account to a Synergis demo system.
 - b. Contact your Genetec Inc. representative to request a ClearID DEMO account and a Synergis demo system.

IMPORTANT: The configuration performed in a demo environment cannot be migrated to a production system.

Deployment tasks

1. Connect your existing production Synergis system with your ClearID production account.
 - a. Install the ClearID plugin.
 - b. Connect Security Center to ClearID.
2. Synchronize identities with your data source.

Depending on your specific requirements, do one of the following:

 - o Synchronize your identities using the API.
 - o Synchronize your identities using the Genetec ClearID™ One Identity Synchronization Tool.
3. In the ClearID web portal, create the sites and areas that you planned earlier.
 - a. Create your sites.

- b. [Create your areas.](#)
- 4. In the ClearID web portal, create the roles and attribute provisioning policies that you planned earlier.
 - a. [Create your roles.](#)
 - b. (Optional) Create attribute-based provisioning policies to automate role memberships.

Parent topic: [ClearID Best practices](#)

Browse

- [About cardholder and identity relationships](#)
- [About custom fields in ClearID](#)
- [About ClearID One Identity Synchronization Tool attribute fields](#)

4 | ClearID plugin

4.1 | About ClearID plugin for Security Center

The Genetec ClearID™ Plugin integrates Genetec ClearID™ with Security Center and connects Synergis™ and ClearID cloud services. Any actions performed in ClearID are automatically synchronized with Synergis.

NOTE: Genetec ClearID™ was designed with a focus on the API. This API focus means that an Account administrator can create an API integration and use their own tools or services to communicate with our API.

You can download the ClearID plugin for Security Center [here](#).

Browse

- [ClearID API](#)

4.2 | About cardholder and identity relationships

Depending on the type of systems you want to integrate in Genetec ClearID™, you can choose to manage your cardholders and credentials manually or use ClearID to manage them automatically.

For cardholders that aren't created by ClearID, ClearID doesn't initially know which *identity* the *cardholder* belongs to. In this situation, ClearID finds different cardholder fields, identifies relationships, and associates them with the correct corresponding identities in the ClearID system.

ClearID compares the following information before creating a relationship between a cardholder and an identity:

Global unique identifier (GUID)

When our system creates a cardholder, we use the same GUID as the identity to create it.

Tip: You can find the GUID in the identity record URL for a ClearID user.

Code

```
https://demo.clearid.io/techdoc/organization/identities/139e92cd-44b9-427e-8727-bf7681ef0a8d
```



Where 139e92cd-44b9-427e-8727-bf7681ef0a8d is the GUID.

Email address

If the business email is the same as the cardholder email.

External ID

This field is an external identifier for creating identities in ClearID using the identity service API. The ClearID plugin creates this field in Security Center as a custom field for cardholders.

Best Practice: In Config Tool, check that all your cardholders have a valid business email address or external ID before adding your systems in ClearID. This check ensures that cardholders are correctly associated with the corresponding identities. For more information, see [Best practices for setting up ClearID with an existing Synergis system](#).

Scenario 1: Automatically manage cardholders and credentials

Select the Genetec ClearID: Cardholder and credential changes are synchronized back to Security Center radio button when you have a Security Center system and you want ClearID to create and manage your cardholders and credentials.

For example, a customer has a new Security Center system that is deployed without any cardholders or credentials already defined. By installing the ClearID plugin and adding access to identities, the corresponding cardholders and credentials are populated in the Security Center system and are automatically synchronized.

Tip: Use the Credentials configuration in the ClearID portal to synchronize your credentials.

For more information about credentials synchronization, see [Configuring credential replication in ClearID](#).

Scenario 2: Manually manage cardholders and credentials

Select the Security Center: Cardholders and credentials in ClearID are read-only radio button when you want ClearID to use existing cardholders and credentials without managing their state. In this situation, ClearID has access to Security Center cardholders and credentials in read-only mode because you want ClearID to know about your cardholders and credentials, but you never want ClearID to modify them.

For example, a customer has Security Center set up with 1000 cardholders and they use the ClearID plugin to connect the system to ClearID:

- If the Genetec ClearID: Cardholder and credential changes are synchronized back to Security Center radio button isn't selected when they add their systems, none of the cardholders or credentials information is modified or synchronized. Cardholders and credentials must be created and synchronized using other solutions. For example, Lightweight Directory Access Protocol (LDAP), Global Cardholder Synchronizer role, import plugins, and so on.
- If the Security Center system is already synchronized with an LDAP, they should synchronize ClearID with the same LDAP source.

Tip: Use LDAP or the *Global Cardholder Synchronizer* role in Security Center to create and synchronize cardholders and credentials.

For more information about global cardholder synchronization, see [Global cardholder management](#).

Browse

- [Reviewing cardholders and identities information in ClearID](#)
- [Adding a system to ClearID](#)
- [Synchronizing ClearID identity pictures with Security Center](#)

4.3 | Downloading and installing the ClearID plugin

To integrate the Genetec ClearID™ web application into Security Center, you must install the ClearID plugin on a Security Center server.

Before you begin

Ensure the following:

- Your server meets the [recommended system requirements](#).
- A [compatible version](#) of Security Center is installed.

What you should know

Best Practice: Although it's possible to host the ClearID role on any server, for best system performance host that role on a dedicated expansion server.

- To install or configure the plugin in Security Center, you must be a Site administrator. For example, local security, system integrator, or Security Center administrator.
- Synergis Professional or Omnicast Professional is required for plugins support in Security Center.
- Failover or Federation™ are not supported.

Procedure

1. Open the GTAP Product Download page.
2. From the Download Finder list, select your version of Security Center.
3. Search for your package by name and download it.
4. Download the plugin .exe file [here](#).
5. Follow your browser prompts to download the .exe file.
6. Stop the Genetec Server, and close Security Desk and Config Tool.
7. Open the extracted folder, right-click the setup.exe file, and click Run as administrator.
8. Open the downloaded file folder location, right-click the setup.exe file, and click Run as administrator.
9. Follow the installation instructions.

The plugin is installed to C:\Program Files (x86)\Genetec Inc\Genetec Security Center Plugins - ClearID\ by default.

10. On the Installation Wizard Completed page, click Finish.

After you finish

Return to Config Tool, and connect the ClearID plugin to ClearID cloud services account.

Best Practice: Use the Genetec™ Update Service (GUS) to keep the ClearID plugin up to date. For more information, see [About the Genetec Update Service](#).

Browse

- [How the ClearID plugin works with Security Center](#)

4.4 | Creating the ClearID plugin role

Before you can configure and use the Genetec ClearID™ plugin, you must create the plugin role in Config Tool.

Before you begin

[Download and install the plugin.](#)

What you should know

- To install or configure the plugin in Security Center, you must be a Site administrator. For example, local security, system integrator, or Security Center administrator.
- Each plugin role can only connect to or communicate with one unique ClearID system name at a time. For environments with multiple systems, you must create a plugin role for each system.

Procedure

1. From the Config Tool homepage, open the Plugins task.
2. In the Plugins task, click Add an entity () , and select Plugin.
The plugin creation wizard opens.
3. On the Specific info page, select the server on which the plugin role is hosted, the plugin type, and the database for the plugin role, and then click Next.
If you do not use expansion servers in your system, the Server option is not displayed.
IMPORTANT: The entry in the Database server field might default to the (local)\SQLEXPRESS setting. If this is not the correct server, choose the correct server from the Database server list.
4. On the Basic information page, specify the role information:
 - a. Enter the Entity name.
 - b. Enter the Entity description.
 - c. Select the Partition for the plugin role.
If you do not use partitions in your system, the Partition option is not displayed. Partitions are logical groupings used to control the visibility of entities. Only users who are members of that partition can view or modify the role.
 - d. Click Next.
5. On the Creation summary page, review the information, and then click Create, or Back to make changes.
After the plugin role is created, the following message is displayed: The operation was successful.
6. Click Close.
7. If you require multiple systems in your ClearID environment, repeat this procedure for each additional role that you require.

Results

The plugin role appears in the entity browser.

After you finish

You can now [connect Security Center to ClearID](#).

4.5 | Connecting Security Center to ClearID

Before you can connect the Genetec ClearID™ plugin role to your ClearID account, you must add your ClearID system and download an activation file. This activation file is then used to connect your Security Center system to the ClearID web application.

Before you begin

[Create the plugin role.](#)

What you should know

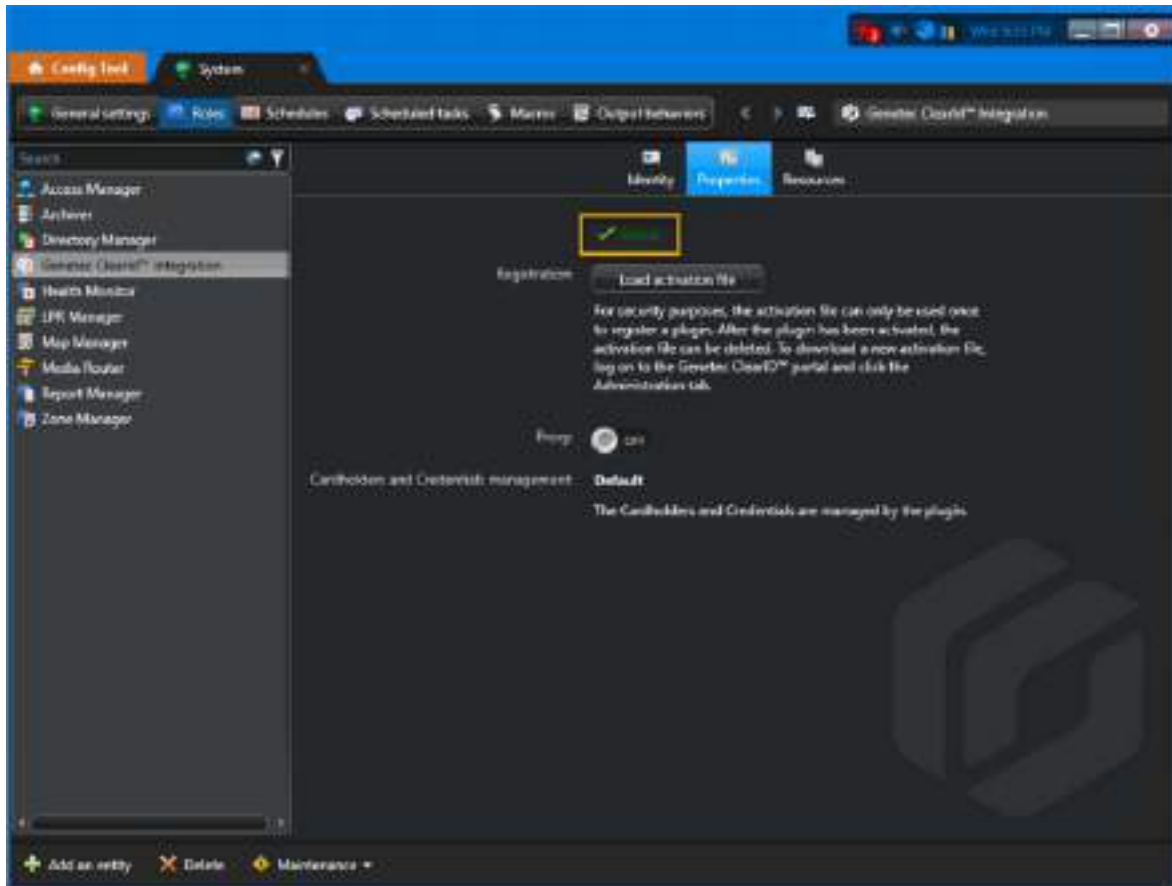
- To create systems in ClearID, you must be a Global administrator.
- To install or configure the plugin in Security Center, you must be a Site administrator. For example, local security, system integrator, or Security Center administrator.
- An activation file is used to authenticate the communication between your Security Center system and the ClearID web application.

Procedure

1. (Optional) If you have pre-existing Synergis™ cardholders, [review your cardholders and identities information](#).
2. [Add a system to ClearID](#).
3. [Download the activation file for the system you just created](#).
4. [Configure the connection settings using the activation file you just downloaded](#).
5. If you require multiple systems in your ClearID environment, repeat these steps for each additional system name that you require.

Results

The ClearID plugin is now connected to Security Center.



Browse

- Synchronizing ClearID identity pictures with Security Center

4.5.1 | Reviewing cardholders and identities information in ClearID

To ensure that cardholders are correctly associated with their corresponding identities in Genetec ClearID™ when systems are added, check that all cardholders have a valid business email address.

Before you begin

Learn about cardholder and identity relationships.

What you should know

This procedure is only applicable when you are setting up ClearID with an existing Synergis™ system that contains cardholders.

- All existing cardholders in Security Center require a valid business email address before they can be associated with their corresponding identities in ClearID.
- If all cardholders are created by ClearID, then the GUID is used to associate the cardholders with their corresponding identities automatically.

Procedure

To review identities in ClearID:

1. From the Home page, click Organization > Identities.
2. Click an identity in the list to see the identity details.

The following example shows a ClearID identity:

Organization / Identities / Test Cloud Employee

Test Cloud Employee

General Access Roles Delegations Device reports Access control User permissions Risk management Credentials

General **Active**

First name: Test **Last name:** Cloud Employee **Phone number:** **Mobile phone number:**

Middle name: **Business email:** cloudemployee@test.com **Personal email:**

Preferred name: Test Cloud Employee **Social link:** **Social ID:**

Country: Canada **State or Province:** **Street:**

City: **Zip or Post code:**

Company

Company: Genetec **Primary role:** Type to search... **Worker type description:** **Worker type code:**

Department: **Supervisor name:** **Job title:** **Employee number:**

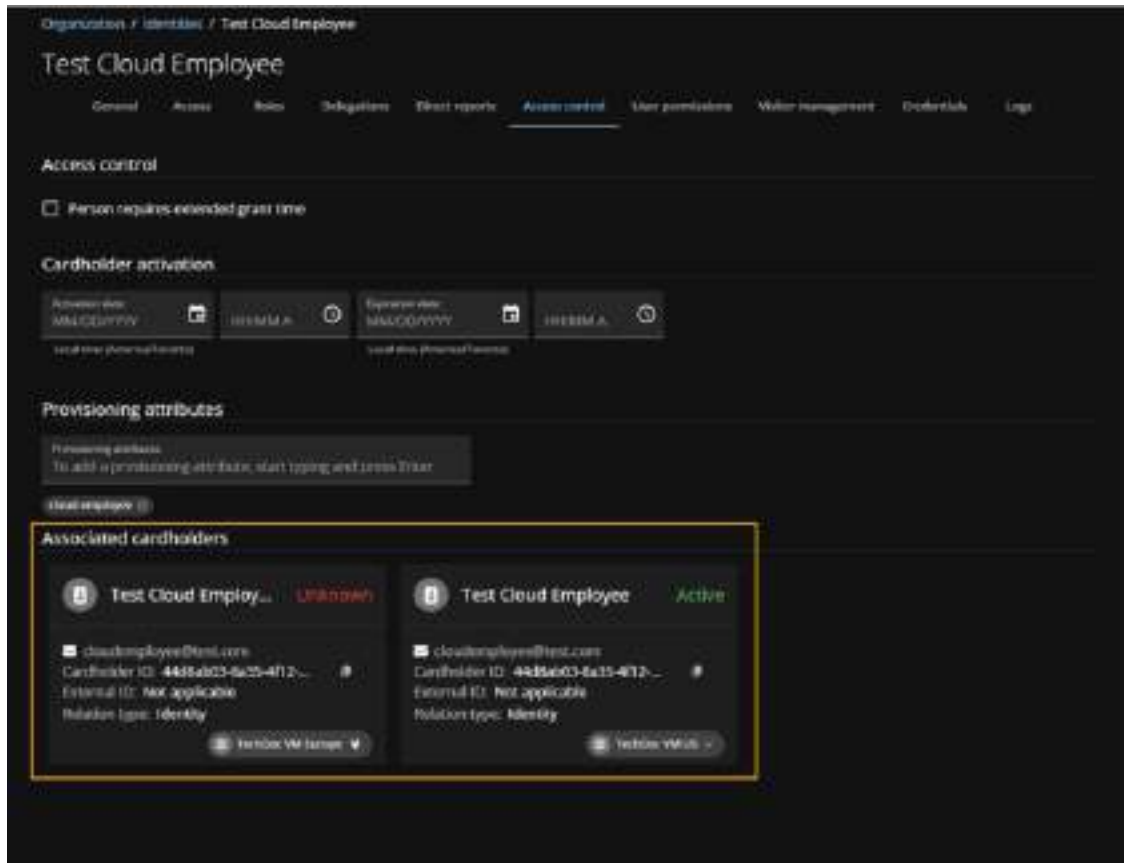
Supervisors

Name	Email
No supervisors	

Requests from this user do not require supervisor approval.

To review cardholders associated with a ClearID identity:

1. From the Home page, click Organization > Identities.
2. Click an identity in the list to see the identity details.
3. Click Access control.
A list of Security Center cardholders associated with a ClearID identity is displayed in the Associated cardholders section.



After you finish

Add your systems.

Parent topic: Connecting Security Center to ClearID

Browse

- About cardholder and identity relationships
- Synchronizing ClearID identity pictures with Security Center

4.5.2 | Adding a system to ClearID

Before you can connect the Genetec ClearID™ plugin role to your ClearID account, you must add your Security Center systems to ClearID.

Before you begin

- Create the plugin role.
- (Optional) If you have pre-existing Synergis™ cardholders, follow the best practices for Setting up Genetec ClearID™ with an existing Synergis™ system.
 - In Config Tool, check that all your cardholders have a valid business email address or external ID before adding your systems in ClearID. This check ensures that cardholders are correctly associated with the corresponding identities.
- Connect Security Center to ClearID.

What you should know

- To create systems in ClearID, you must be a Global administrator.

Procedure

1. Log on to your ClearID account.
2. From the Dashboard, click Administration > Add system.

← BACK

Add system

System name *

A descriptive name to identify your system. This can be changed later.

Data center region *

The region where your system information will be stored. This choice is permanent and cannot be changed.

Cardholder and credential management

The source of truth for cardholders and credentials.

☒ Genetec ClearID™: Cardholder and credential changes are synchronized back to Security Center.

☐ Security Center: Cardholders and credentials in ClearID are read-only.

Terms of service

☐ I accept the [Genetec Cloud Services - Subscriber terms of service](#) *

Cancel Save

NOTE: The Data center region option is not available for accounts deployed in regional architectures, such as Europe-only, Canada-only, or Australia-only data centers.

3. In the Add system dialog box, complete all the fields:
- Enter a system name.
Tip: Use a system name that represents the name of the account and the associated data center region. For example, GenetecEuropeSC.
 - From the Data center region list, select a region that applies to the geographical location of your system or where you want data stored.
 - If you want ClearID to populate cardholder and credential fields automatically, select Genetec ClearID™: Cardholder and credential changes are synchronized back to Security Center.
This is the default option.
 - If you want to manage cardholder and credential fields manually, select Security Center: Cardholders and credentials in ClearID are read-only.
 - Select the checkbox to accept the terms of service, and click Save.

← BACK

Add system

System name *

Montreal HQ

A descriptive name to identify your system. This can be changed later.

Data center region *

Canada

The region where your system information will be stored. This choice is permanent and cannot be changed.

Cardholder and credential management

The source of truth for cardholders and credentials.

☒ Genetec ClearID™: Cardholder and credential changes are synchronized back to Security Center.

☐ Security Center: Cardholders and credentials in ClearID are read-only.

Terms of service

☒ I accept the [Genetec Cloud Services - Subscriber terms of service](#) *

Cancel Save

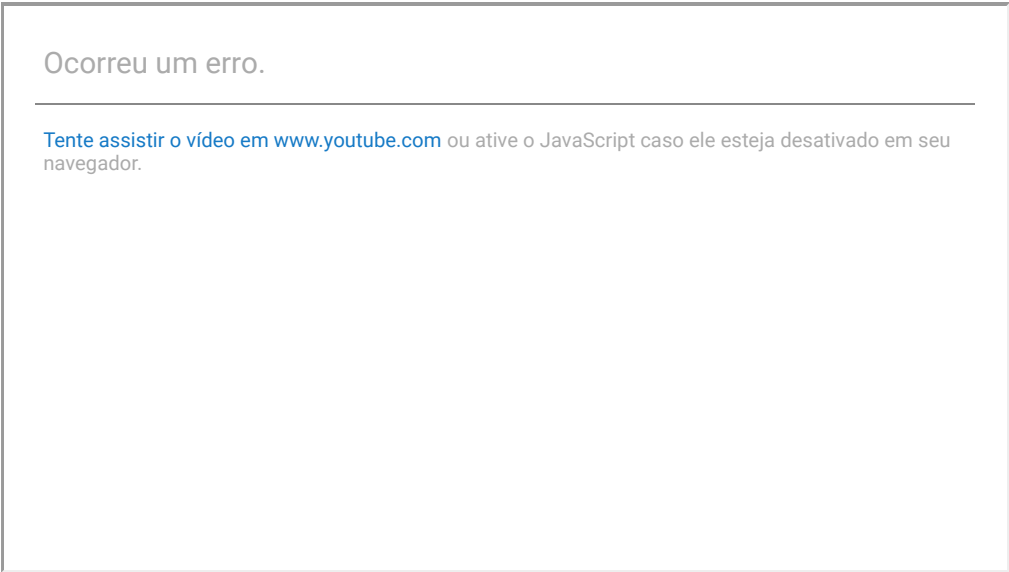
Results

Your new system is created. The system remains inactive until you download an activation file and register the ClearID plugin.



Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.



After you finish

- Download the activation file.
Parent topic: Connecting Security Center to ClearID
Browse
- About ClearID system states
 - About cardholder and identity relationships

4.5.3 | Downloading an activation file for ClearID

Before you can connect the Genetec ClearID™ plugin role to your ClearID account, you must download an activation file. This activation file is then used to connect your Security Center system to the ClearID web application.

Before you begin

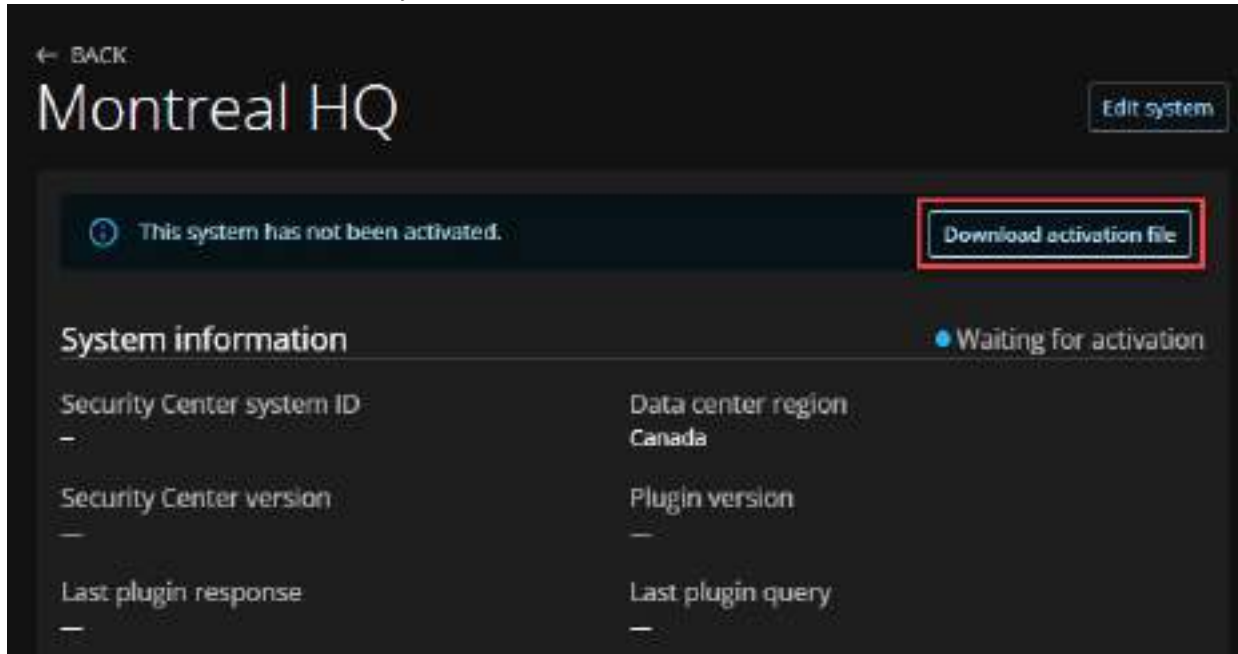
Add a system to ClearID.

What you should know

- To install or configure the plugin in Security Center, you must be a Site administrator. For example, local security, system integrator, or Security Center administrator.

Procedure

1. From the Dashboard, click the Administration tab.
2. On the Systems page, select a system.
3. Click Download activation file to save the file in json format.



Tip: Note the location of the activation file for later use. By default, the activation files are named systemname-systemID-activation-file.json.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.



After you finish

Configure the connection settings.

Parent topic: Connecting Security Center to ClearID

4.5.4 | Configuring connection settings for ClearID

To configure connection settings, you must load a previously downloaded activation file. This activation file is then used to connect your Security Center system to the Genetec ClearID™ web application.

Before you begin

[Download an activation file for ClearID.](#)

What you should know

- To install or configure the plugin in Security Center, you must be a Site administrator. For example, local security, system integrator, or Security Center administrator.
- An activation file is used to authenticate the communication between your Security Center system and the ClearID web application.
- For security purposes, the activation file can only be used once to register a plugin. After the plugin is activated, the activation file can be deleted.

Procedure

1. From the Config Tool homepage, open the Plugins task.
2. Select ClearID Integration from the entity browser, and click the Properties tab.
3. Click Load activation file and select the activation file that you previously downloaded.
4. (Optional) Configure the proxy server settings:

A proxy server is a server that verifies and forwards incoming client requests to other servers for further communication. For example, when a client is unable to meet the security authentication requirements of the server but should be permitted access to some services.

ON

Specifies that a proxy server is required to access the Internet. This option is typically used by customers behind a firewall or where network access to the Internet is restricted.

OFF

Specifies that a proxy server is not required. This is the default.

Proxy URL

If Proxy is enabled, enter the proxy URL supplied by your organization. For example, <https://proxy:8080/outgoing>. This information is typically supplied by the network administration team.

5. (Optional) Configure the proxy authentication settings:
Proxy authentication is the process of validating user credentials for access to a proxy server. This authentication typically includes a username and can also include a password.

ON

Specifies that proxy authentication is required.

OFF

Specifies that proxy authentication is not required.

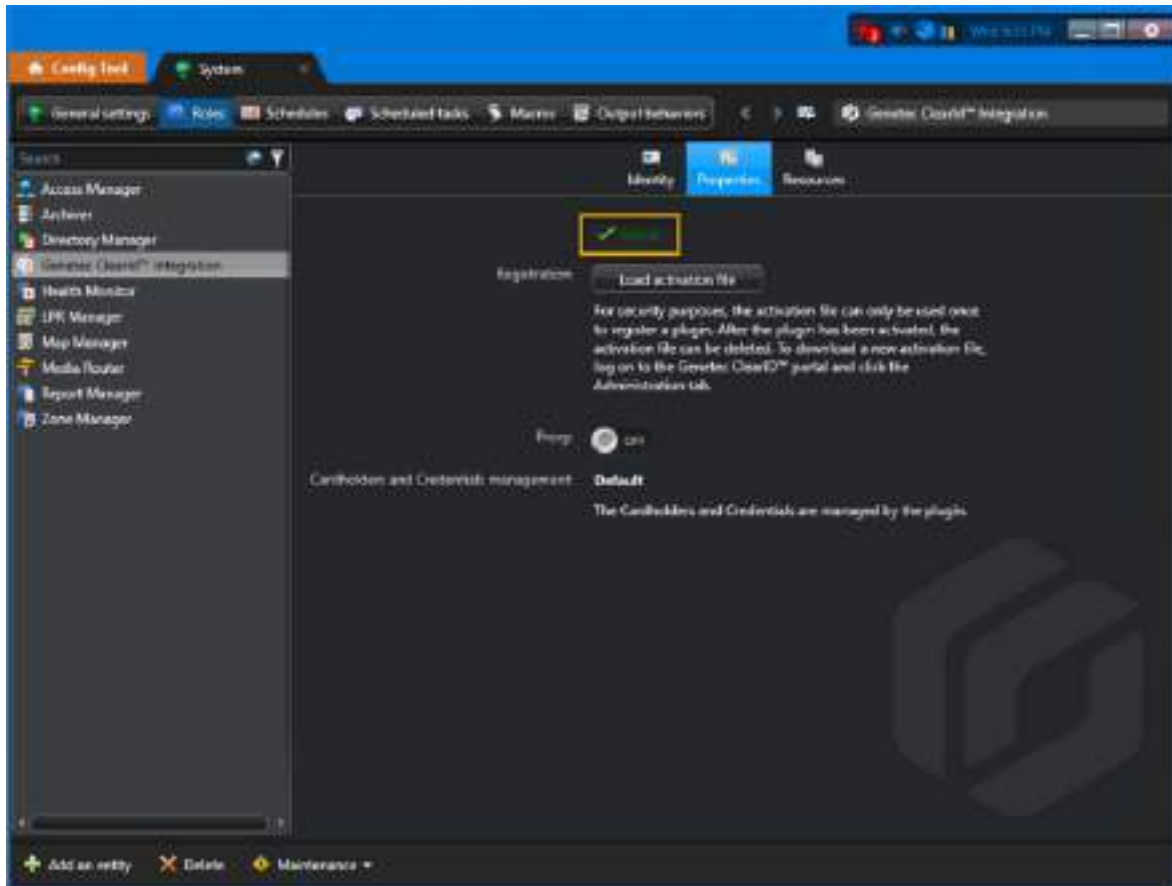
Proxy username

If proxy authentication ON was enabled, enter the proxy username supplied by your organization.

6. If proxy authentication ON is specified, set a proxy authentication password:
 - a. Click Set password.
 - b. Enter a New Password and then confirm the password.
NOTE: Use industry best practices for creating strong passwords.
 - c. Click Apply to save your password.
7. Click Apply to save all changes.

Results

The ClearID plugin is now connected to Security Center.



Parent topic: Connecting Security Center to ClearID

4.6 | Granting user privileges for the ClearID plugin

To allow users to access the Genetec ClearID™ plugin features and tasks, you must grant them the correct user privileges in Security Center.

What you should know

For administrators to install and configure the plugin in Config Tool, and for operators to use Security Desk functions, the correct user privileges must be granted to their user accounts.

This topic lists the minimum user privileges required.

NOTE: You might require more privileges, depending on the tasks you want to perform in Config Tool and Security Desk. For more information, see the [Security Center privileges spreadsheet](#) for your version.

Procedure

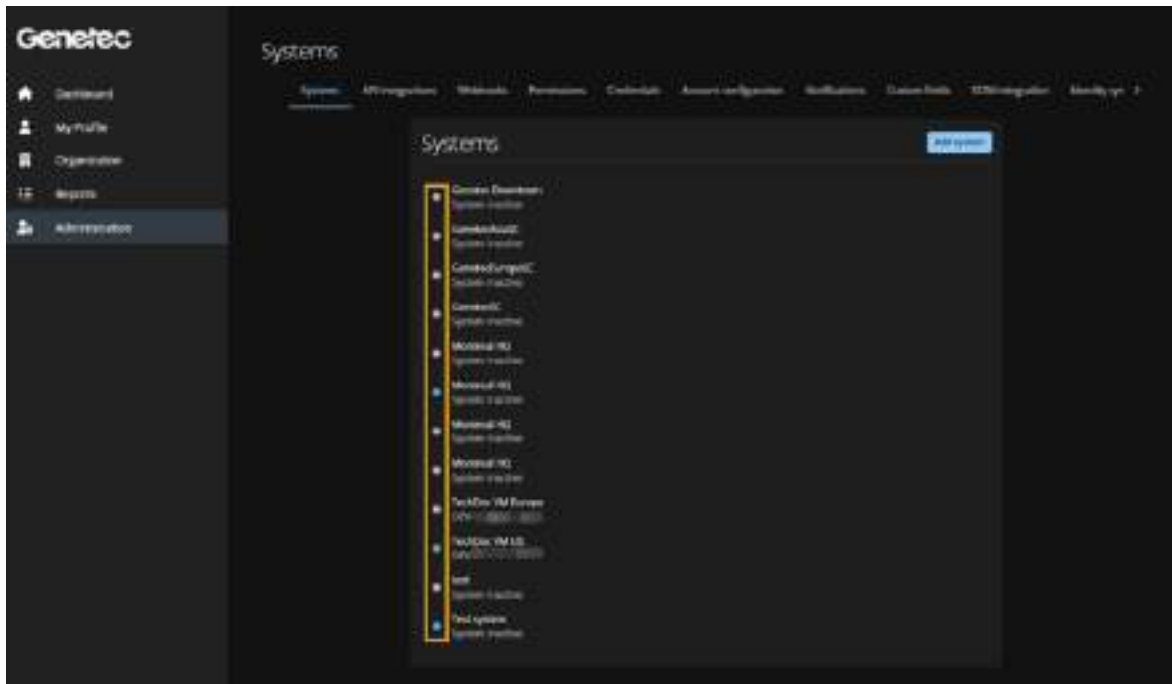
1. From the Config Tool homepage, open the User management task.
2. Select the relevant user, and click the Privileges tab.
3. Set the following privileges to Allow:
 - Application privileges > Security Desk
 - Application privileges > Config Tool
 - Administrative privileges > System management > View role properties
 - Administrative privileges > System management > View server properties
 - Task privileges > Administration > Plugins
4. (Optional) Set the custom field privileges that you require to Allow.
 - Administrative privileges > Access control management > View cardholder group properties > Modify cardholder group properties > Modify custom fields
 - Administrative privileges > Access control management > View cardholder properties > Modify cardholder properties > Modify custom fields
 - Administrative privileges > Access control management > View credential properties > Modify credential properties > Modify custom fields
 - Administrative privileges > Access control management > View visitor properties > Modify visitor properties > Modify custom fields
 - Administrative privileges > System management > View general settings > Modify custom field definitions
5. Click Apply.

Browse

- [About custom fields in ClearID](#)

4.7 | About ClearID system states

When you create or configure a Genetec ClearID™ system, the system goes through different states before being online or active. You can see the real-time status of ClearID systems on the Systems page.



Hover over the dot beside each ClearID system name to view its status:

Creating

Indicates that a new *system name* is being created.

New

Indicates that the *system name* has been successfully created. The activation file can now be downloaded to register the system.

Not available

Indicates that the API is not available, or is unable to respond.

Offline

Indicates that the system is offline. This status is displayed when the plugin has not sent a *heartbeat* response within 10 - 15 minutes to ClearID.

Online

Indicates that the system is registered, online, and connected to the ClearID plugin.

Unknown

Indicates that the system status cannot be obtained.

Waiting for activation

Indicates that the activation file was downloaded and the system is waiting for activation.

Warning

Indicates that the ClearID cloud services or the ClearID plugin did not process a message request within 10 minutes.

Tip: Move your mouse over a system status in the Status column to display the status explanation in the user interface.

Browse

- Adding a system to ClearID

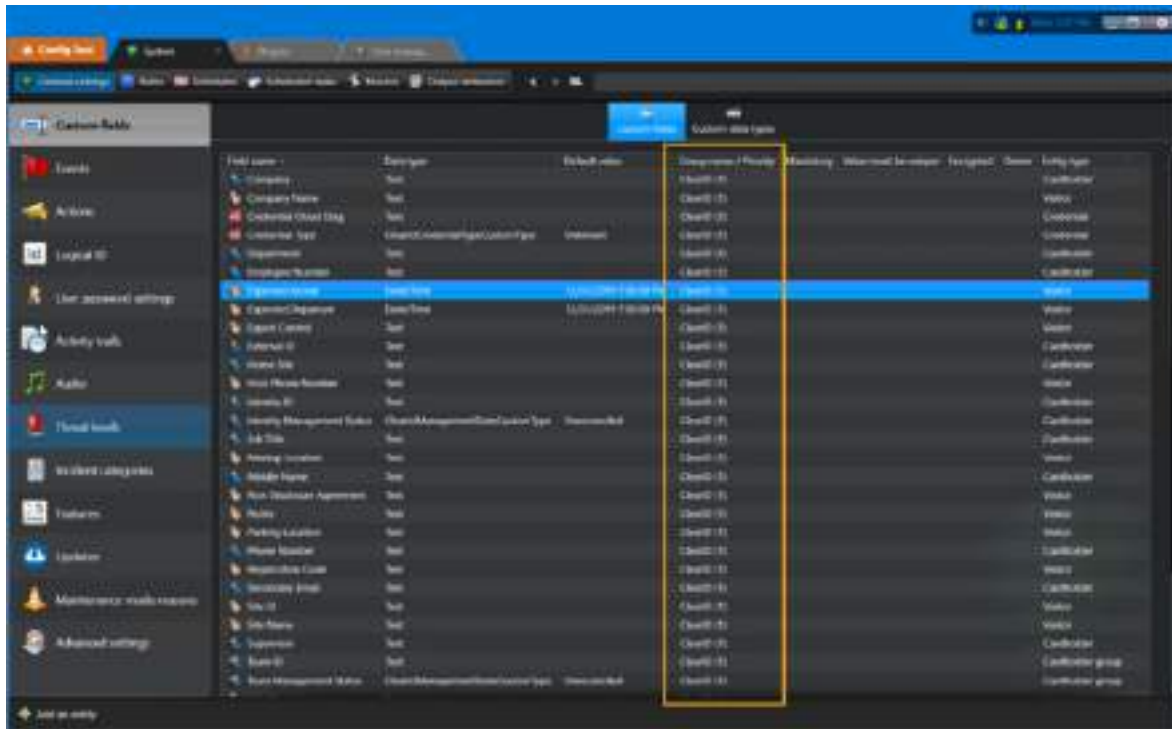
4.8 | About custom fields in ClearID

A custom field is a user-defined property associated with an entity type. Custom fields are useful for storing additional information.

In Security Center, Genetec ClearID™ uses custom fields for visitors, credentials, and cardholders functions. The group name ClearID is used to identify the custom fields associated with ClearID, and can be found in the Group name/Priority column.

IMPORTANT: ClearID custom fields should be used as read-only fields. These custom field values are populated and managed by ClearID. If you have existing custom fields, and the name and entity type matches the ClearID custom fields, ClearID will use the existing custom fields.

You can see the complete list for your organization in Config Tool. In the System task, click General settings > Custom fields.



NOTE: Only users with the privilege *Modify custom field definitions* can view custom fields.
Browse

- Granting user privileges for the ClearID plugin

4.8.1 | Modifying ClearID custom fields in Config Tool

You can modify Genetec ClearID™ custom fields in Config Tool so that they are displayed to specific groups or users. For example, you might display visit reason, registration code, expected arrival, and expected departure to a group that contains your security team or building reception team.

Before you begin

Make sure that the Genetec ClearID: Cardholder and credential changes are synchronized back to Security Center radio button is selected for the ClearID system, otherwise no custom fields are displayed.

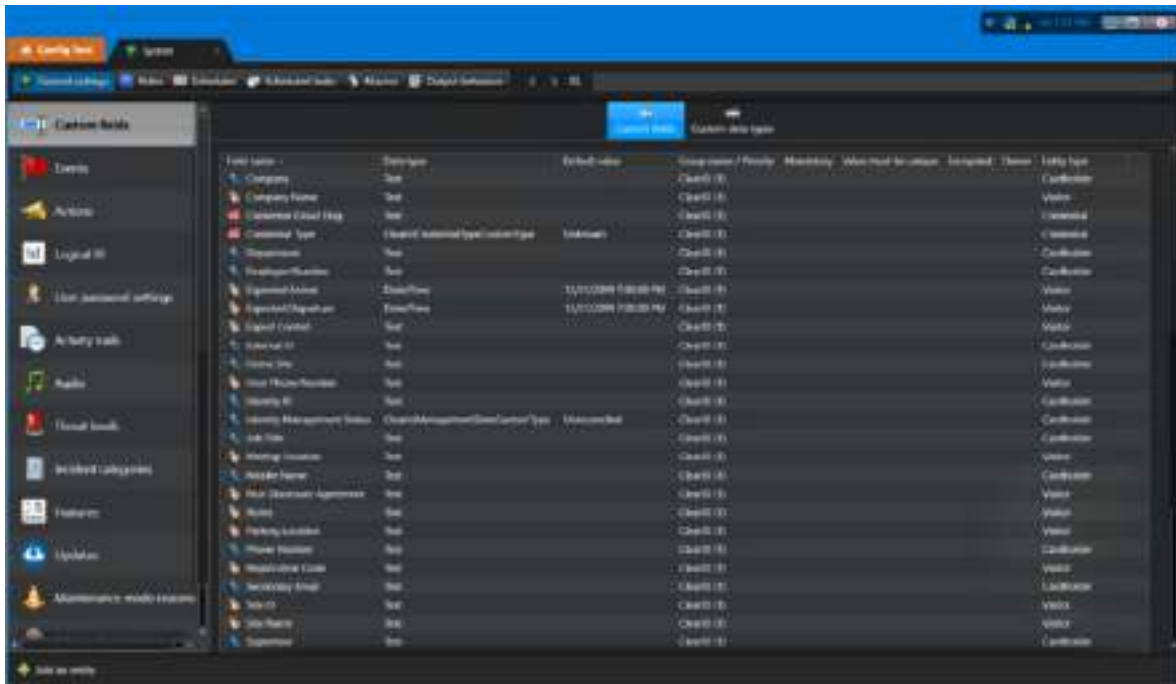
What you should know

Only users with the privilege to *Modify custom field definitions* can view custom fields.

- At least one identity must have been synchronized before any custom fields are displayed.

Procedure

1. In Config Tool, Open the System task.
2. Click Custom fields.



3. In the Custom fields tab, double-click a Field name to select the custom field that you want to modify.

4. In the Edit custom field dialog, make any changes that you require.

a. In the Definition section, make any changes that you require.

IMPORTANT: Do not select the Mandatory checkbox for custom fields. In ClearID, custom fields must not be mandatory or unique otherwise synchronization issues can occur.



b. In the Layout section, make any changes that you require.

For example, you could add a group name to categorize your custom fields, or you could remove a custom field from a group when a grouping is no longer applicable.

Genetec ClearID[®] User Guide
Displayed in the header

c. In the Security section, make any changes that you require.

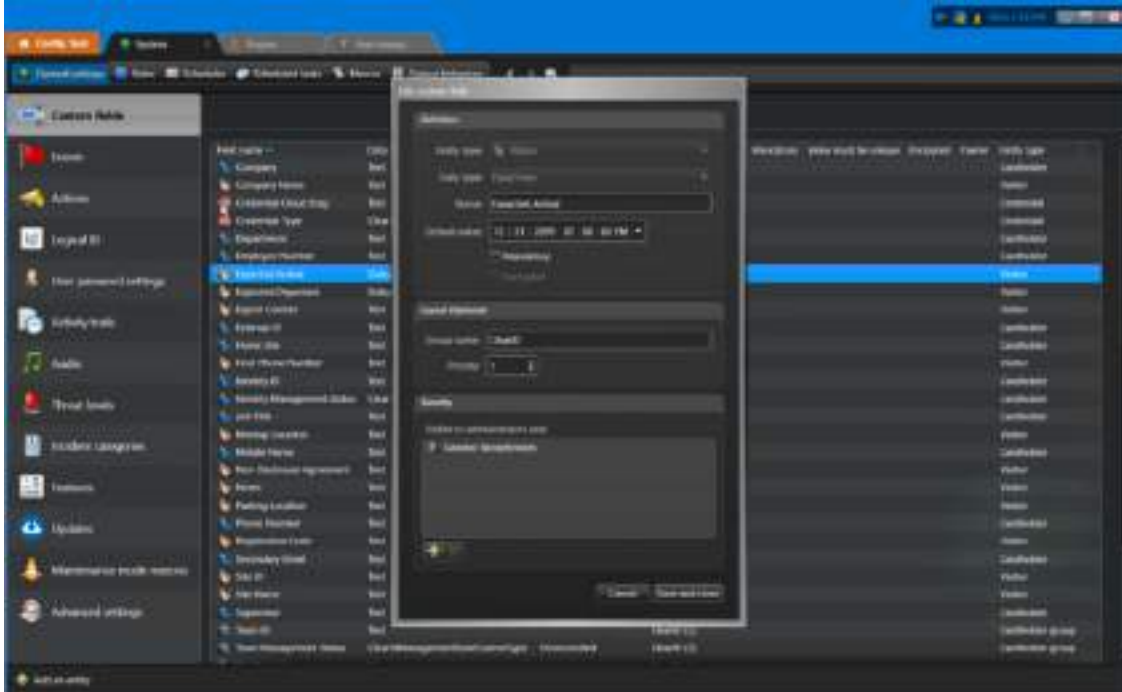
For example, you might add users or user groups in the Security section so that the custom field is displayed to them.

For information about user groups or custom fields, see [Creating user groups](#) or [About custom fields](#) on the TechDoc Hub.

d. Click Save and close.

Example

The following example shows the *Expected arrival* custom field. Using the Security section of the Edit custom field dialog, the Genetec Receptionists user group has been added so that the *Expected arrival* custom field can be displayed to members of the group.



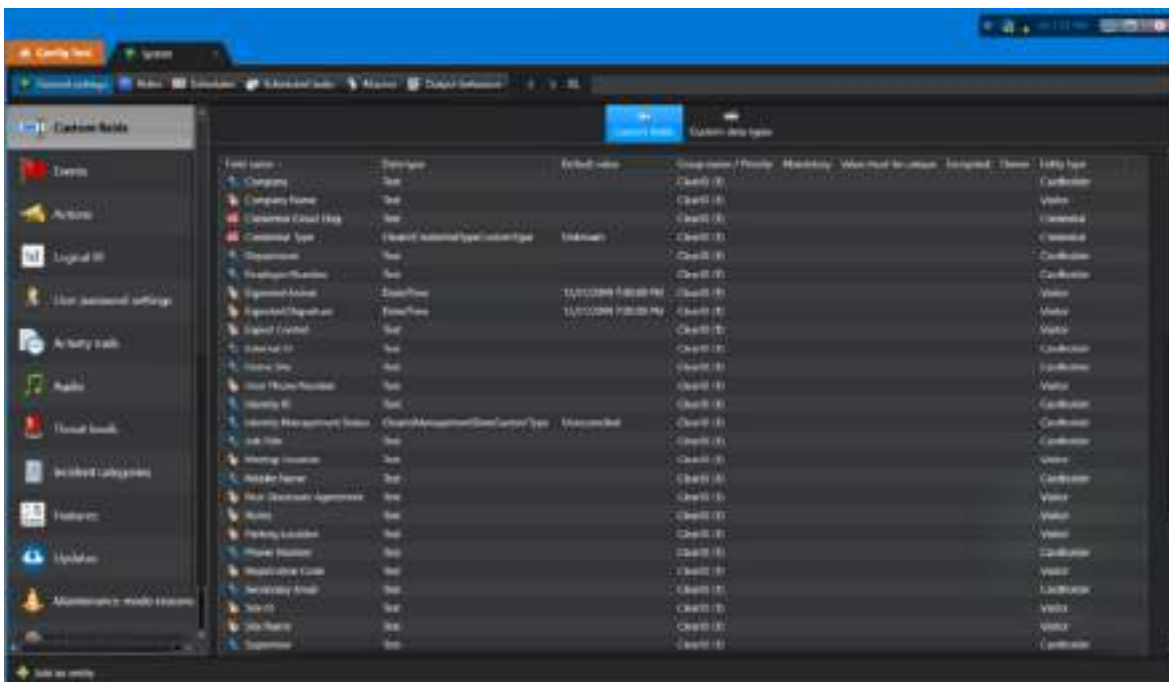
Parent topic: [About custom fields in ClearID](#)

Browse

- Custom fields not displayed in Security Desk
- Granting user privileges for the ClearID plugin

4.8.2 | Custom fields relationships

Use the following custom fields information to understand the relationship between Genetec ClearID™ identity field names and Security Center entity type fields.



Cardholder fields

Cardholder fields are used to synchronize cardholder information with an identity in ClearID.

Field name	Data type	Default value	Group name (And Priority)
Company	Text		ClearID (1)
Department	Text		ClearID (1)
Employee Number	Text		ClearID (1)
External ID	Text		ClearID (1)
Home Site	Text		ClearID (1)
Identity ID	Text		ClearID (1)
Identity Management Status	ClearIdManagementStateCustomType	Unreconciled	ClearID (1)
Job Title	Text		ClearID (1)
Middle Name	Text		ClearID (1)
Phone Number	Text		ClearID (1)
Secondary Email	Text		ClearID (1)
Supervisor	Text		ClearID (1)
Worker Type Code	Text		ClearID (1)
Worker Type Description	Text		ClearID (1)

Cardholder group fields

Cardholder group fields are used to synchronize cardholder group information with a role in ClearID.

- The Team ID represents the role ID in ClearID.
- The Team Management Status indicates whether ClearID is managing cardholders and credentials or not (managed by ClearID, not managed by ClearID, deleted by ClearID, or unreconciled).

Field name	Data type	Default value	Group name (And Priority)
Team ID	Text		ClearID (1)
Team Management Status	ClearIdManagementStateCustomType	Unreconciled	ClearID (1)

Credential fields

Credential fields are used by ClearID to keep the credentials up to date.

Field name	Data type	Default value	Group name (And Priority)
Credential Cloud Etag	Text		ClearID (1)
Credential Type	ClearIdCredentialTypeCustomType	Unknown	ClearID (1)

Visitor fields

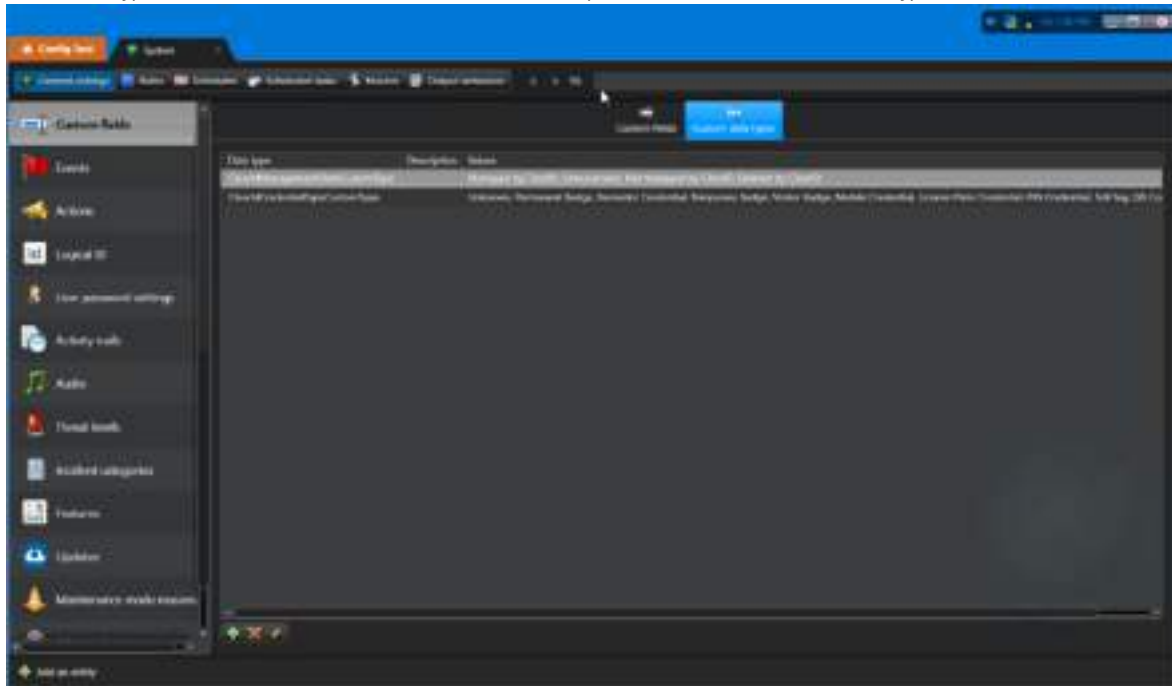
These visitor fields are used to synchronize visitor information.

Genetec ClearID™ User Guide Displayed in the header

Field name	Data type	Default value	Group name (And Priority)
Company Name	Text		ClearID (1)
Expected Arrival	Date and time	12/31/2099 7:00:00 PM	ClearID (1)
Expected Departure	Date and time	12/31/2099 7:00:00 PM	ClearID (1)
Export Control	Text		ClearID (1)
Host Phone Number	Text		
Meetup Location	Text		ClearID (1)
Non Disclosure Agreement	Text		ClearID (1)
Notes	Text		ClearID (1)
Parking Location	Text		ClearID (1)
Registration Code	Text		ClearID (1)
Site ID	Text		ClearID (1)
Site Name	Text		ClearID (1)
Visit Event Name	Text		ClearID (1)
Visit Reason	Text		ClearID (1)
Visitor ID	Text		ClearID (1)
Watchlist Status	Text		ClearID (1)

Custom data types

Custom data types are used for some custom fields to define the accepted values associated with the data types.



NOTE: All custom fields are labels used to define a property associated with a Security Center entity type that might be useful to an organization. The fields included in the description here are merely descriptive labels. All the custom data types might not be applicable to or used by ClearID.

Data type	Values
ClearIdManagementStateCustomType	Managed by ClearID, Unreconciled, Not managed by ClearID, Deleted by ClearID

Data type	Values
ClearIdCredentialTypeCustomType	Unknown, Permanent Badge, Biometric Credential, Temporary Badge, Visitor Badge, Mobile Credential, License Plate Credential, Pin Credential, Toll Tag, QR Code

Parent topic: [About custom fields in ClearID](#)

5 | Managing identities and users

5.1 | Creating identities in ClearID

From time to time, you might need to create an identity manually in Genetec ClearID™. For example, for an identity that isn't part of the usual mass import process or synchronization of identities using LDAP, One Identity, or API solutions.

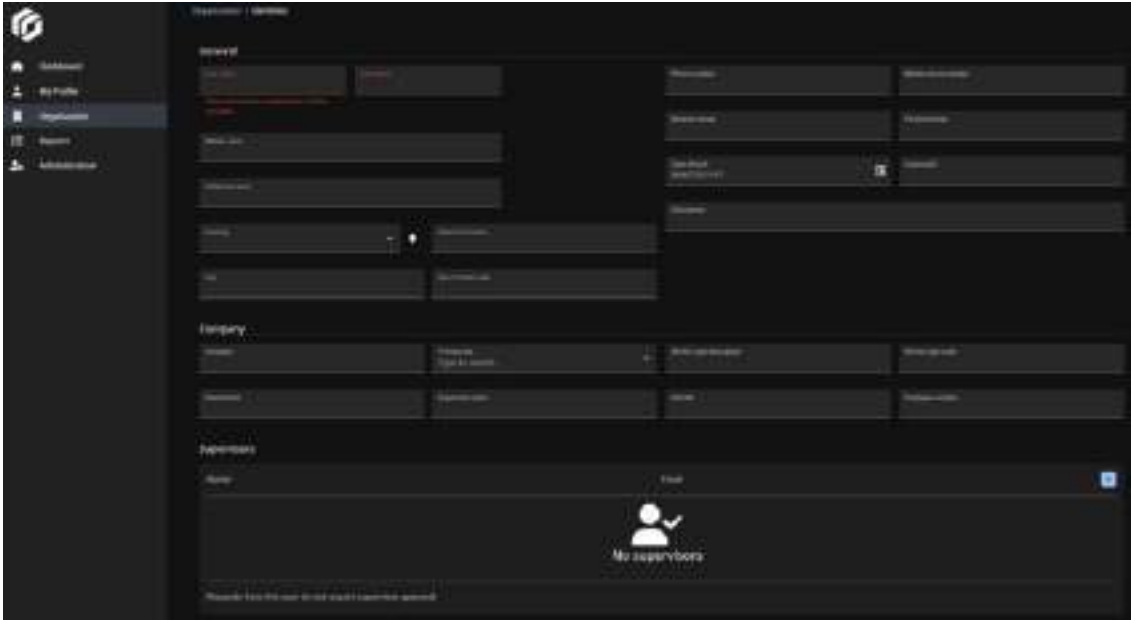
What you should know

Only an account administrator can create identities.

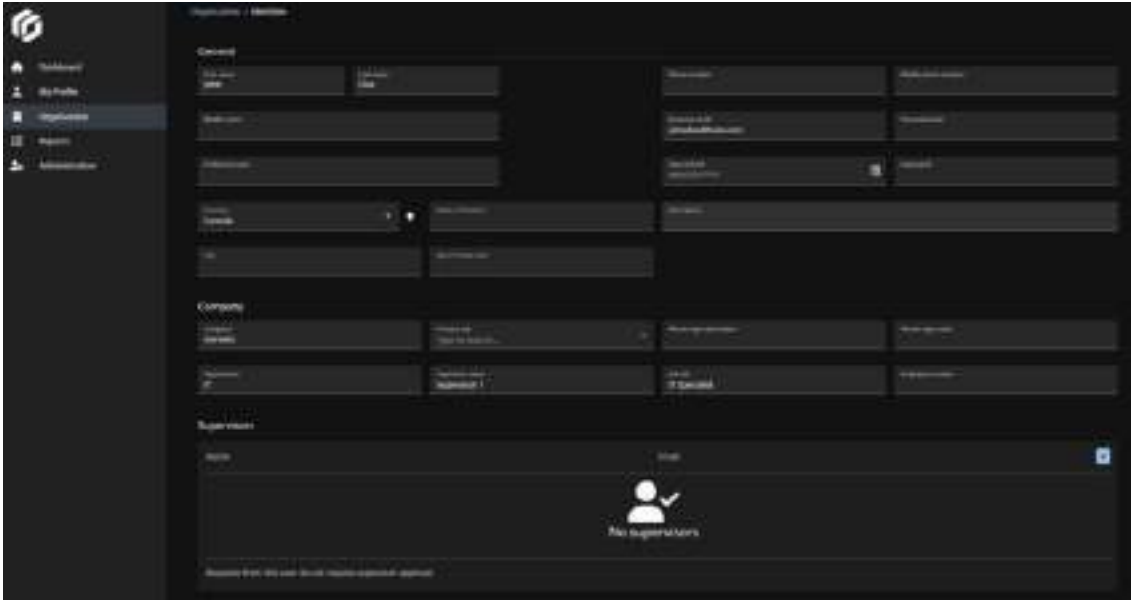
Account administrators can create an identity manually in the web portal when the identity isn't part of a mass import or synchronization of identities using LDAP, One Identity, or API solutions. For example, a *contractor*, *system integrator*, or other identities might be added manually.

Procedure

- 1. Click Organization > Identities.
- 2. Click Add an identity.



- 3. Complete the mandatory fields:
 - a. Enter a First name.
 - b. Enter a Last name.
 - c. Select a country from the list.
Tip: Enter the first letter of the country to jump to that part of the country list.
- 4. (Optional) Complete any additional fields that you require. For example:
 - a. Enter a Business email address.
 - b. Enter a Company name.
 - c. Enter a Department.
 - d. Enter a Supervisor name.
 - e. Enter a Job title.
 - f. Complete other fields as required.



5. Click Save to create the identity in Genetec ClearID™.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Grant the identity access to the web portal.
Browse

- Logging on to ClearID
- Viewing direct reports in ClearID

5.2 | Identity fields in ClearID

Use the following information to help you understand the identity fields that are used in Genetec ClearID™. The following table explains which fields are mandatory, which fields are used by Security Center, and which fields are available for use by provisioning rules.

ClearID identity fields	Type or format	Mandatory in ClearID	Pushed to Security Center	Security Center field name	Available in provisioning rules
Activation date	Date		✓	Activation	
Business email	Email		✓	Email address	
City	Text				
Company	Text		✓	Company	✓

Genetec ClearID®; User Guide

Displayed in the header

ClearID identity fields	Type or format	Mandatory in ClearID	Pushed to Security Center	Security Center field name	Available in provisioning rules
Country	ISO 3 Character	✓			✓
Date of birth	Date				
Department	Text		✓	Department	✓
Description	Text		✓	Description	✓
Display name	Text		✓	Entity name	
Employee number	Text		✓	Employee number	
Expiration date	Date		✓	Expiration	
Extended grant time required	True or False		✓	Use extended grant time	✓
External ID	Text		✓	External ID	✓
First name	Text	✓	✓	First name	
Home site	Unique ID		✓	Home site	✓
Identity ID	Unique ID		✓	Identity	
Job title	Text		✓	Job title	✓
Last name	Text		✓	Last name	
Middle name	Text		✓	Middle name	
Mobile phone number	Phone number				
Personal email	Email		✓	Secondary email	
Phone number	Phone number		✓	Phone number	
Provisioning attributes	List				✓
State/Province	Text				
Status	Active or Inactive	✓	✓	Status	✓
Supervisor name	Text		✓	Supervisor	✓
Supervisor(s)	List of identities				✓
Worker type code	Text			Worker type code	✓
Worker type description	Text		✓	Worker type description	✓
Zip code	Text		✓		

Browse

- [Configuring role-based access control policies in ClearID](#)
- [About custom identity fields in ClearID](#)

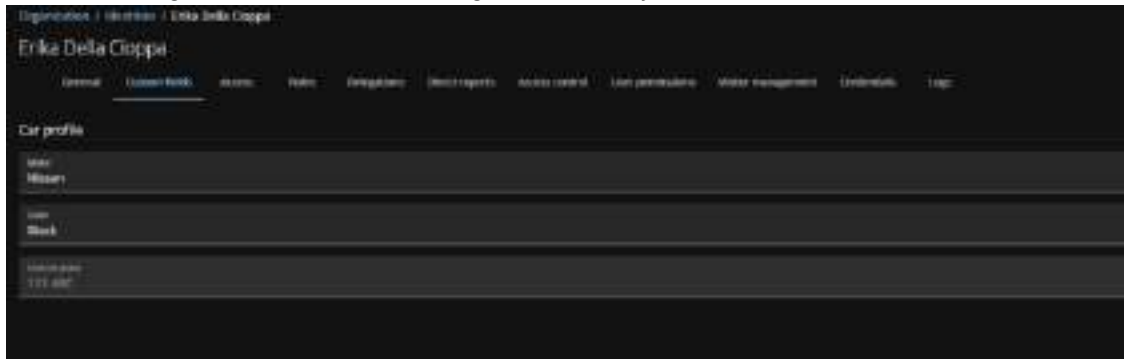
5.3 | About custom identity fields in ClearID

Custom fields are user-defined properties associated with identities in the Genetec ClearID™ web portal.

In Genetec ClearID™, custom identity fields add additional configurable information to identities, separate from the system's default identity fields. *Account administrators* create and manage these custom fields in the ClearID web portal. The custom fields can be manually populated in the identity profile or can be synchronized from an external data source. The custom fields can be synchronized to linked Security Center systems as needed.

NOTE: Select Synchronize custom field values with external systems to automatically synchronize the custom fields with Security Center. No prior setup is required, and custom fields can be populated by the *Account administrators* later.

Custom identity fields can include information such as vehicle profiles, employee types, worker schedules, and more for all identities in the ClearID portal. The custom fields are organized in sections and can be configured to be read-only.



Browse

- [Creating custom identity fields in ClearID](#)
- [Identity fields in ClearID](#)

5.4 | Creating custom identity fields in ClearID

To collect and store additional information about identities in the Genetec ClearID™ web portal, *Account administrators* can create custom fields and set them to synchronize with Security Center as needed.

Before you begin

Learn about custom identity fields.

What you should know

You must be an *Account administrator* to create custom identity fields.

Procedure

1. In the ClearID portal, click Administration > Custom fields.
2. Create a custom field section.

Custom field sections group related custom fields together to be displayed on identity profile pages.

- a. Click Add custom field section.
- b. On the New custom field section page, fill out the necessary fields.

Section ID

In the Section ID field, enter a unique ID for your custom field section.

IMPORTANT: The section ID is used for organization and troubleshooting purposes. This value cannot be changed later.

Display name

In the Display name field, enter a name for the custom field section. The name is displayed on identity profile pages.

- c. Click Save.

3. (Optional) Click  to edit a custom field section.

- a. On the new page, edit the custom field section as needed:

Display name

Edit the selected section's display name.

Custom fields

Add, view, or edit custom fields within the selected custom field section.

Delete custom field section

Delete the selected custom field section.

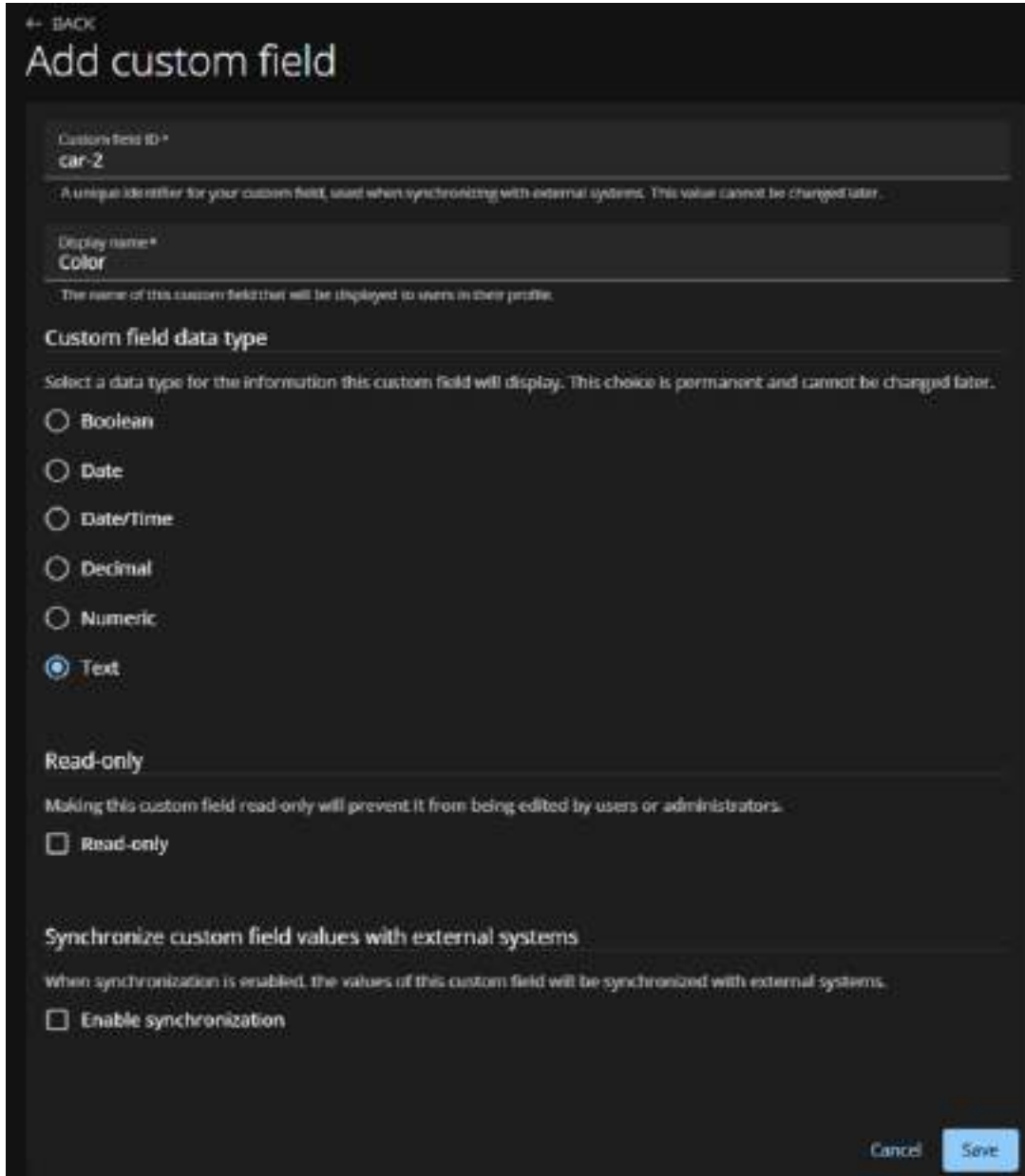
b. Click Save.

4. Add custom fields to the custom field section.

a. Click  to edit the custom field section.

b. Click Add custom field.

c. Configure the custom field as needed:



Custom field ID

In the Custom field ID field, enter a unique ID for the custom field.

Display name

In the Display name field, enter a name for the custom field.

Custom field data type

In the Custom field data type section, select the data type for the information displayed in the custom field.

Read-only

In the Read-only section, choose whether to restrict users and administrators from editing the custom field on the identity profile page.

NOTE: The read-only feature is intended to be used when synchronizing ClearID with an external source.

Synchronize custom field values with external systems

In the Synchronize custom field values with external systems section, choose whether to synchronize the custom field with Security Center.

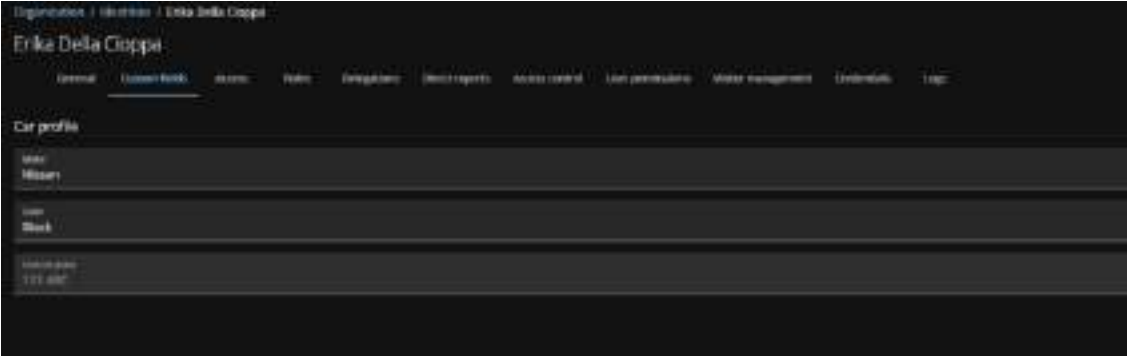
- d. Click Save.
5. (Optional) Create a custom field that will not be displayed on the identity profile page.

NOTE: These custom fields will still synchronize with Security Center if Synchronize custom field values with external systems is selected.

- a. In the ClearID portal, click Administration > Custom fields.
- b. Click Add custom field.
- c. Repeat step 4 c.
- d. Click Save.

Results

You can view and fill custom fields by navigating to Organization > Identities > Identity > Custom fields.



Browse

- [About custom identity fields in ClearID](#)

5.5 | Granting additional permissions for identities and roles in ClearID

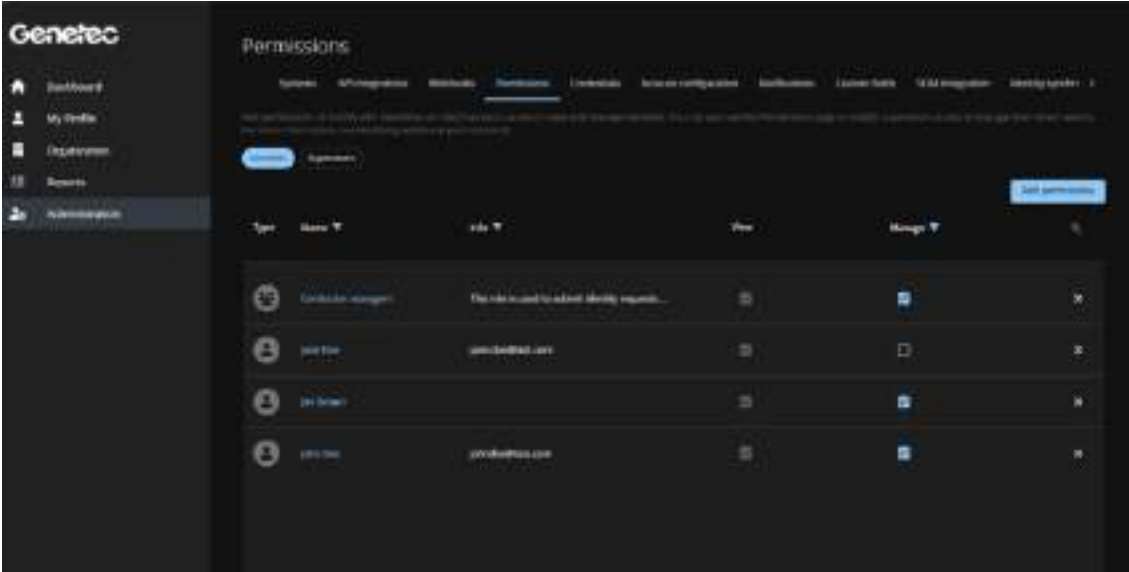
Some organizations require more access than the default permissions provided for a Genetec ClearID™ user. You can grant identities and roles additional permissions so that they can view or manage all identities in the system.

What you should know

Only an account administrator can add identity and role permissions.

Procedure

1. From the Home page, click Administration > Permissions.



2. Click Add permissions.

The screenshot shows the 'Permissions' dialog box with the 'Identities' tab selected. The 'Identities' field contains 'jack' and a search prompt 'Type to search...'. Below it, the 'Permissions' section has 'View' checked and 'Manage' unchecked. The 'Reason' field is empty. The dialog has 'Cancel' and 'Add identities' buttons at the bottom.

3. In the Permissions dialog, select either Identities or Roles to add the permissions you require.

4. If you selected Identities, complete the following:

- In the Identities field, enter one or more identities that you want to grant extra access.
A maximum of 20 identities per request is supported.
- In the Permissions section, select the permissions you want to add to the identities selected earlier.

View

Access to view identities is granted by default.

Manage

Select the Manage checkbox to add permissions to modify identities.

NOTE: If you make updates to identities that are synchronized with an external data source, the synchronization can overwrite your manage permission changes. Manage permissions are useful for identities being manually entered into ClearID.

- In the Reason field, enter a reason why the access was added.

This screenshot shows the 'Permissions' dialog box with the 'Identities' tab selected. The 'Identities' field contains 'jack' and a search prompt 'Type to search...'. Below it, the 'Permissions' section has both 'View' and 'Manage' checked. The 'Reason' field contains the text 'Access required to view and manage identities'. The dialog has 'Cancel' and 'Add identities' buttons at the bottom.

5. If you selected Roles, complete the following:

- In the Roles field, enter one or more roles that you want to grant extra access.
A maximum of 20 roles is supported.
- In the Permissions section, select the permissions you want to add to the roles selected earlier.

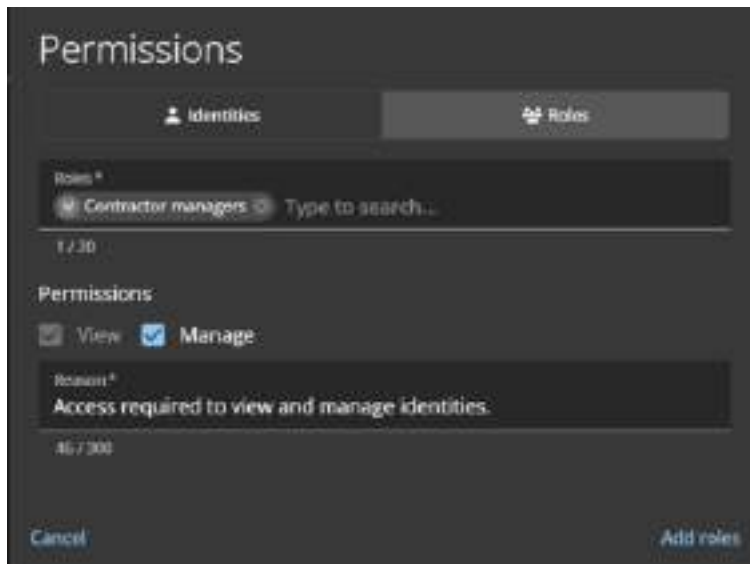
View

Access to view identities is granted by default.

Manage

Select the Manage checkbox to add permissions to modify identities.

- In the Reason field, enter a reason why the access was added.



6. Click Add identities or Add roles to submit your changes.

Results

The specified identities or roles now have the required permissions to view and manage identities.

After you finish

View identities or Modify identities.

Browse

- Transferring direct reports in ClearID

5.6 | Granting additional permissions for supervisors in ClearID

Some organizations require more access than the default permissions provided for a Genetec ClearID™ supervisor. You can grant supervisors additional permissions so that they can manage their direct reports.

What you should know

Only an account administrator can grant supervisors access to manage their direct reports.

Procedure

1. From the Home page, click Administration > Permissions.
2. Click the Supervisors tab.
3. Select the Grant supervisors access to manage their direct reports checkbox to grant supervisors the required permissions to update General identity profile information and Access Control settings.



4. Click Save to confirm the changes.

Results

Supervisors now have more control to manage their direct reports. They can now modify General identity information fields and Access control settings.

After you finish

Modify your direct reports information.

Browse

- Transferring direct reports in ClearID

5.7 | Viewing additional permissions in ClearID

You can use the Permissions page to review who (identities or roles) has extra access to view and manage identities. You can also use the Permissions page to verify if supervisors have extra access to manage their direct reports.

Before you begin

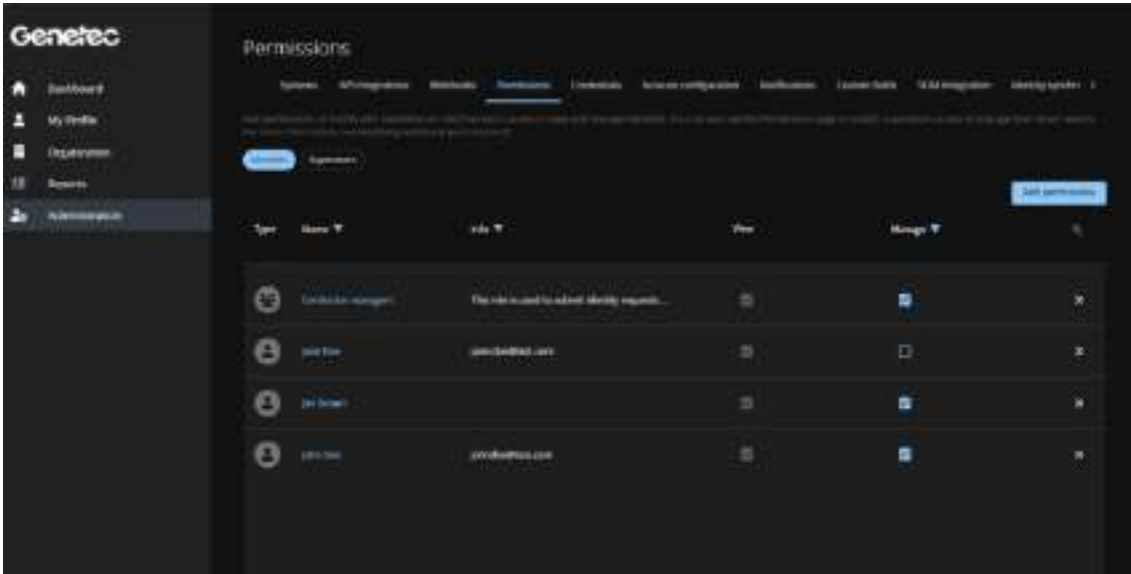
- Grant additional permissions for identities and roles.
- Grant additional permissions for supervisors.

What you should know

Only an account administrator can view identity and role permissions or supervisor permissions.

Procedure

1. From the Home page, click Administration > Permissions.



- In the Type column, each row has a visual identifier to signify the entry as either a role or an identity.
2. In the Name column, click  to filter results by identity or role name.
 3. In the Info column, click  to filter results by an email address, or enter words to search for in the permission information.
 4. In the Manage column, click  to filter results by permission. For example, to see which identities have View and Manage permissions.
 5. (Optional) Click Clear filters () to reset filters and restore the default page view.
 6. (Optional) Click the Supervisors tab to verify if supervisors have access to manage their direct reports.



After you finish

Modify additional permissions.

5.7.1 | Modifying additional permissions in ClearID

You can use the Permissions page to modify who (identities or roles) has extra access to view and manage identities. You can also use the Permissions page to modify supervisors access to manage their direct reports.

Before you begin

[View additional permissions.](#)

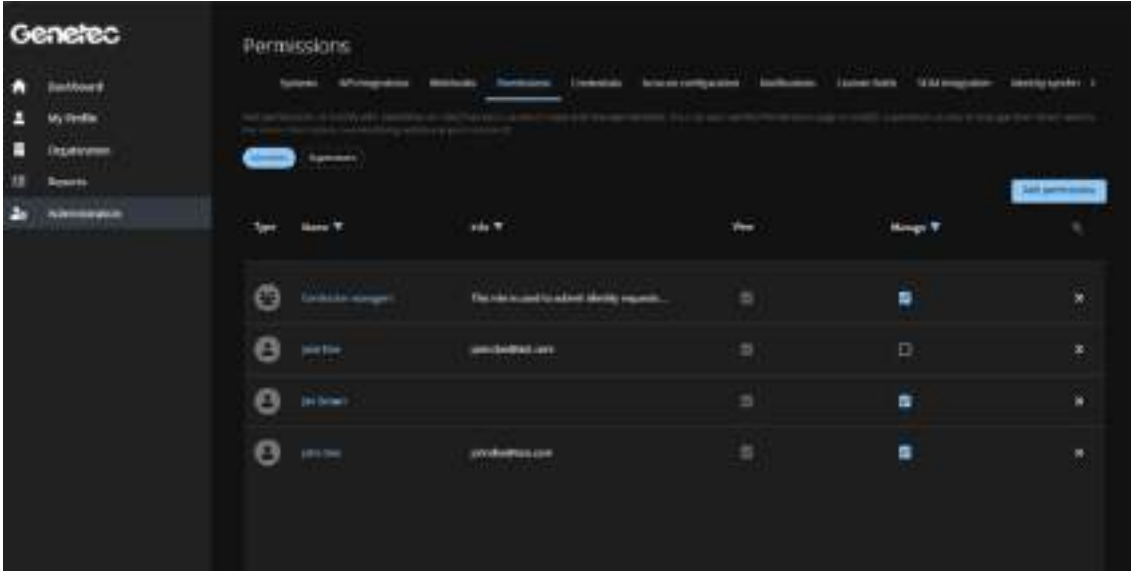
What you should know

Only an account administrator can modify identity and role permissions.

Procedure

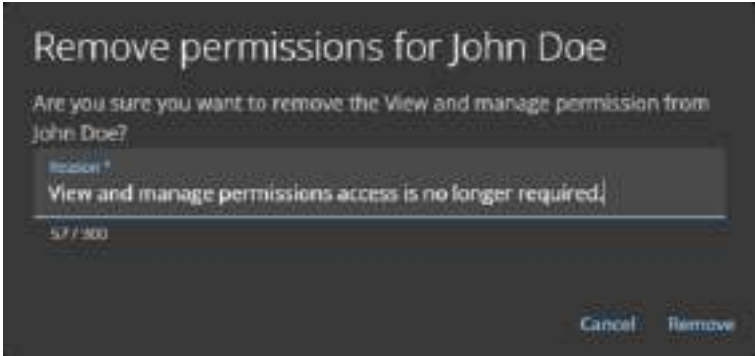
To modify identity and role permissions:

- 1. From the Home page, click Administration > Permissions.



In the Type column, each row has a visual identifier to signify the entry as either a role or an identity.

- 2. In the Name column, click to filter results by identity or role name.
- 3. In the Info column, click to filter results by an email address, or enter words to search for in the permission information.
- 4. In the Write column, click to filter results by permission. For example, to see which identities have Read and Write permissions.
- 5. (Optional) Click Clear filters () to reset filters and restore the default page view.
- 6. (Optional) In the Write column, select or clear the check box next to an identity or role to add or remove their Write access.
 - a. Click Save to submit your changes.
- 7. (Optional) Click the next to an identity or role to remove extra permissions (Read and Write) that are no longer required.



- a. Enter a Reason.
- b. Click Remove.

To modify supervisor permissions:

- 1. (Optional) Click the Supervisors tab to modify supervisor permissions.



- a. Make the changes that you require and click Save.

Parent topic: [Viewing additional permissions in ClearID](#)

5.8 | Viewing identities in ClearID

You can view identities in Genetec ClearID™ to check their access control status, general identity information, or verify if they have any supervisors specified.

Before you begin

[Create your identities.](#)

What you should know

Only account administrators or identities or roles with the required permissions can view identities.

Procedure

1. From the Home page, click Organization > Identities.
2. Select an option from the drop-down menu to display the identities that you require. Choose one of the following:
 - Active**
Displays active identities.
 - Inactive**
Displays inactive identities.
 - All**
Displays all active and inactive identities.
3. In the Search field, enter some search criteria and press enter.
4. Select an identity from the list to view the identity details.

The screenshot shows the 'Fred Smith' user profile page in the Genetec ClearID system. The page has a dark theme and a top navigation bar with tabs: General, Access, Roles, Delegations, Direct reports, Access control, User permissions, Visitor management, Credentials, and Logs. The 'General' tab is selected. The profile information is organized into sections: 'General' (with an 'Active' status indicator), 'Company', and 'Supervisors'. The 'General' section includes fields for First name (Fred), Last name (Smith), Phone number, Mobile phone number, Middle name, Business email (fred.smith@test.com), Personal email, Preferred name (Fred Smith), Date of birth (MM/DD/YYYY), Gender (M), Country (Canada), State or Province, Description, City, and Zip or Postal code. The 'Company' section includes Company, Primary job (Type to search...), Worker type description, Worker type code, Department, Supervisor name, Job title (Contractors Manager), and Employee number. The 'Supervisors' section shows a table with columns for Name and Email, and a message stating 'No supervisors' with a note that requests from this user do not require supervisor approval.

Organization: P Identities: P Fred Smith

Fred Smith

General Access Roles Delegations Direct reports Access control User permissions Visitor management Credentials Logs

General Active

 First name: Fred Last name: Smith Phone number: Mobile phone number: Middle name: Business email: fred.smith@test.com Personal email: Preferred name: Fred Smith Date of birth: MM/DD/YYYY Gender: M Country: Canada State or Province: Description: City: Zip or Postal code:

Company

Company: Primary job: Type to search... Worker type description: Worker type code: Department: Supervisor name: Job title: Contractors Manager Employee number:

Supervisors

Name	Email
 No supervisors	

Requests from this user do not require supervisor approval.

5. In the General tab, review the identity details including any associated supervisors, and the identity status (active or inactive).
6. (Optional) Additional tabs are also provided to review other details and options associated with the selected identity as follows:

Custom fields

Custom fields associated with the selected identity.

Access

Access associated with the selected identity.

Roles

Roles associated with the selected identity added by a provisioning policy or manually added.

Delegations

Delegations associated with the selected identity.

Direct reports

Reportees associated with the selected identity.

Access control

Access control associated with the selected identity including extended grant time, cardholder activation, provisioning attributes, and associated cardholders.

User permissions

Web portal user or administrator access permissions associated with the selected identity.

Visitor management

List of sites where selected identity can invite visitors.

Credentials

Synchronized credentials associated with the selected identity.

Tip: A credential synchronization can also be performed at the individual identity level. Select an identity then click the Credentials tab and click Synchronize.

Logs

Identity event logs for activities associated with the selected identity.

After you finish

[Modify your identities.](#)

5.9 | Modifying identities in ClearID

After you have added identities, you might need to modify the identity details. You can deactivate or activate an identity, or modify identity details after a change in job title, department, company, supervisors, personal information, and so on.

Before you begin

[Create your identities.](#)

What you should know

- Only account administrators, supervisors, or identities or roles with the required permissions can modify identities.
- Only account administrators can delete identities.

IMPORTANT: If you make updates to identities that are synchronized with an external data source, your changes can be overwritten by the synchronization.

Procedure

1. From the Home page, click Organization > Identities.
2. Select an option from the drop-down menu to display the identities that you require. Choose one of the following:

Active

Displays active identities.

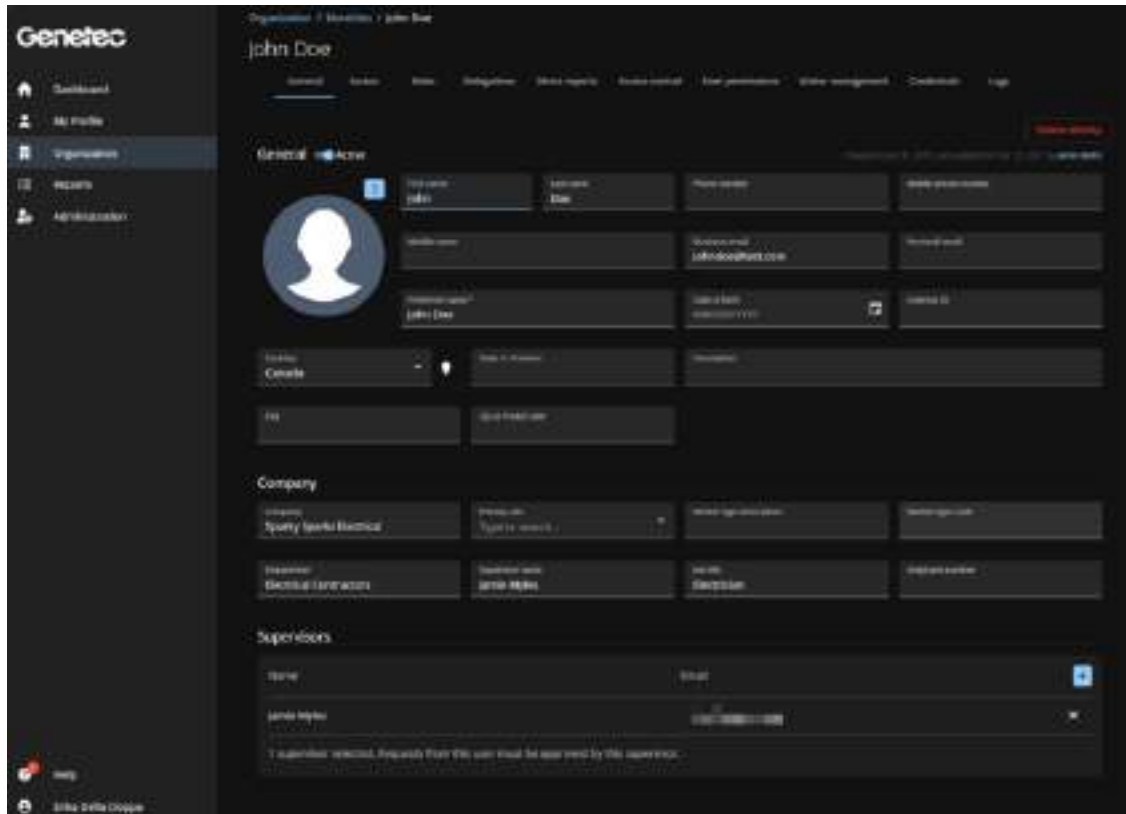
Inactive

Displays inactive identities.

All

Displays all active and inactive identities.

3. In the Search field, enter your search criteria and press enter.
4. Select an identity from the list to view the identity details.



5. Modify any settings, or deactivate or activate an identity as required.
For example, after a change in job title, department, company, supervisors, personal information, and so on.
6. Click Save to submit your changes.

After you finish

Delete Identities that are obsolete or no longer required.

Browse

- Synchronizing ClearID identity pictures with Security Center

5.10 | Deleting identities in ClearID

An administrator can delete identities that have become obsolete or are no longer required. For example, when a person leaves the organization, or when an identity was created in error.

Before you begin

You must have identities that were previously created, that are now ready for deletion.

What you should know

Only account administrators can delete identities.

- Search functions and audit trail information are retained after an identity is deleted so that you can check when the person had their access removed and the reason.
- The identity is also removed from all associated approver, owner, or manager lists or identity requests if applicable.

Procedure

1. From the Home page, click Organization > Identities.
2. Select an option from the drop-down menu to display the identities that you require. Choose one of the following:

Active

Displays active identities.

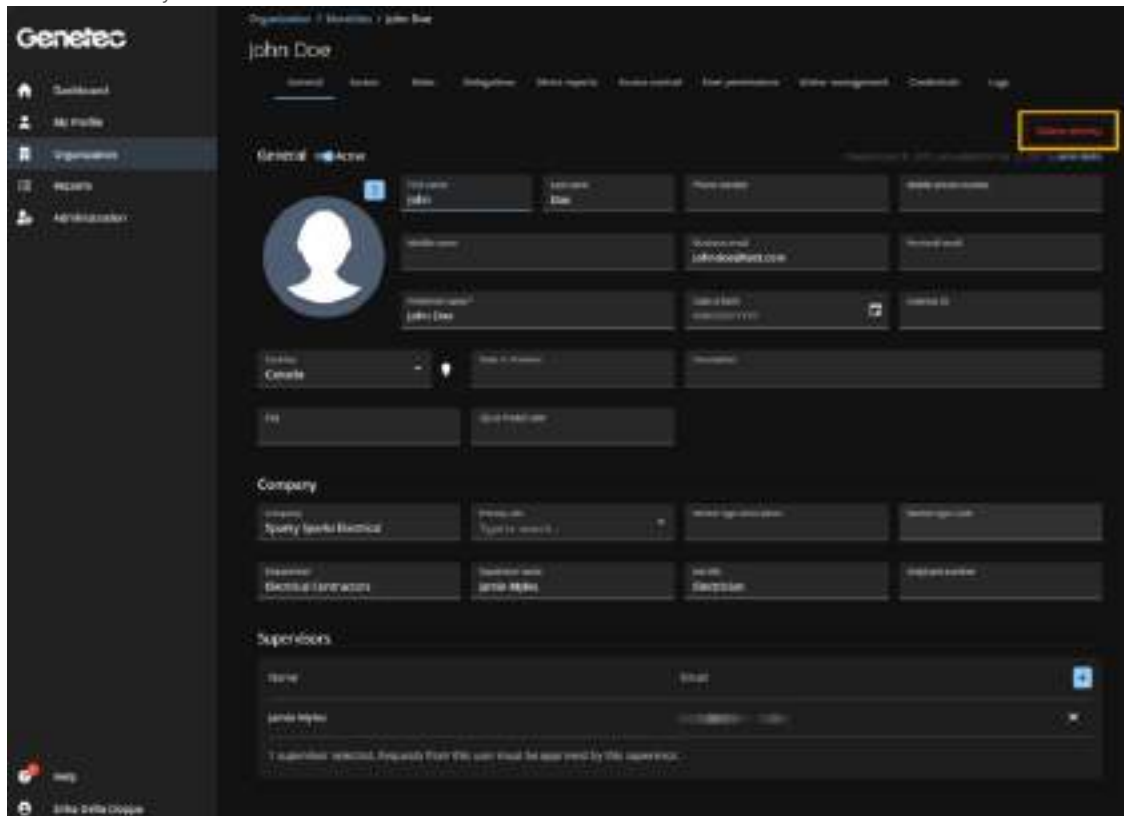
Inactive

Displays inactive identities.

All

Displays all active and inactive identities.

3. In the Search field, enter your search criteria and press enter.
4. Select an identity from the list to view the identity details.
5. Click Delete identity.



6. Click Remove to confirm the deletion.

5.11 | Synchronizing ClearID identity pictures with Security Center

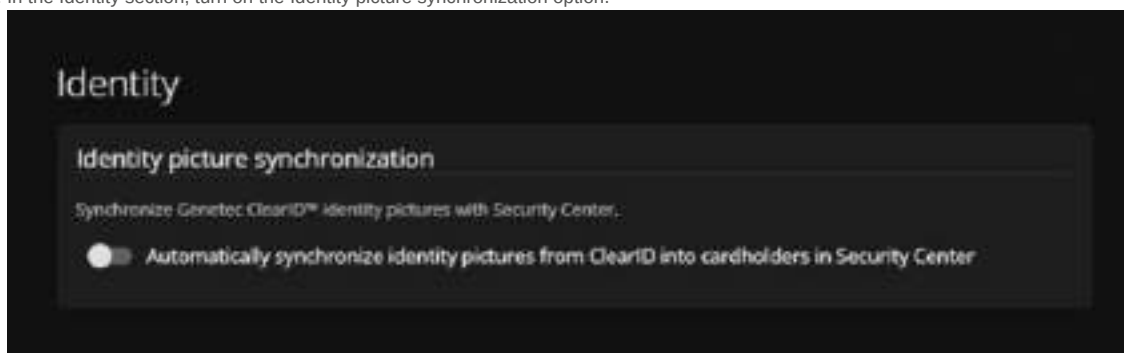
To manage identity and cardholder pictures in one place, *Account administrators* can set Genetec ClearID™ as the preferred data source for all cardholder pictures in Security Center.

Before you begin

Ensure that Security Center is connected to ClearID.

Procedure

1. In the ClearID web portal, click Administration > Account configuration.
2. In the Identity section, turn on the Identity picture synchronization option.



3. ClearID identity pictures are automatically synchronized with Security Center, replacing existing cardholder pictures. If updates to cardholder pictures are made directly through Security Center after Identity picture synchronization is turned on, ClearID overrides these updates.
NOTE: If no identity pictures are found in ClearID when identity picture synchronization is first turned on, cardholder pictures in Security Center aren't replaced.

Browse

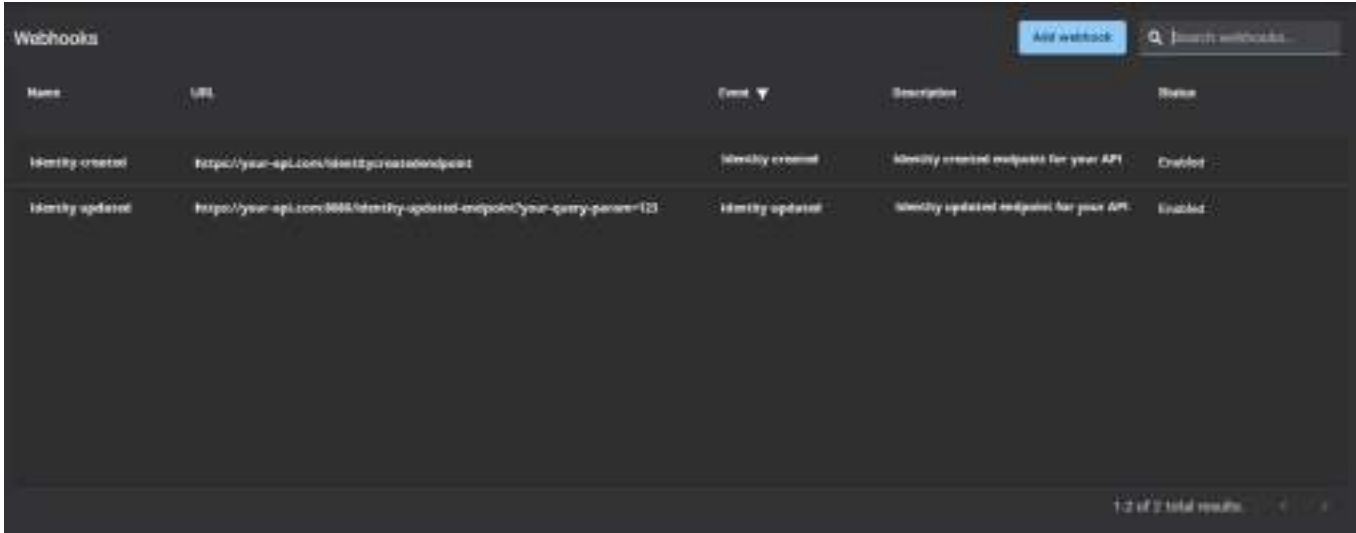
- Connecting Security Center to ClearID
- About cardholder and identity relationships
- Reviewing cardholders and identities information in ClearID
- Modifying identities in ClearID

5.12 | About webhooks in ClearID

A webhook is a user-defined HTTP callback. A webhook can be triggered by an event in a web application and can be used to send data or notifications to a third-party Application Programming Interface (API).

Webhooks in Genetec ClearID™

In ClearID, webhooks can be created and used to notify third-party APIs when specific events occur.



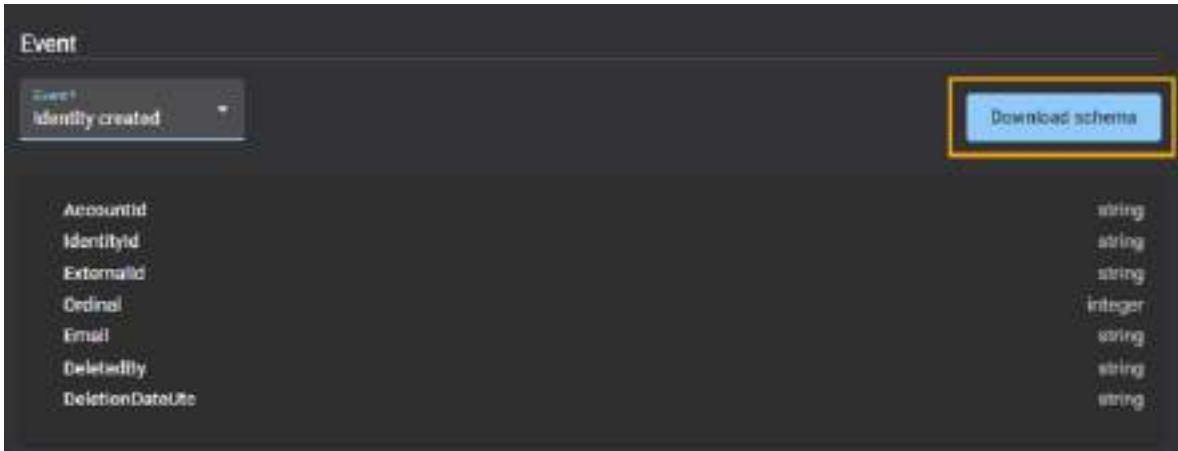
For example, an email notification with a link to detailed information about an identity could be sent when an Identity updated event occurs, or if you require other stakeholders to be notified after an Identity requests created or Identity requests updated event occurs.

Webhook processing

After the webhook is created, the webhook service listens for a subset of specified events coming from other ClearID services. When the specified event occurs the webhook service notifies the API specified in the Webhook details section URL field.

Webhook event schemas

The schema describes the object that is sent through the webhook and the contents of the schema vary depending on the event type specified. The webhook event schema can be downloaded from the Event section of the webhook to help understand the data structure of the events so that they can be retrieved and processed correctly on the user's side of the webhook integration.



For more information about downloading the schema, see [Creating webhooks in ClearID](#).

Webhook logs

Third-party API owners can use webhook logs to verify the status of every HTTP callback request sent to the third-party URL and to troubleshoot unreceived webhooks or other associated issues. For example, sender issues, receiver issues, and so on.

Webhook logs include the following:

Callback date

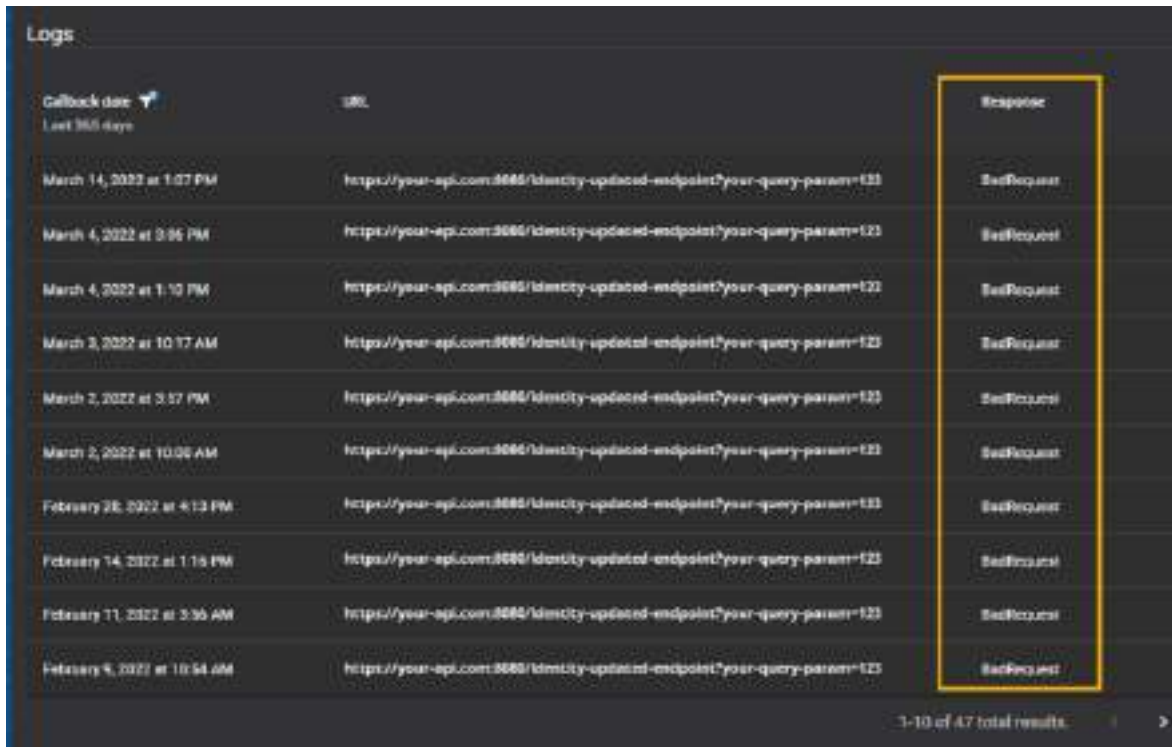
When the callback was sent (includes date range filters).

URL

The URL used to forward the webhook event notification to the relevant third-party API (program or application).

Response

The response state indicates whether the HTTP callback was successfully received by third-party API or not. For example, accepted, bad request, internal server error, and so on.



Callback date	URL	Response
Last 365 days		
March 14, 2022 at 1:07 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
March 4, 2022 at 9:06 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
March 4, 2022 at 1:10 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
March 3, 2022 at 10:17 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
March 2, 2022 at 3:57 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
March 2, 2022 at 10:06 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
February 28, 2022 at 4:13 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
February 14, 2022 at 1:16 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
February 11, 2022 at 3:36 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
February 9, 2022 at 10:54 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request

NOTE: The webhook Logs section is only displayed at the end of the webhook details after the first callback has occurred.

5.13 | Creating webhooks in ClearID

You can create webhooks in Genetec ClearID™ to integrate with third-party solutions APIs so that you can notify interested parties when specific events occur.

Before you begin

[Learn about webhooks.](#)

What you should know

- Only an account administrator can create webhooks in ClearID.
- External organizations are responsible for developing their own third-party solution APIs (programs or applications) that consume ClearID webhook HTTP callback notifications.

Procedure

1. From the Home page, click Administration > Webhooks.
2. Click Add webhook.

← BACK

Add webhook

General

Name *

Description

☒ Enabled

Webhook details

URL *

Secret

Additional headers

Name	Value
No additional headers found	

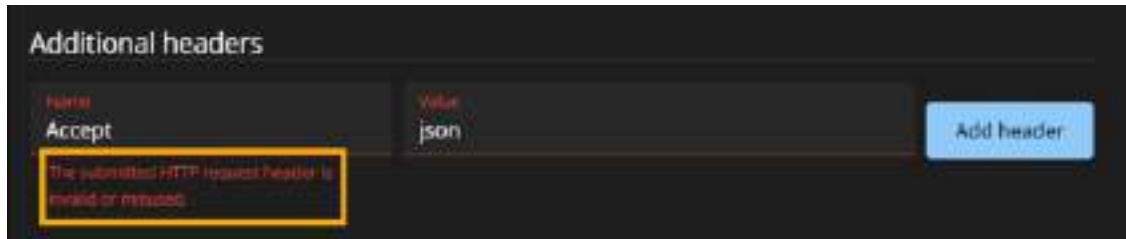
Add header

Event

Event *

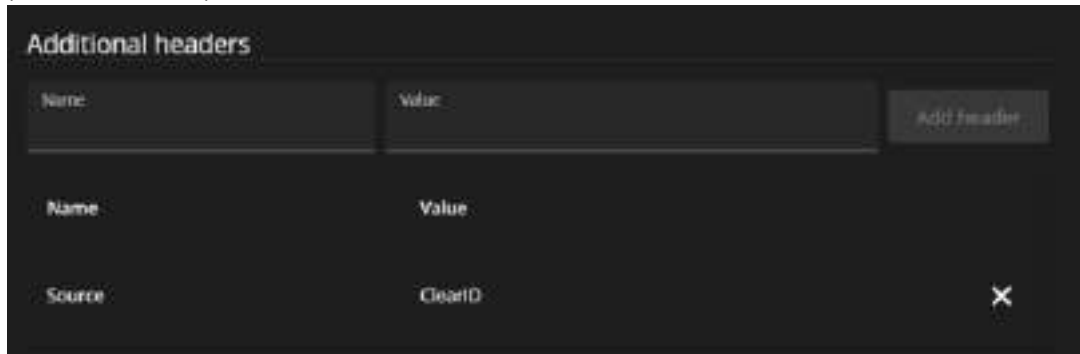
Download schema

3. In the General section, complete the fields:
 - a. (Optional) Select the Enabled checkbox to enable the webhook.
NOTE: When the webhook is *disabled*, the HTTP callback doesn't happen.
 - b. In the Name field, enter a meaningful Name so that you can easily identify your webhook later on.
For example, Identity updated or Identity requests created webhook and so on.
 - c. In the Description field, enter a Description that describes the purpose of the webhook.
For example, what the webhook is for, and what API (program or application) it notifies when events occur.
4. In the Webhook details section, complete the fields:
 - a. Enter a valid HTTPS:// URL for your API (program or application).
URLs can include ports and query parameters as follows:
 - Example 1: `https://my-api.com/identityupdatedendpoint`
 - Example 2: `https://my-api.com:8080/identity-updated-endpoint?my-query-param=123`This URL is used to forward the webhook event notification to the relevant third-party API (program or application).
NOTE: Your organization is responsible for providing the URL that you want the webhook event notifications forwarded to.
 - b. (Optional) Enter the Secret (App key) if required by the third-party API.
The secret (App key) is used to authenticate communications between the ClearID webhook and your organizations third-party API.
5. (Optional) In the Additional headers section, complete the fields:
Extra custom HTTP headers can be added in the HTTP callback request. These custom headers can be used by the third-party API on the user's side of the integration.
NOTE: If you enter an invalid or reserved header, the following message is displayed The submitted HTTP request header is invalid or misused.



- a. Enter the header parameter Name.

For example, if you had one event coming from multiple sources, extra HTTP request headers could be used to specify where event is coming from (ClearID or external API).



- b. Enter the header parameter Value.

- c. (Optional) Click Add header to add extra HTTP request headers as required.

For example, if your API is expecting or requires a specific set of headers (Host, Origin, Language, and so on).

- d. (Optional) Click  to remove any headers that are no longer required.

6. In the Event section, configure the settings you require:

- a. From the Event list, select an event that you want this webhook to listen for.

- b. Click Download schema and follow your browser prompts.

Best Practice: Use the downloaded schema information to understand the data structure of the events so that they can be retrieved and processed correctly on the user's side of the integration.

The following example shows an extract from a schema-identitycreated.json file:

Code

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "IdentityDeletedCallbackModel",
  "type": "object",
  "additionalProperties": false,
  "required": [
    "AccountId",
    "IdentityId",
    "DeletedBy",
    "DeletionDateUtc"
  ],
  "properties": {
    "AccountId": {
      "type": "string",
      "description": "The account id for which this identity is member of.",
      "minLength": 1
    },
    "IdentityId": {
      "type": "string",
      "description": "A unique id to identify the identity.",
      "minLength": 1
    },
    "ExternalId": {
      "type": [
        "null",
        "string"
      ],
      "description": "External ID"
    },
    "Ordinal": {
      "type": [
        "integer",
        "null"
      ],
      "description": "Commit ordinal in the storage.",
      "format": "int64"
    },
    "Email": {
      "type": [
```

```
"null",  
"string"  
],
```



7. Click Save.

Results

Your webhook is now configured to integrate with a third-party API (program or application) to notify interested parties when specific events occur.

After you finish

Using the downloaded schema, configure your third-party API to receive and process the webhook notifications.

5.13.1 | Modifying webhooks in ClearID

After you have created your webhooks, you might need to modify the webhook details. You can deactivate or activate a webhook, and modify the webhook details or event type if required.

Before you begin

[Create your webhooks.](#)

What you should know

Only an account administrator can modify webhooks in Genetec ClearID™.

Procedure

1. From the Home page, click Administration > Webhooks.
2. Select the webhook that you want to modify.
Tip: If the list is long, use the Search field to find the webhook that you require.
3. In the General section, modify the fields as required.
 - a. (Optional) Move the Enabled slider to enable or disable the webhook.

NOTE: When the webhook is *disabled*, the HTTP callback does not happen.
4. In the Webhook details section, modify the fields as required:
5. (Optional) In the Additional headers section, modify the fields as required:
6. In the Event section, modify the settings as required.
7. Click Save.

Parent topic: [Creating webhooks in ClearID](#)

5.14 | Viewing webhook logs in ClearID

To troubleshoot unreceived webhooks or other associated issues, third-party Application Programming Interface (API) owners can use the webhook logs to verify the status of every HTTP callback request sent to the third-party URL.

Before you begin

[Create your webhooks.](#)

What you should know

- Only an account administrator or third-party API owner can view webhook logs in Genetec ClearID™.
- The webhook Logs section is only displayed at the end of the webhook details after the first callback has occurred.

Procedure

1. From the Home page, click Administration > Webhooks.
2. Select the webhook that you want to troubleshoot.
Tip: If the Webhooks list is long, you can use the Search field to find the webhook that you require.
3. In the Logs section Callback date column, click to select a specified range or use the Date range picker to specify your own range.
NOTE: The callback data range time period is limited to a maximum of 1 year and the callback information is displayed in reverse chronological order.
The following image shows callback logs containing *Accepted* responses.

Logs		
Callback date 	URL	Response
Last 365 days		
May 2, 2022 at 3:16 PM	https://your-api.com/identitycreatedendpoint	Accepted
April 26, 2022 at 5:40 PM	https://your-api.com/identitycreatedendpoint	Accepted
April 12, 2022 at 4:18 PM	https://your-api.com/identitycreatedendpoint	Accepted
March 28, 2022 at 3:23 PM	https://your-api.com/identitycreatedendpoint	Accepted
March 28, 2022 at 9:47 AM	https://your-api.com/identitycreatedendpoint	Accepted
March 25, 2022 at 10:22 AM	https://your-api.com/identitycreatedendpoint	Accepted
March 25, 2022 at 5:18 AM	https://your-api.com/identitycreatedendpoint	Accepted
March 25, 2022 at 4:49 AM	https://your-api.com/identitycreatedendpoint	Accepted
March 24, 2022 at 10:31 AM	https://your-api.com/identitycreatedendpoint	Accepted
March 24, 2022 at 9:28 AM	https://your-api.com/identitycreatedendpoint	Accepted
1-10 of 58 total results. < >		

The following image shows callback logs containing *BadRequest* responses.

Logs		
Callback date 	URL	Response
Last 365 days		
March 14, 2022 at 1:07 PM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
March 4, 2022 at 3:05 PM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
March 4, 2022 at 1:10 PM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
March 3, 2022 at 10:17 AM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
March 2, 2022 at 3:57 PM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
March 2, 2022 at 10:06 AM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
February 28, 2022 at 4:13 PM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
February 14, 2022 at 1:16 PM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
February 11, 2022 at 3:36 AM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
February 9, 2022 at 10:54 AM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
1-10 of 47 total results. < >		

4. Review the Logs information as follows:
 - a. In the Callback date column, check when the callback was sent (includes date range filters).
 - b. In the URL column, verify the URL used to forward the webhook event notification that a specified event occurred to the relevant third-party API (program or application).
 - c. In the Response column, review the states to verify whether the HTTP callback was received successfully by third-party API or not. For example, Accepted, BadRequest, InternalServerError, and so on.
 - d. (Optional) Navigate through the callback logs (forwards or backwards in time) by clicking the Next page or Previous page icons.

5.15 | Granting access to the ClearID web portal

Before a user can access the Genetec ClearID™ web portal, you must grant them the required *User* or *Administrator* permissions for the website.

Before you begin

The identity that you want to grant access to must exist in the system.

What you should know

- To grant *User* or *Administrator* permissions for the website, you must be an account administrator.

Procedure

Choose one of the following:

- Grant user access to the web portal
- Grant administrator access to the web portal

Results

The selected identity now has access to the web portal with either User or Administrator privileges.

After you finish

[Log on to the web portal.](#)

Browse

- Viewing sites where a user can invite visitors

5.15.1 | Granting user access to the ClearID web portal

Before a user can access the Genetec ClearID™ web portal, you must grant them the required permissions for the website.

Before you begin

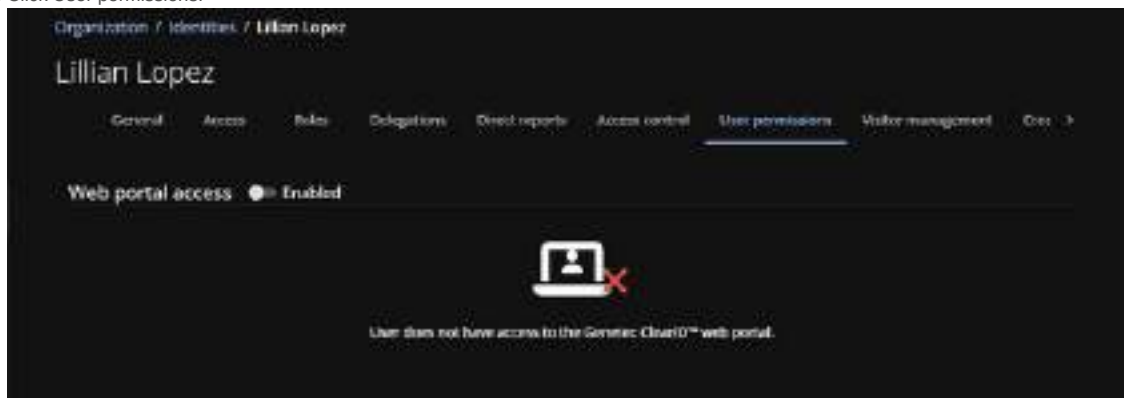
The identity that you want to grant access to must exist in the system.

What you should know

- To grant user permissions for the website, you must be an account administrator.

Procedure

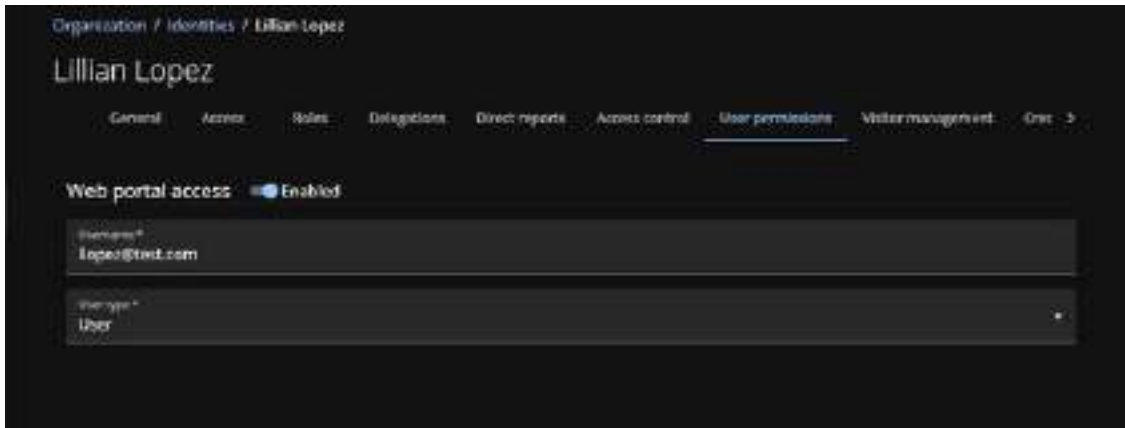
1. Click Organization > Identities.
2. Search for a user or select one from the Identities list.
3. Click User permissions.



4. In the User permissions section, click or move the Web portal access slider to Enabled to grant access to the web portal.
If the slider is disabled the identity cannot access the web portal.

NOTE: Some organizations do not enable web portal access for some or all of their identities because their organization does not require employee requests or web portal access.

5. In the Username field, enter a valid email address.
6. In the User type list, select User for default user access to the web portal.
7. Click Save to confirm your changes.

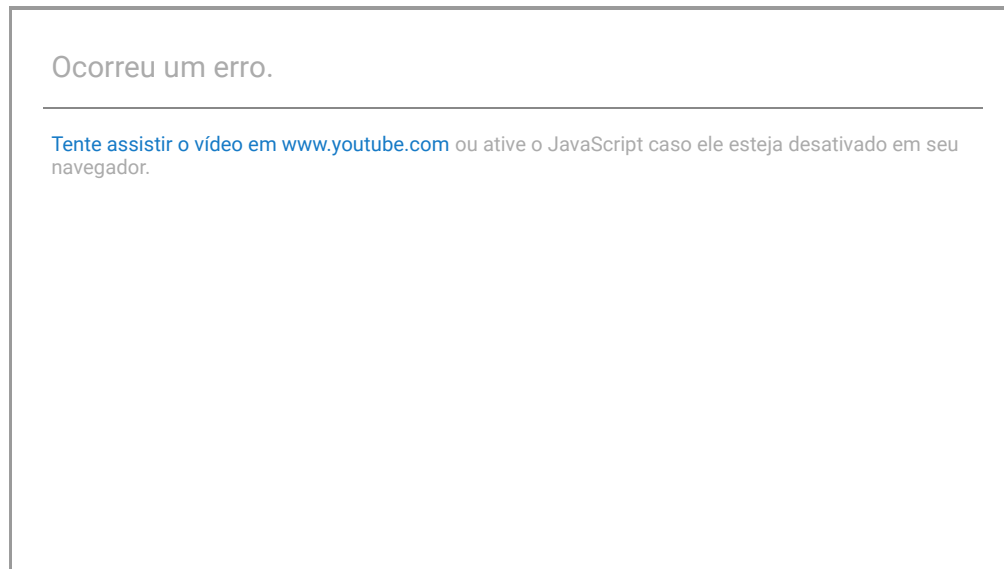


Results

The selected identity now has access to the web portal with the default User privileges.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.



After you finish

Log on to the web portal.

Parent topic: Granting access to the ClearID web portal

5.15.2 | Granting administrator access to the ClearID web portal

Before an administrator can access the Genetec ClearID™ web portal, you must grant them the required permissions for the website.

Before you begin

The identity that you want to grant access to must exist in the system.

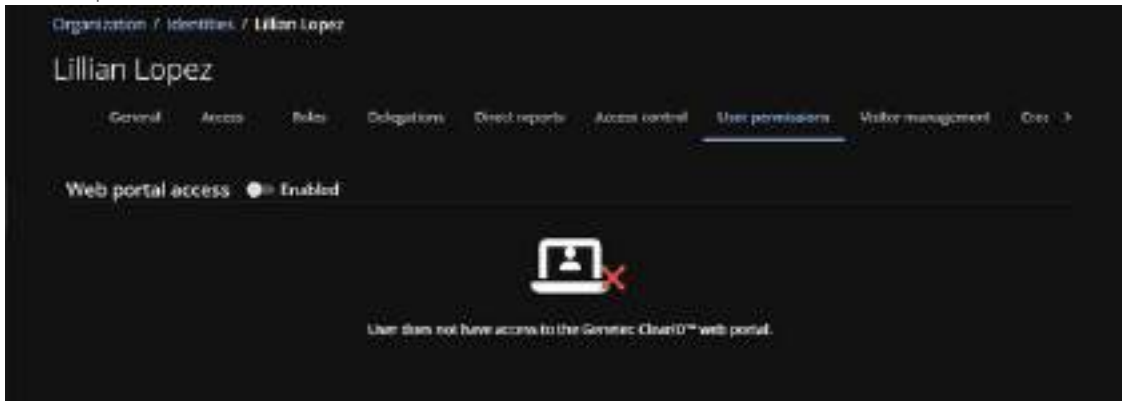
What you should know

- To grant administrator permissions for the website, you must be an account administrator.

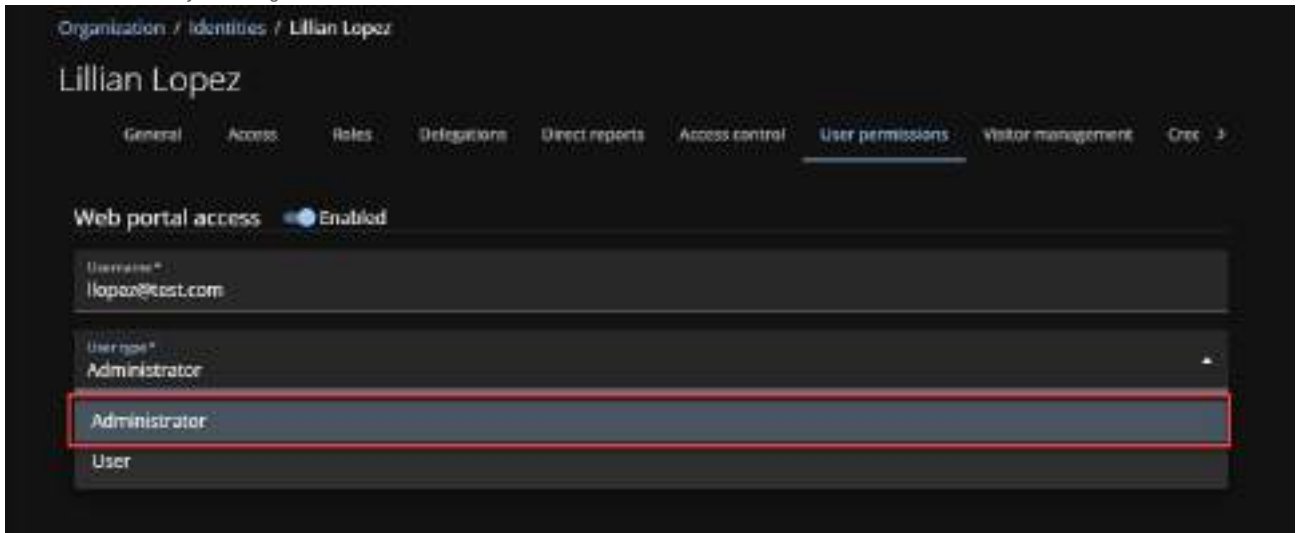
IMPORTANT: When a new account is created, an end user designated as the account administrator will receive a Welcome to Genetec ClearID™ and a New ClearID Account - ACCOUNTNAME email notification. By default, Administrator access is given to the end user that receives the email. If a system integrator or other identity also requires administrator access, their administrator access must be added by the end user (account administrator).

Procedure

1. Click Organization > Identities.
2. Search for a user or select one from the Identities list.
3. Click User permissions.



4. In the User permissions section, click or move the Web portal access slider to Enabled to grant access to the web portal.
If the slider is disabled the identity cannot access the web portal.
NOTE: Some organizations do not enable web portal access for some or all of their identities because their organization does not require employee requests or web portal access.
5. In the Username field, enter a valid email address.
6. In the User type list, select Administrator for Administrator access to the web portal.
7. Click Save to confirm your changes.



Results

The identity now has access to the web portal with Administrator privileges.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Log on to the web portal.

Parent topic: Granting access to the ClearID web portal

5.16 | Viewing your profile in ClearID

You can use the Profile page to view your profile and check your access or role membership in Genetec ClearID™.

What you should know

- The profile in ClearID is displayed to the employee in a read-only view and can't be modified. The profile contains the site, worker type description, supervisor name, and other information.
- An *employee* can check their profile at any point in time to understand what information ClearID stores about them. They can also see if the information is outdated and request an update.

Tip: Check your department or job title after a job change to ensure that you have the correct access.

Procedure

1. From the homepage, click My Profile.

The screenshot shows a user profile page for 'John Doe'. At the top, there's a 'My Profile' header with a sub-header 'John Doe'. Below this is a navigation bar with tabs: 'General', 'Access', 'Roles', 'Delegations', 'Direct reports', 'Credentials', 'Preferences', and 'Manage'. The 'General' tab is selected. The main content area is titled 'My Profile' with a status 'Active'. It features a profile picture of a man with glasses and a beard. Below the picture are several input fields for personal information: 'First name' (John), 'Last name' (Doe), 'Phone number', 'Mobile phone number', 'Middle name', 'Business email' (jdoe@hmi.com), 'Personal email', 'Preferred name' (John), 'Date of birth' (MM/DD/YYYY), 'Gender', 'Country' (Canada), 'State or Province' (Quebec), 'City', 'City or Postal code', 'Company' (Genetec), 'Primary role' (Type to search...), 'Work email domain', 'Work email code', 'Department' (United Content Services), 'Supervisor name', 'Job title' (Content Developer), and 'Employee number'. Below the company section is a 'Supervisors' section with a table header 'Name' and 'Email'. The table is empty, and a message states 'No supervisors'. At the bottom of the supervisors section, it says 'Requests from this user do not require supervisor approval.'

2. In the General tab, review your identity details including any associated supervisors, and the identity status (active or inactive).
3. (Optional) Additional tabs are also provided to review other details and options associated with your identity as follows:

Custom fields

Custom fields associated with your identity.

Access

Access associated with your identity.

Roles

Roles associated with your identity added by a provisioning policy or manually added.

Delegations

Delegations associated with your identity.

Direct reports

Reportees associated with your identity.

Access control

Access control associated with your identity including extended grant time, cardholder activation, provisioning attributes, and associated cardholders.

User permissions

Web portal user or administrator access permissions associated with your identity.

Visitor management

List of sites where your identity can invite visitors.

Credentials

Synchronized credentials associated with your identity.

Logs

Identity event logs for activities associated with your identity.

After you finish

[View your site and area access.](#)

5.16.1 | Configuring your ClearID portal theme preferences

You can customize your Genetec ClearID™ portal theme to match your personal preferences by choosing between light or dark mode.

What you should know

Your theme preferences only apply to your user profile. If you don't configure a personal theme, your theme matches the portal theme configured by the *Administrator*.

Procedure

1. In the ClearID web portal, click My Profile > Preferences.
2. In the Theme section, configure your theme preferences.
 - a. From the Mode list, choose between Light, Dark, and System.

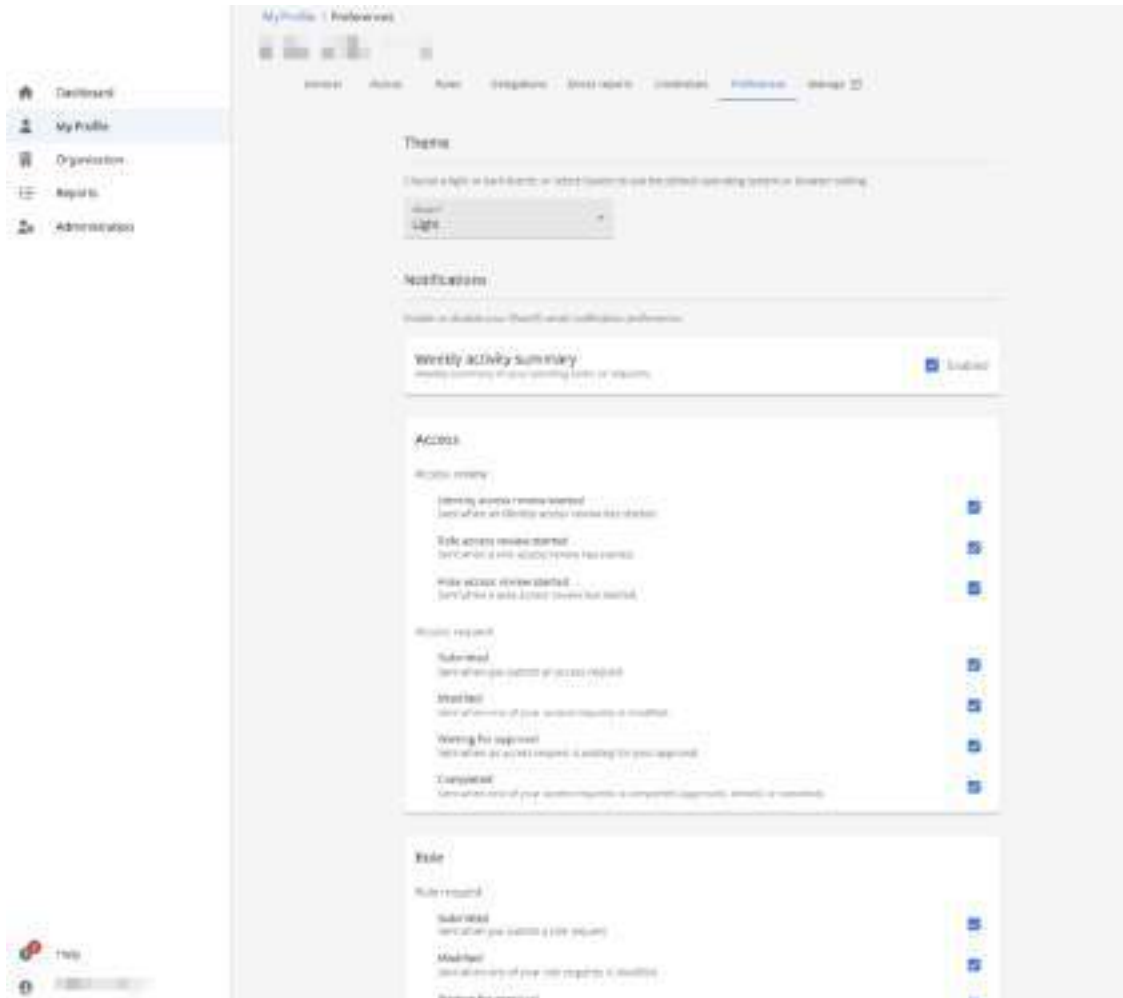


NOTE: Selecting System uses your default operating system or browser settings.

3. Click Save.

Example

The ClearID portal of a user with light mode selected:



Parent topic: Viewing your profile in ClearID

5.17 | Viewing your site and area access in ClearID

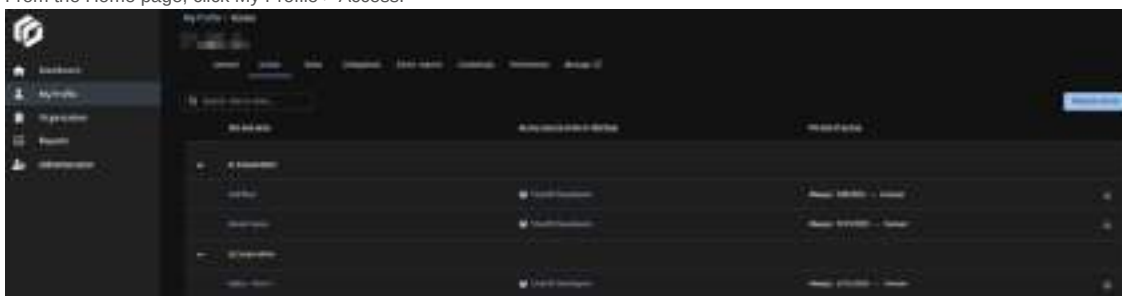
You can use the Profile Access page to review your site and area access. This information can be used to help you identify if you need to request more access in your main site or other sites.

What you should know

The Access page displays all sites and areas that the logged in user has access to and includes the access source and the period of access.

Procedure

1. From the Home page, click My Profile > Access.



- The sites and areas you have access to are displayed in the Site and area column.
2. (Optional) Click the blue text in the Site and area column to jump to the Access page.
3. (Optional) Click the blue text in the Access source column to jump to the Roles page.

After you finish

Submit access requests for other areas as required.

5.18 | Setting request visibility for users in ClearID

To manage the types of requests that web portal users can make, you can change the request visibility settings in the Genetec ClearID™ web portal.

What you should know

You must be an *Account administrator* to change request visibility settings.

NOTE: Changing these settings affects the types of requests all web portal users can make.

Procedure

1. In the ClearID portal, click Administration > Account configuration.
2. In the Request visibility section, configure the settings as needed:

Enable request visibility for web portal users

Turn on the Enable request visibility for web portal users option to allow users to make requests in the web portal.

Request access

Select Request access to allow users to request access to an area for themselves, for roles, or for other identities.

Request role

Select Request role to allow users to request role membership for themselves or for other identities.

Request an identity

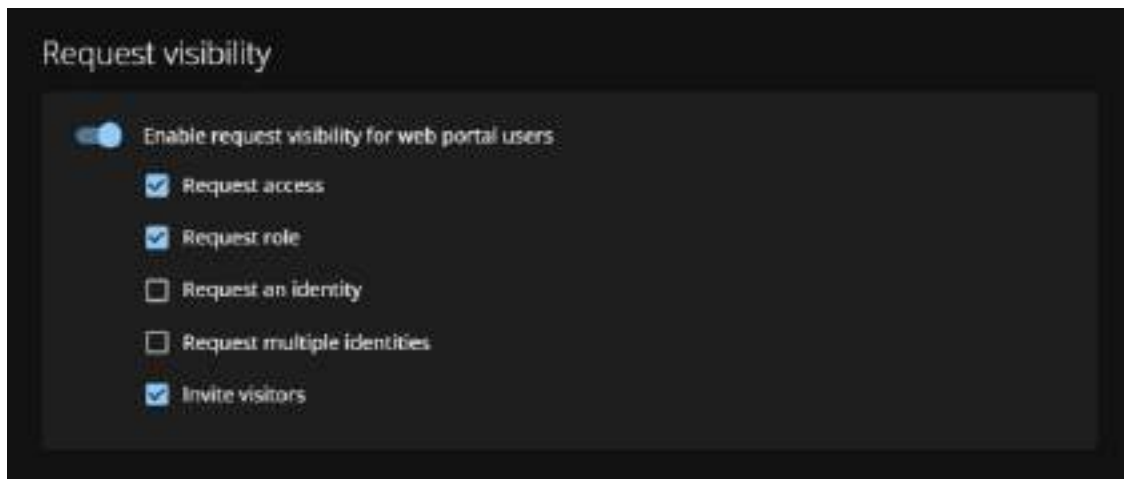
Select Request identity to allow users to create an identity in the system.

Request multiple identities

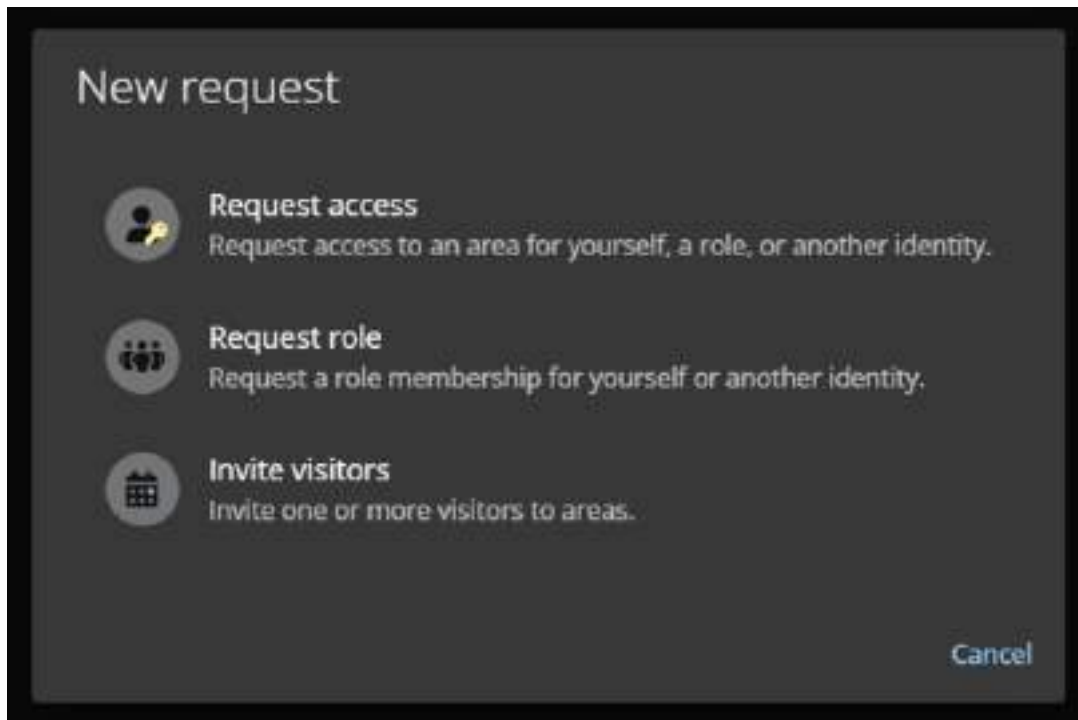
Select Request multiple identities to allow users to create multiple identities in the system.

Invite visitors

Select Invite visitors to allow users to invite one or more visitors to areas.



3. Click Save.
Users can only access selected request types in the New request dialogue.

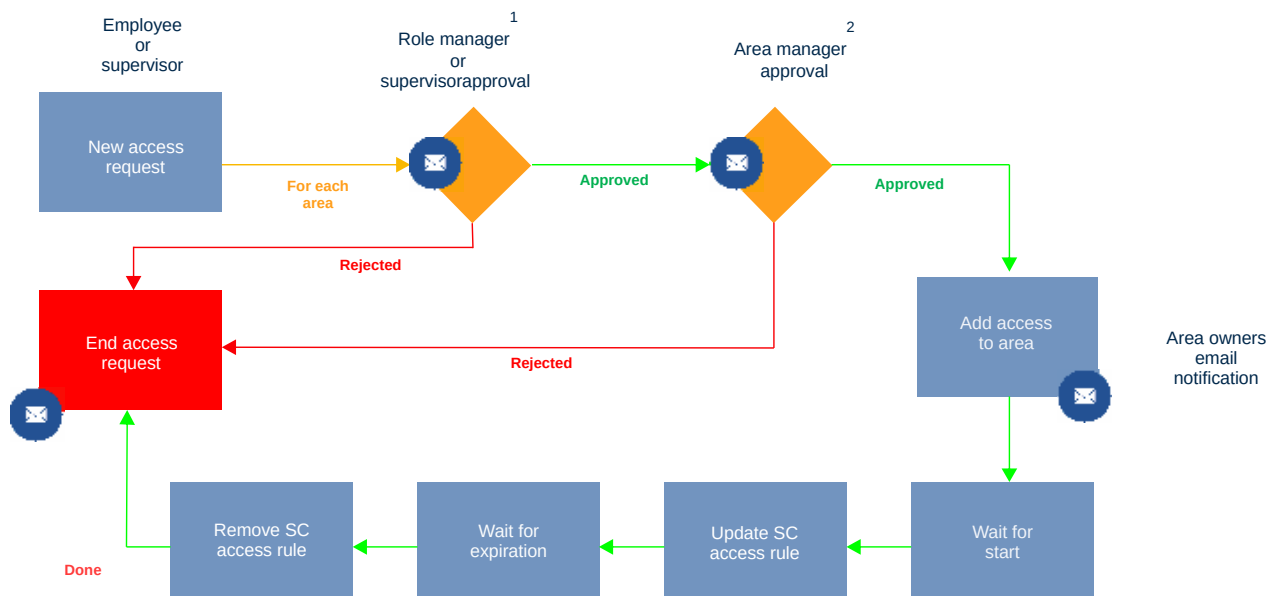


5.19 | About access request workflow in ClearID

An access request workflow is a series of activities performed by the system or authorized people during the life cycle of an access request. The activities can change the state and properties of access requests, affect other entities in the system, or wait for a condition to be met.

The workflow helps automate access request tasks, such as approving or rejecting access requests, so that people involved in the review and approval process can focus on other tasks.

The following diagram illustrates the *access request workflow* that occurs in Genetec ClearID™ and Synergis™.



¹ (Optional) Role manager or supervisor approval can be enabled for the area.

² (Optional) Area manager approval can be enabled for the area.

NOTE: By default, access requests are limited to the minimum access required. This limits what a user can do with an access card.
Browse

- About workflows in ClearID
- Creating exceptions to the access request approval workflow in ClearID

5.20 | Requesting access in ClearID

To request access for yourself, another identity, or a team member, you can use the Genetec ClearID™ self-service portal. Using a self-service portal with area managers specified simplifies the approval process, and avoids interrupting a chain of people who might or might not be the correct approvers.

Before you begin

- Familiarize yourself with workflows.

What you should know

Employees, managers, and supervisors of different secure areas can request access for themselves or their employees using a self-service Web portal.

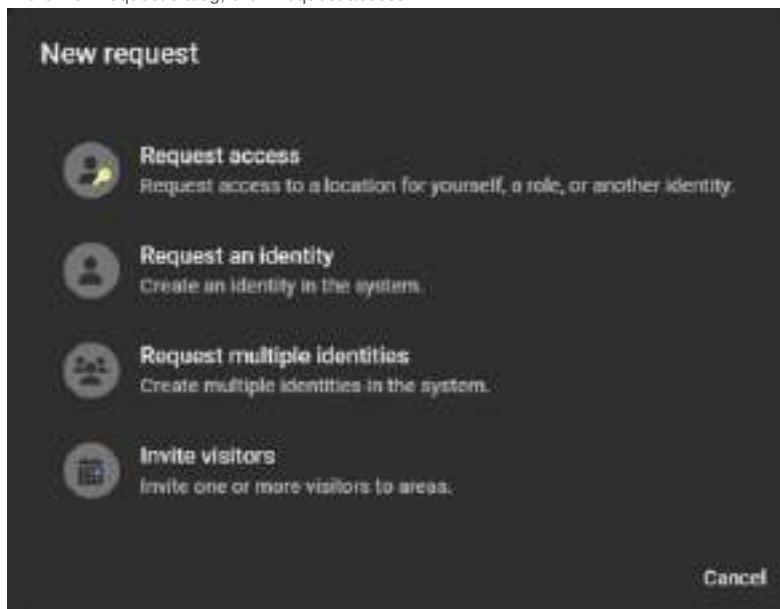
NOTE: In the past, most sites access control solutions would typically not track or record why access was required.

In ClearID, the access request includes: who requested access, site, area, when, and why the access is required.

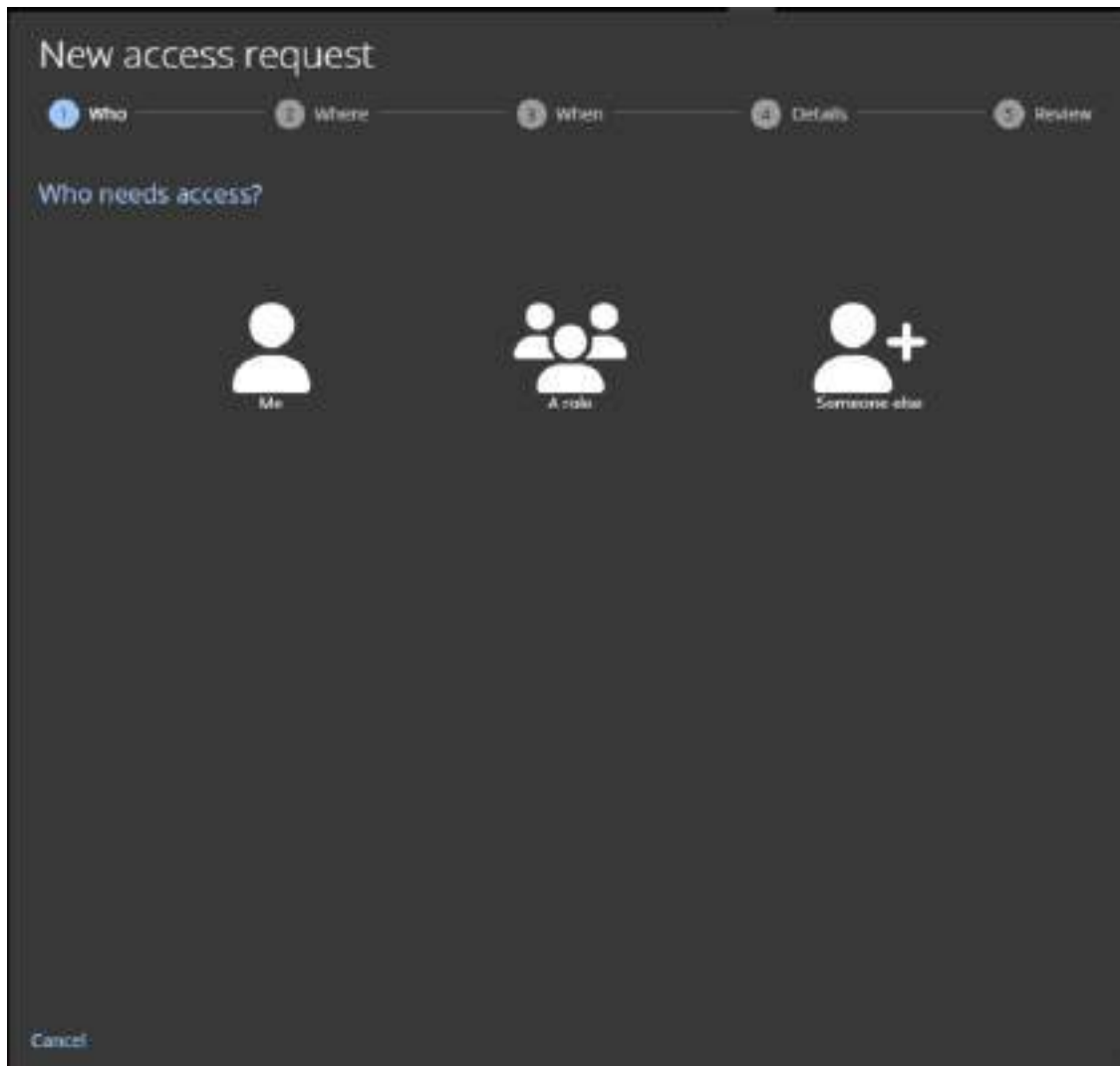
- Separate access requests and approval workflows are created for each request for access to an area.
- After the request summary is confirmed, it's automatically assigned to the right individuals for approval.
- After the approval process occurs, the requester receives an email notifying them whether the access request was approved or rejected.

Procedure

1. Log on to the self-service portal.
2. Click Dashboard > My requests.
3. Click New request.
4. In the New request dialog, click Request access.



5. In the Who section of the New access request dialog, click an option to choose who needs access:



a. (Optional) If you selected Me, the New access request wizard is automatically updated to include the information of the currently logged in user.

b. (Optional) If you selected A role, search for or select a role from the list.

The New access request wizard is updated to include the information of the selected role.

IMPORTANT: Only a *role owner* or *role manager* can view and request access for roles. They can only request access for the roles that they manage.

c. (Optional) If you selected Someone else, search for or select an individual from the list.

The New access request wizard is updated to include the information of the selected individual.

NOTE: A supervisor or team leader can request access for someone in their team, group, or department.

6. In the Where section of the New access request dialog, select a site from the site list.

a. Search for or select one or more areas and click Next.

The screenshot shows a dark-themed dialog box titled "New access request for John Doe". At the top, there is a progress bar with five steps: "Who" (checked), "Where" (active), "When", "Details", and "Review". Below the progress bar, the question "Which site do you need access to?" is displayed. A dropdown menu labeled "Site*" shows "Genetec Albert Einstein" as the selected option. Below this, the question "Which areas do you need access to?" is shown, followed by a note: "One request will be created for each area selected. A maximum of 10 areas can be selected at a time." A search bar labeled "Areas" contains the text "Main Entrance" and an "Add more" button. To the right of the search bar is a placeholder text "Type to search...". At the bottom left is a "Cancel" button, and at the bottom right are "Back" and "Next" buttons.

NOTE: Only areas created with Public visibility are shown in this list.

7. In the When section of the New access request dialog, enter the dates that you require or select them using the calendar picker.

The screenshot shows a web-based form titled "New access request for John Doe". At the top, there is a progress bar with five steps: "Who" (checked), "Where" (checked), "When" (active), "Details" (disabled), and "Review" (disabled). Below the progress bar, the section "When do you need access?" contains two informational icons: one stating "A site policy limit is currently active, individual access is limited to 30 days" and another stating "The dates and times shown here are in the America/Toronto time zone." Below these are two date pickers: "Start date*" set to "04/03/2025" and "End date*" set to "04/04/2025". A "Duration" dropdown is set to "2 d". The section "Following which schedule?" includes the instruction "Select a period with a schedule that meets your access requirements for each area." Below this, there is a table with one row: "Main Entrance" and a "Schedule*" dropdown menu set to "Always". At the bottom left is a "Cancel" button, and at the bottom right are "Back" and "Next" buttons.

- a. Select the schedule that you require for each area and click next.

IMPORTANT: If a site access duration has been enabled, you can't select a duration that exceeds the maximum limit specified in the site access configuration.

8. In the Details section of the New access request dialog, enter the reason for the access request.

NOTE: The Reason for request is a required field and the reason is stored for access review auditing purposes.

- a. Upload any supporting documents to the access request and click Next.

New access request for John Doe

✓ Who

✓ Where

✓ When

4 Details

5 Review

Why do you require this access?

Reason for request *

Access required while performing maintenance work.

50 / 300

Mandatory documents

Driver's license * Provided ⓘ

✕

JohnDoe_DriverLicense.pdf

10 KB

Certificate of qualification * Provided ⓘ

✕

JohnDoe_CertificateOfQualification.pdf

10 KB

Work permit * Provided ⓘ

✕

JohnDoe_WorkPermit.pdf

10 KB

Cancel

Back

Next

9. Review the request summary.

New access request for John Doe

✓ Who

✓ Where

✓ When

✓ Details

5 Review

Review

The following access requests will be created.



Genetec Albert Einstein • Main Entrance
April 3, 2025 to April 4, 2025 • Always

Cancel

Back

Request access

- If changes are required, click Back and modify the settings.
- If the information is correct, click Request access to submit the access request.
- Click Finish to return to My requests.

Results

Your access request has been submitted and is waiting for the required approvals. Depending on your setup, the request is either automatically approved or waiting for the required approvals. In some situations, the access request might also be manually or automatically canceled or rejected.

Waiting for the required approvals. In some situations, the access request might also be manually or automatically canceled or rejected.

Dashboard

My requests

My location

Help

All

View details

Type	Status	Description	Date submitted
John Doe Access request • All ID	Pending for approval	Genetec Albert Einstein Main Entrance 4/3/2025 to 4/4/2025	12 minutes ago
Jack Access request • All ID	Approved	Genetec Albert Einstein Main Entrance 2/14/2024 to 2/14/2024	1 month ago
John Doe Access request • All ID	Canceled	Genetec Head Office Training Room 11/20/2024 to 11/23/2024	4 months ago
John Doe Access request • All ID	Canceled	Genetec Head Office Training Room 10/18/2024 to 10/25/2024	3 months ago
Jack Access request • All ID	Approved	Genetec Montreal Data Center 8/20/2024 to 8/26/2024	1 month ago

0 Canceled Request

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Confirm whether the request was approved or rejected:

- Check your email for an *Access approved* email.
- Check My requests in ClearID.

Browse

- [Setting a maximum duration for site access in ClearID](#)
- [About email notifications in ClearID](#)
- [Checking the status of access requests in ClearID](#)

Browse

- [Access Request Feature Note \(2 pages\)](#)

5.21 | Adding supervisors manually in ClearID

To help manage requests from your direct reports, you can manually add supervisors to the relevant identity profiles so that the supervisor approval workflow can be used.

Before you begin

[Create your identities.](#)

What you should know

This procedure is for Supervisors who have direct reports.

- To manually add supervisors to identity profiles, you must be an account administrator.

Procedure

1. From the homepage, click Organization > Identities.
2. Search for or select an identity from the list.
 - a. (Optional) Use the Active, Inactive, or All filters to narrow your search.
3. Click the identity that you require.
4. In the Supervisors section, click .

The screenshot shows the Genetec ClearID user management interface for a user named John Doe. The interface is divided into several sections: General, Company, and Supervisors. The Supervisors section is highlighted with a yellow box, showing a list of supervisors and a 'No supervisors' message. The 'Add' button is also highlighted with a yellow box.

5. Search for or select one or more users from the list that you want to add as supervisors and click Add to confirm your selection.
NOTE: Adding multiple supervisors is useful when employees or supervisors work shifts or a rotating days system. In these situations, it's common to have multiple supervisors for different employees on different days.
6. (Optional) Click  to remove any supervisors that are no longer required.
7. Click Save to confirm your changes.

Results

The supervisors that you selected have now been added to the supervisors list for this identity.

The screenshot shows the Genetec ClearID user management interface for a user named John Doe. The interface is divided into several sections: General, Company, and Supervisors. The Supervisors section is highlighted with a yellow box, showing a list of supervisors and a 'No supervisors' message. The 'Add' button is also highlighted with a yellow box.

After you finish

View your direct reports.

5.22 | Viewing direct reports in ClearID

As a *Supervisor*, you can check the access control status, general identity information of your direct reports. You can also use the direct report list for security reviews or auditing purposes.

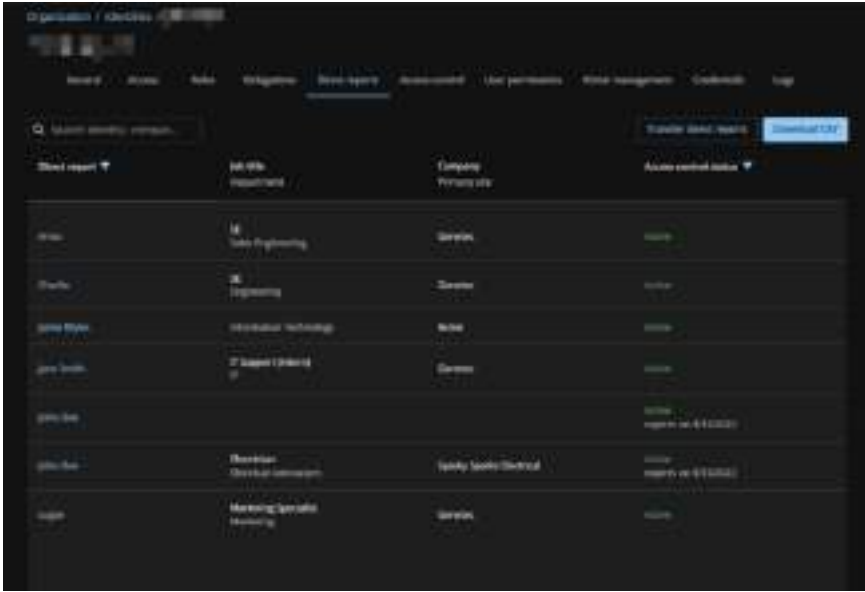
Before you begin

To view *direct reports*, you must be a *Supervisor* or *Account administrator*.

- A *Supervisor* can check general identity information for their direct reports at any point in time, to understand what information Genetec ClearID™ stores about them. They can also see if the information is outdated and request an update.
- An *Account administrator* can check the direct reports of an identity to validate the supervisor link and other information.

Procedure

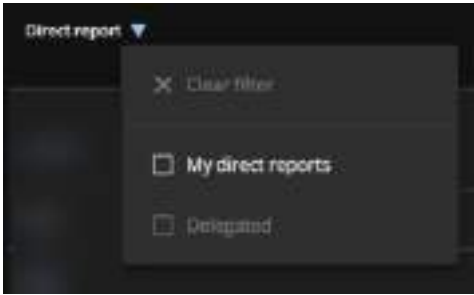
1. From the Home page, click My Profile > Direct reports.



2. Filter the list based on your required criteria:

Direct reports

Click the Direct report filter icon (Y) to filter the list. Choose either My direct reports, Delegated, or both.



My direct reports

Displays employees that are your direct reports.

Delegated

Displays delegated employees (because another user delegated their tasks to you).

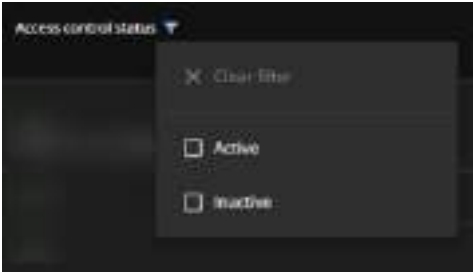
NOTE: Delegated employees are highlighted in the list using a DelegateFromAnotherUser icon .

Clear filter

Click Clear filter (X) to remove selected filters.

Access control status

Click the Access control status filter icon (🔍) to filter the list. Choose either Active, Inactive, or both.



Active

Displays direct reports with an Active access control status.

Inactive

Displays direct reports with an Inactive access control status.

Clear filter

Click Clear filter (✖) to remove selected filters.

Search

Use the Search bar to search for an identity by first name, last name, or company.

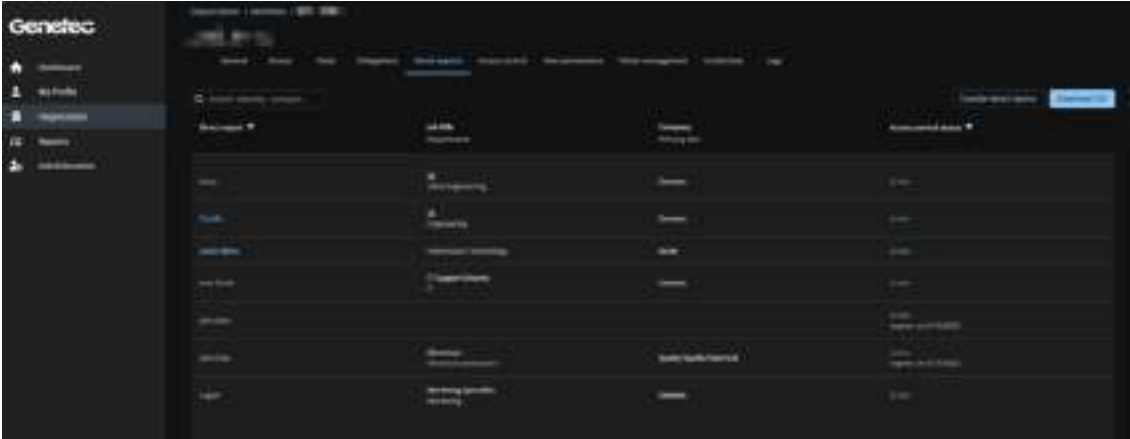
3. Click Download CSV, to download a copy of the direct reports list in CSV format. The report can then be used for auditing purposes, to keep a physical copy, to attach to an audit request, to review offline, or to manipulate or consolidate data in a spreadsheet for other audiences.
 - a. Follow your browser prompts to complete downloading the exported file.

The file is exported as a .CSV file to the default download location for your browser (ClearID Direct reports.csv).

NOTE: The columns and entries in the CSV file can vary depending on the filters you've selected when you download the report.
4. (Optional) Click the name of a direct report in the list to view their identity profile in more detail.

You can also view more details about the identity by browsing the following identity profile pages:

- General
- Access
- Roles
- Delegations
- Access control
- User permissions
- Visitor management
- Credentials
- Logs



After you finish

Manage your direct reports access and roles if required.

Browse

- Adding supervisors manually in ClearID
- Creating identities in ClearID
- About direct reports report in ClearID

5.23 | Managing direct reports in ClearID

Supervisors can manage their direct reports access. This can include general identity information, area access, modifying or removing roles, task delegation, and access control.

Before you begin

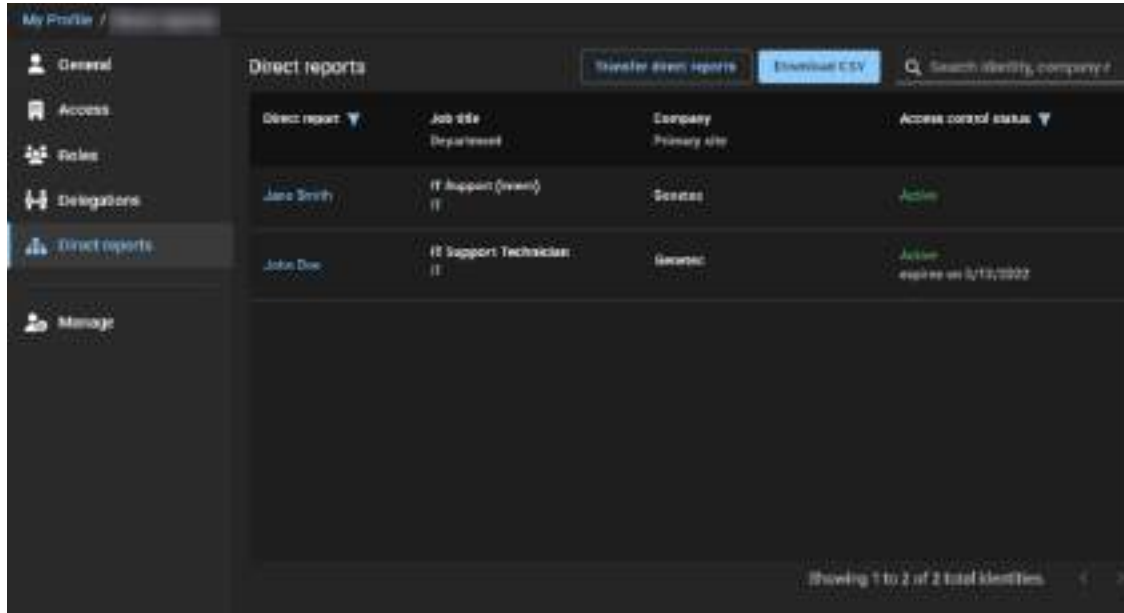
- Adding supervisors manually in ClearID.
- (Optional) Add supervisor access to manage direct reports.

What you should know

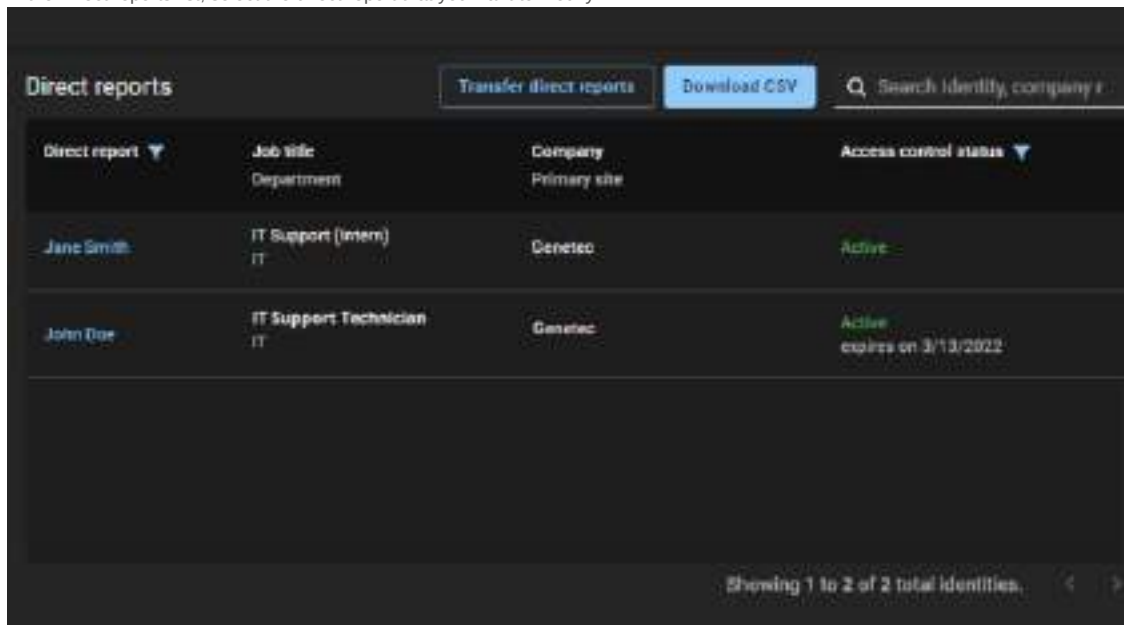
- To manage *direct reports*, you must be a supervisor.
- To modify General identity information or Access control settings for a direct report, you must be a supervisor with the manage direct reports permission.

Procedure

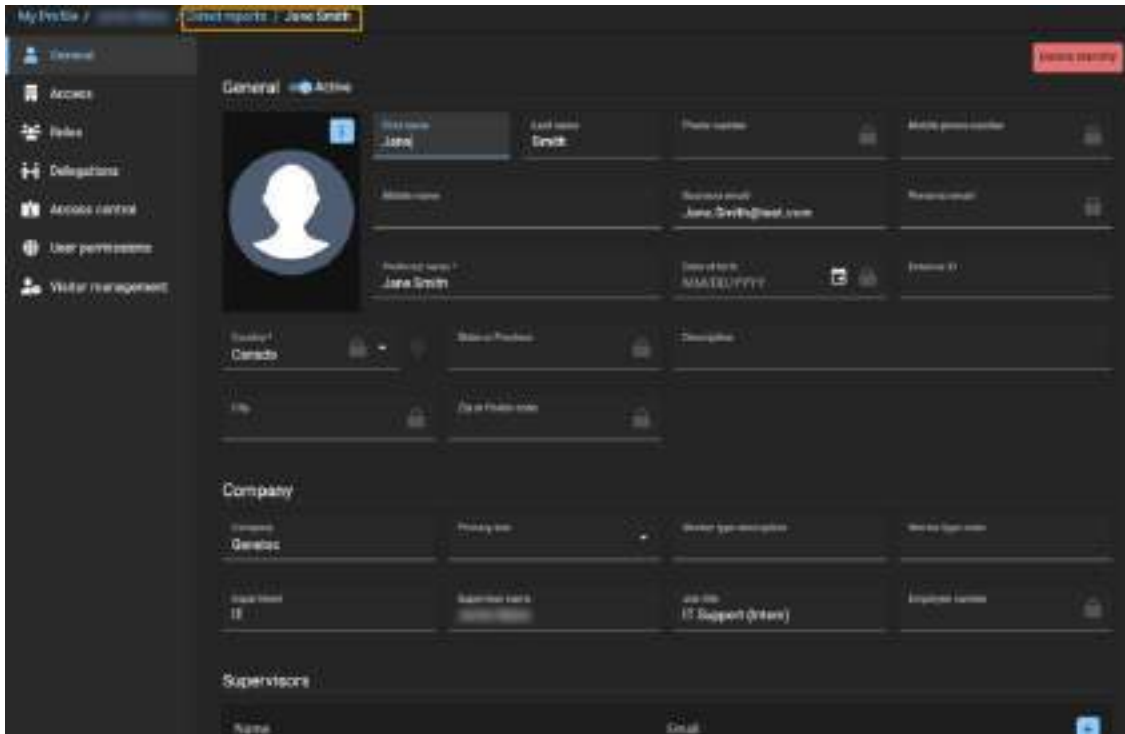
1. From the Home page, click My Profile > Direct reports.



2. In the Direct reports list, select the direct report that you want to modify.



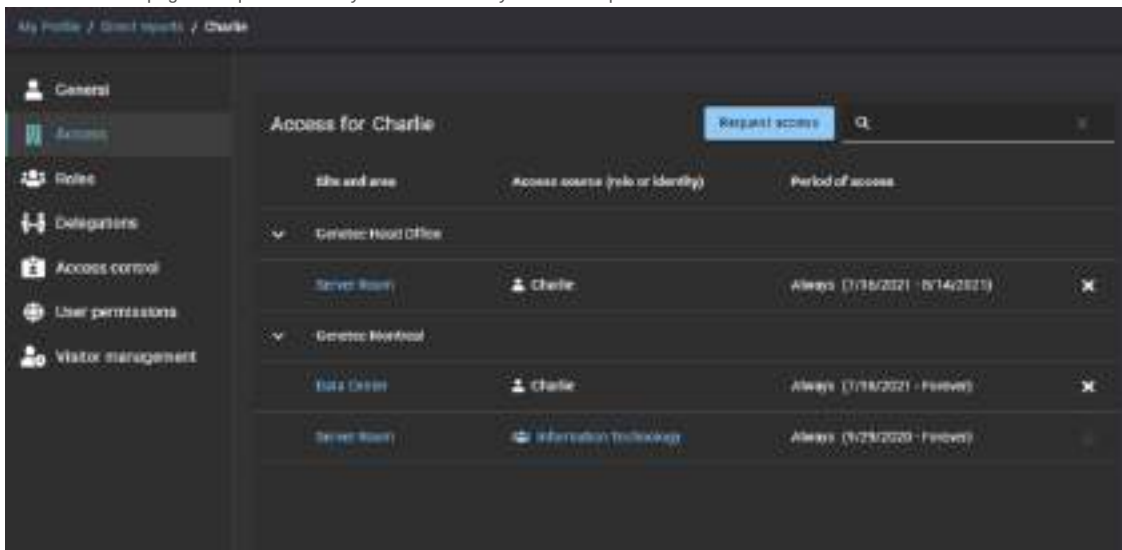
Tip: Use the filters described in [Viewing direct reports in ClearID](#) to search for and select the direct report you require.



IMPORTANT: General identity information attributes are typically synchronized from an external data source to populate the general identity information. If you make updates to identities that are synchronized with an external data source, your changes can be overwritten by the synchronization.

- A supervisor with default permissions cannot modify any of the General identity information for their direct reports.
- A supervisor with manage direct reports permission can modify the General identity information if required. This enhanced permission is typically used to manage contractors or temporary workers who are not synchronized from an external data source.

3. Click the Access page to request or modify area access for your direct report.

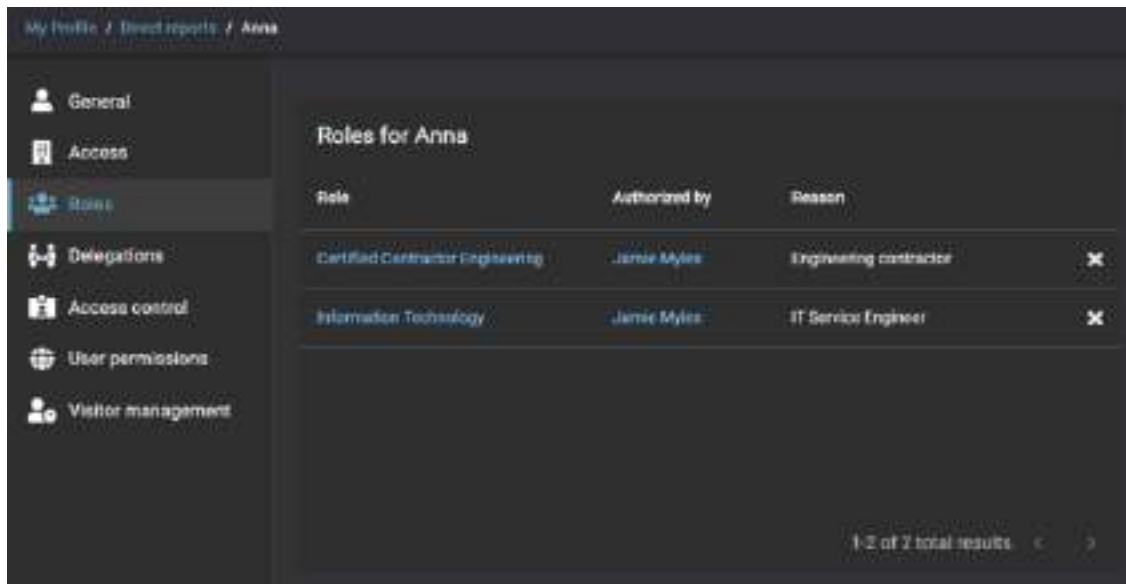


a. Click Request access to request access to one or more areas.

b. Click  to remove any area access that is no longer required and click Revoke to confirm the removal.

NOTE: You can only remove area access that was manually added. Area access that was added using a provisioning policy is identified using the locked () icon and cannot be modified.

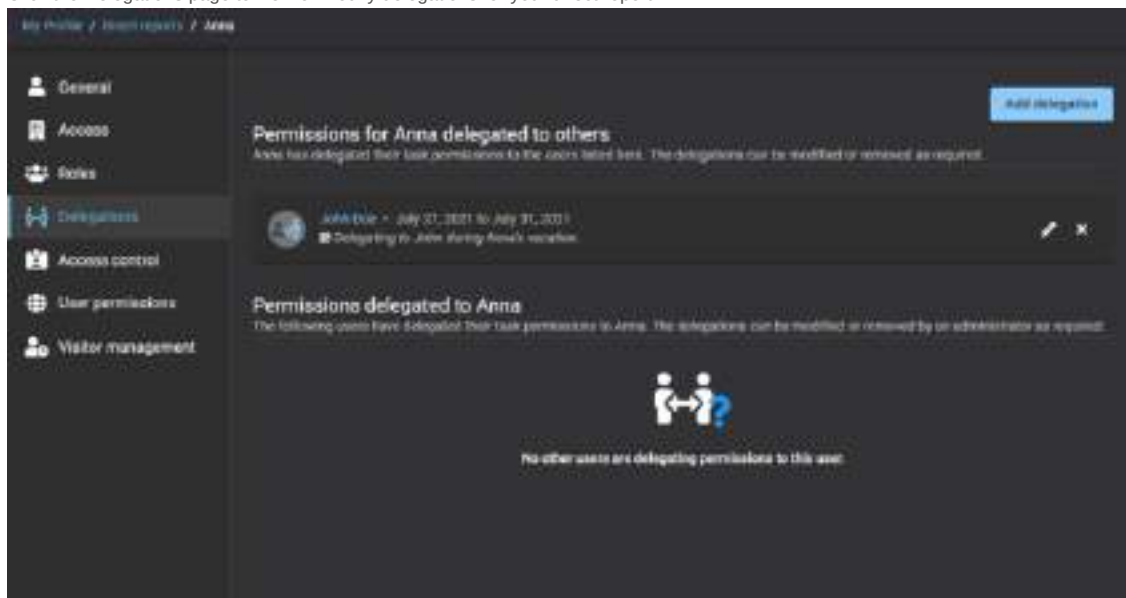
4. Click the Roles page to modify or delete role access for your direct report.



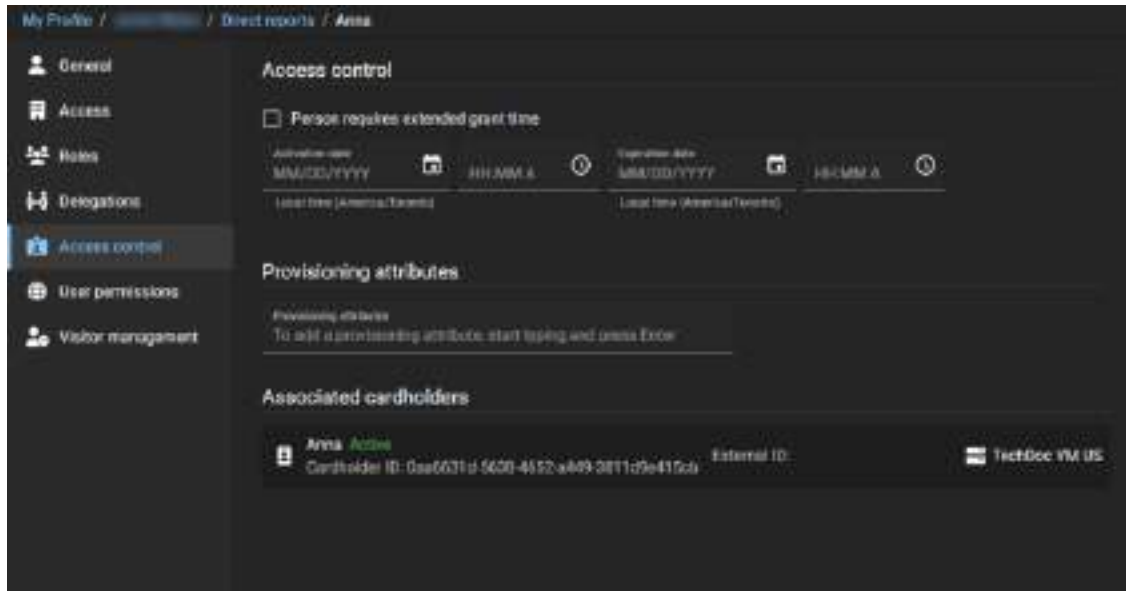
- Click a role hyperlink to view the role details.
- Click  next to a role to remove the role access that is no longer required and click Remove again to confirm.

NOTE: You can only remove roles that were manually added. Roles that were added using a provisioning policy are identified using the locked  icon and cannot be modified.

- Click the Delegations page to view or modify delegations for your direct report.

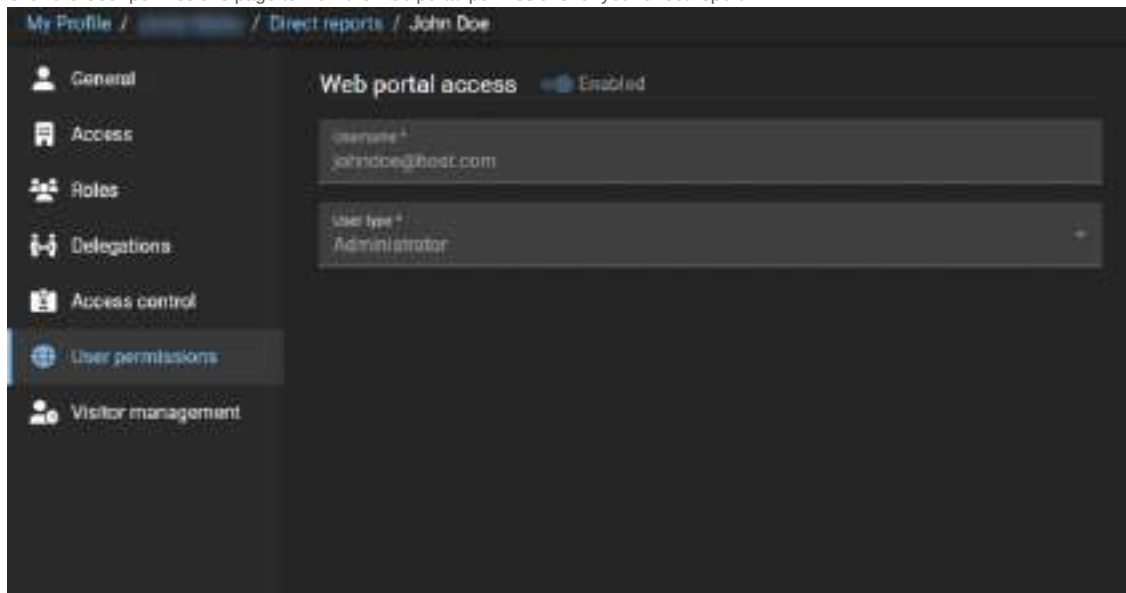


- Click Add delegation to delegate tasks to another user.
 - Click  next to a delegation to modify the settings.
 - Click  next to a delegation to remove a delegation that is no longer required.
- Click the Access control page to view the access control settings for your direct report.

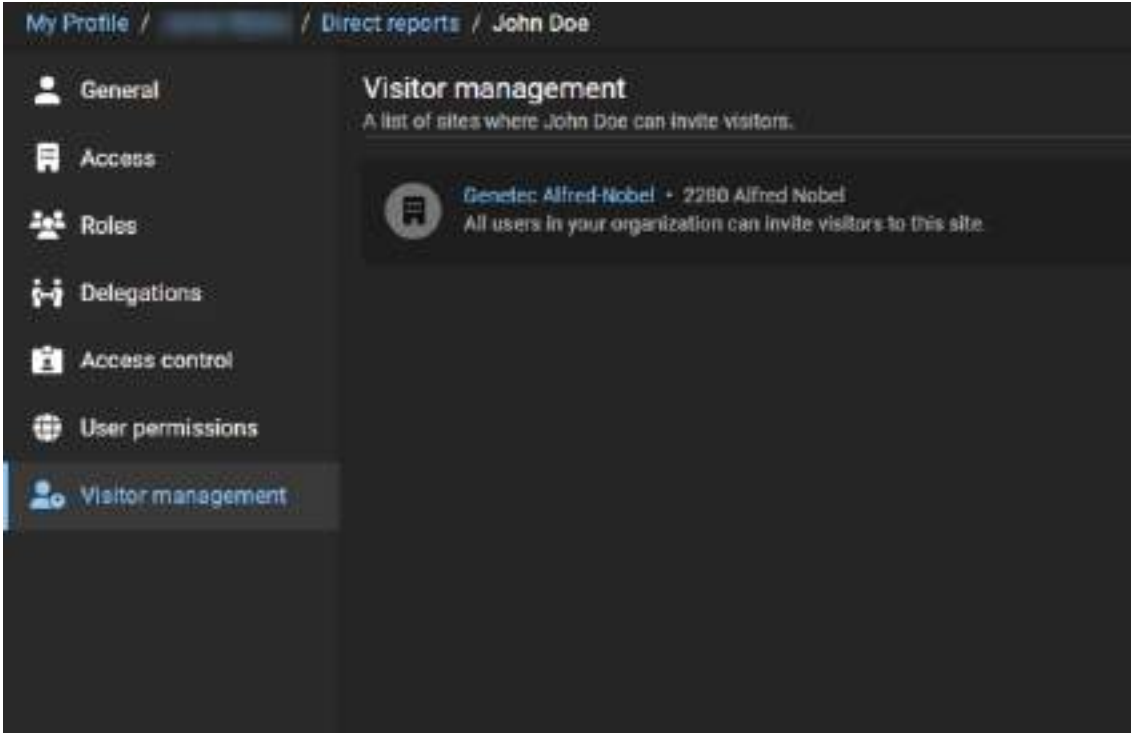


a. (Optional) A supervisor with manage direct reports permission can modify the Access control settings if required.

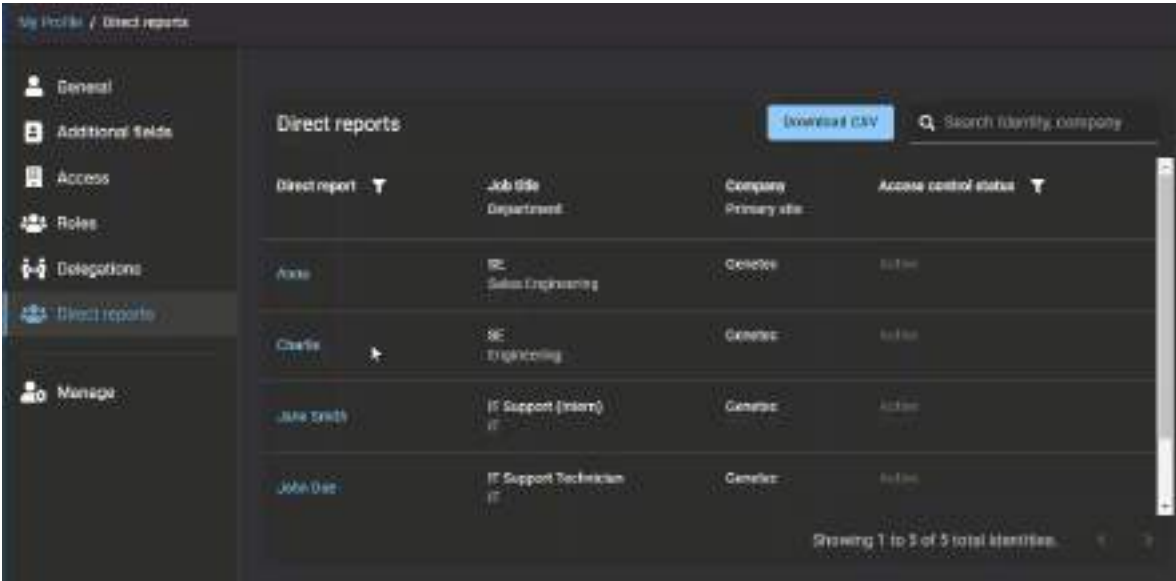
7. Click the User permissions page to view the web portal permissions for your direct report.



8. Click the Visitor management page to view the visitor management settings for your direct report.



Example



Browse

- Granting additional permissions for supervisors in ClearID

5.24 | Transferring direct reports in ClearID

From time to time a supervisor, account administrator, or an identity might need to transfer direct reports. For example, transferring direct reports to a new hire or for a change in supervisor.

Before you begin

You must have a supervisor or an identity with direct reports ready to transfer.

What you should know

To transfer *direct reports*, you must be a supervisor or an identity with elevated write permissions for identities, or an account administrator.

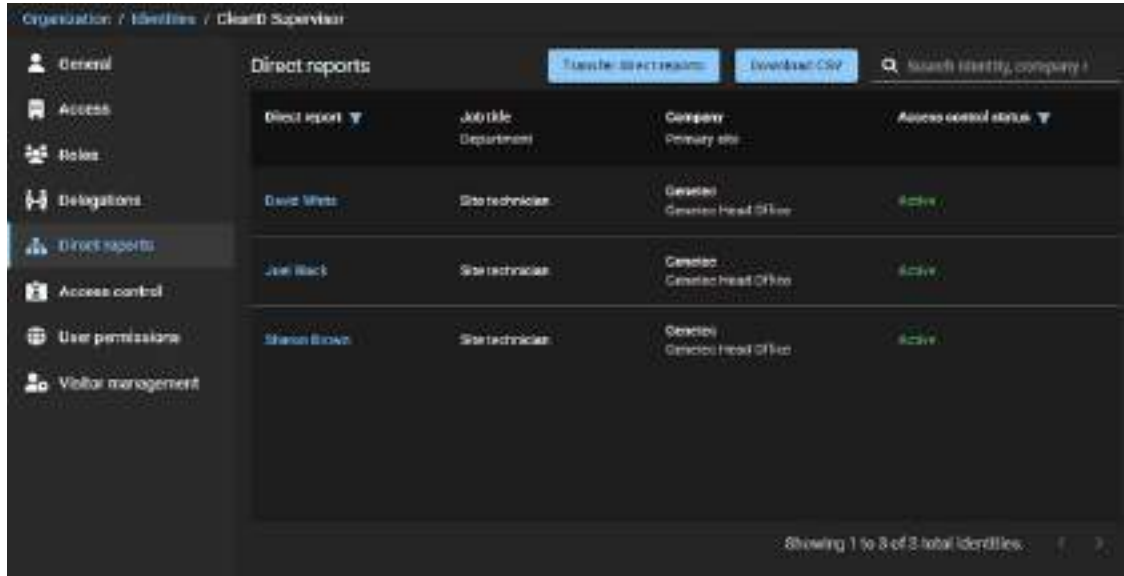
- You can transfer direct reports to another identity (regardless of their permissions).
- You can add a maximum of 20 supervisors when transferring direct reports.

IMPORTANT: This function is intended for identities that are locally managed in Genetec ClearID™. If identities are managed using an external data source, the transfer of direct reports will be overwritten.

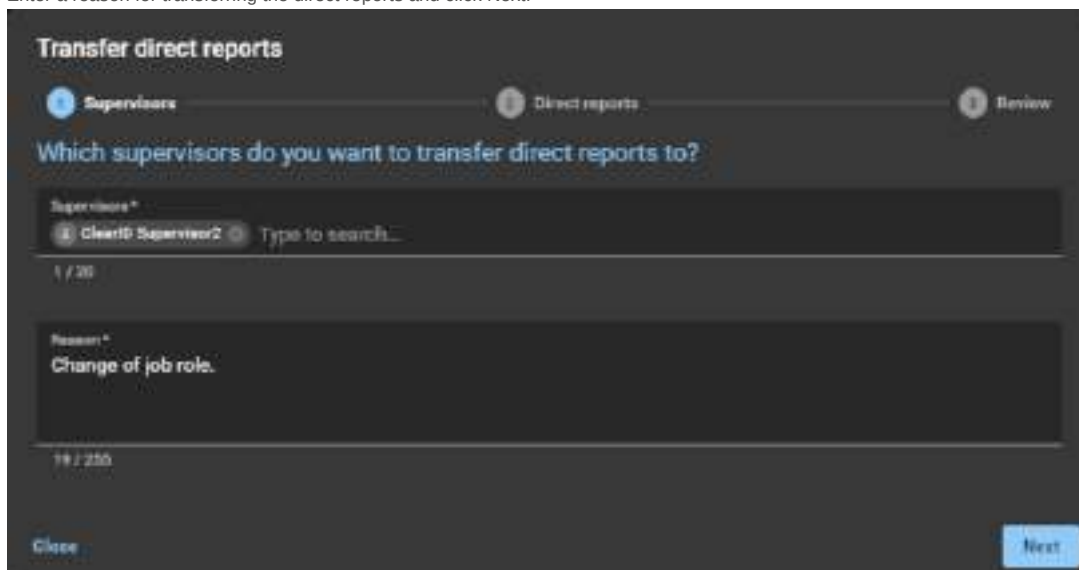
Procedure

To transfer direct reports (Performed by an account administrator or an identity):

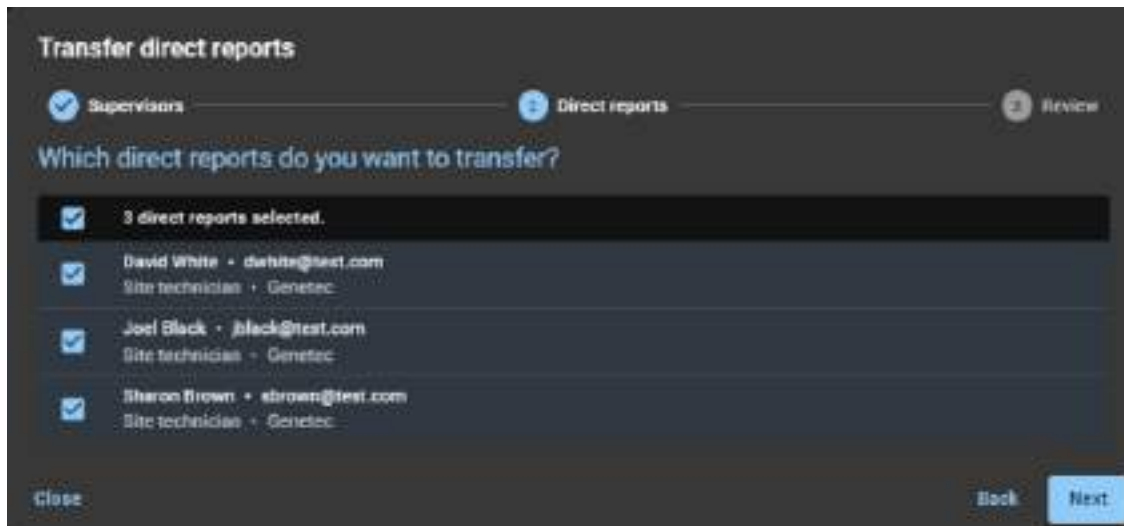
1. From the Home page, click Organization > Identities.
2. Select the identity whose direct reports you want to transfer.
3. Click Direct reports.
4. Click Transfer direct reports.



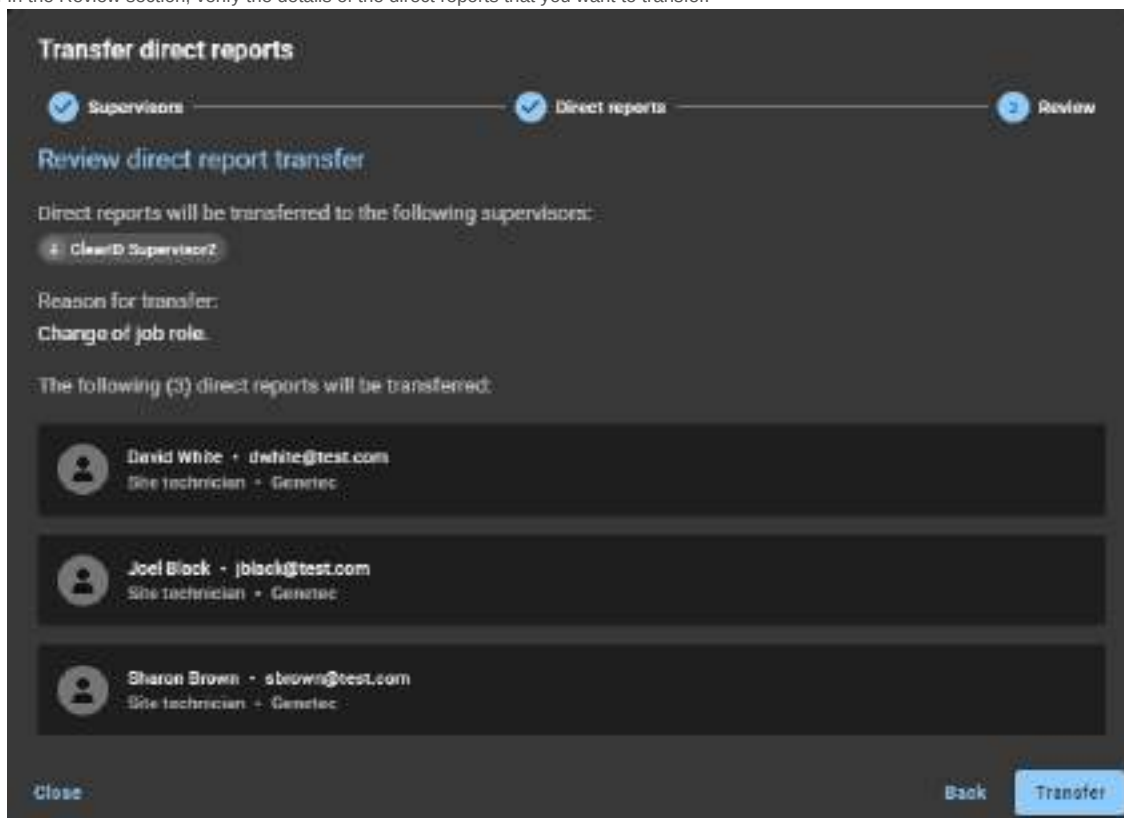
5. In the Supervisors section of the Transfer direct reports dialog, complete the fields.
 - a. Search for and select one or more supervisors.
 - b. Enter a reason for transferring the direct reports and click Next.



6. In the Direct reports section, select the direct reports you want to transfer and click Next.

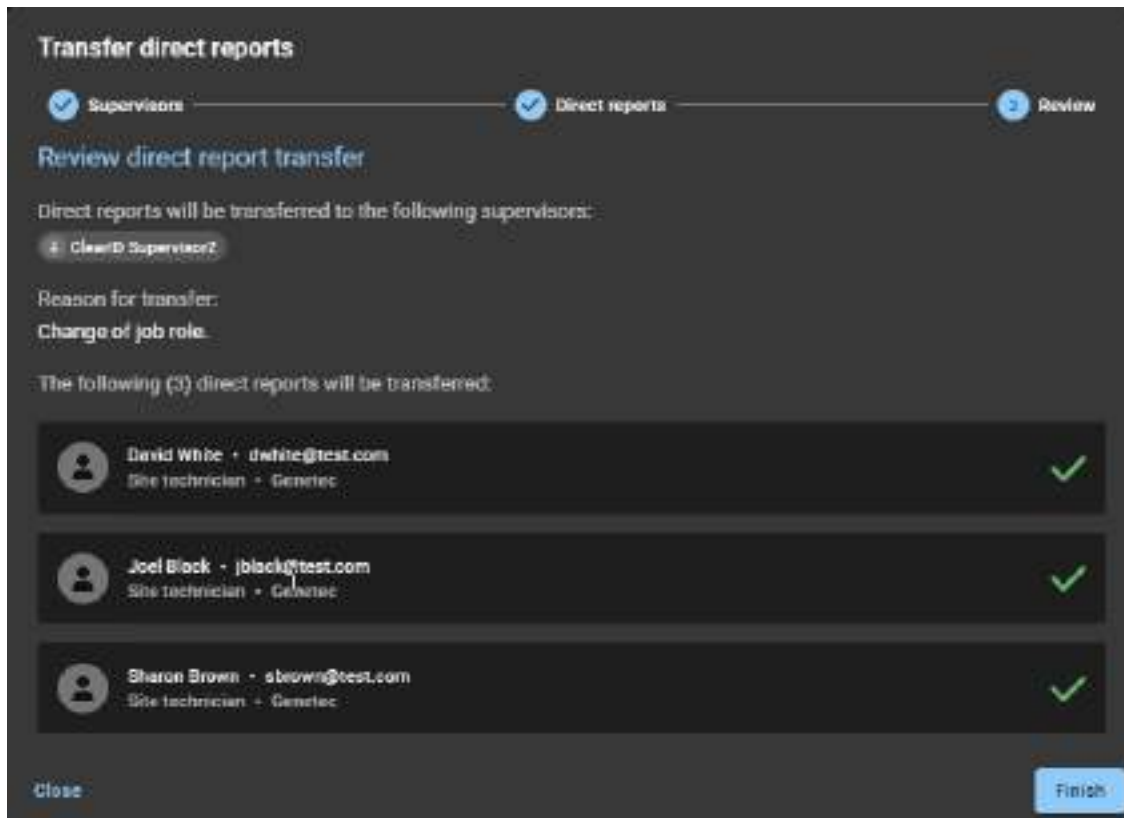


7. In the Review section, verify the details of the direct reports that you want to transfer.



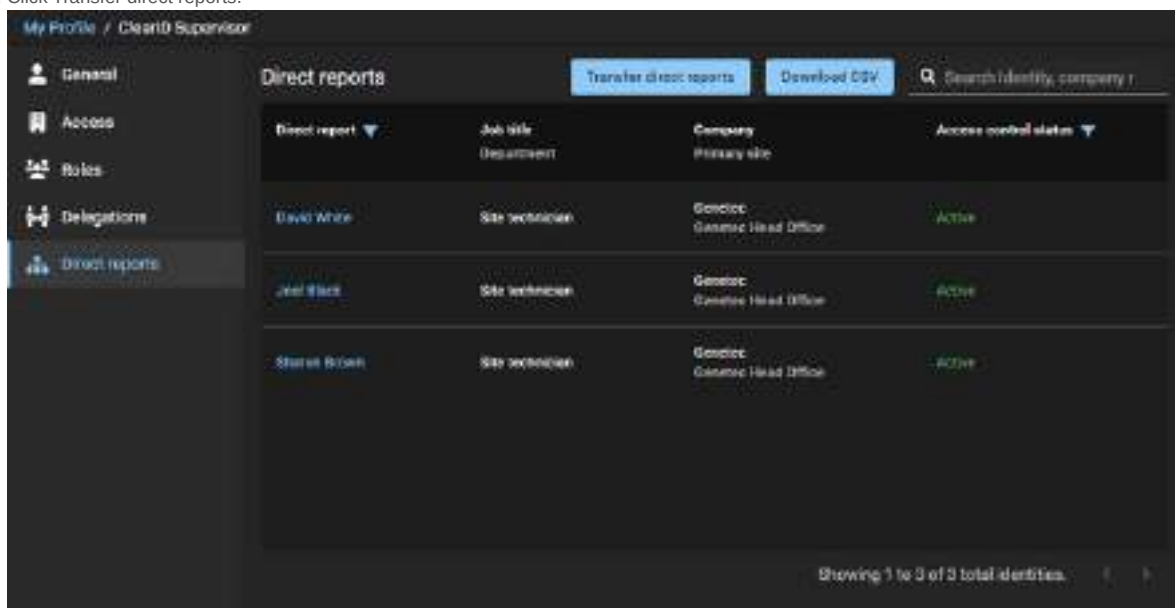
- a. (Optional) If you need to make some additions or changes, click Back to return to previous steps.
- b. If no further changes are required, click Transfer to initiate the transfer.

8. Click Finish to complete the transfer request.



To transfer direct reports (Performed by a supervisor):

1. From the Home page, click My Profile > Direct reports.
2. Click Transfer direct reports.



3. In the Supervisors section of the Transfer direct reports dialog, complete the fields.
 - a. Search for and select one or more supervisors.
 - b. Enter a reason for transferring the direct reports and click Next.

Transfer direct reports

Supervisors Direct reports Review

Which supervisors do you want to transfer direct reports to?

Supervisors *

ClearID Supervisor2 Type to search...

1 / 20

Reason *

Change of job role.

19 / 235

Close Next

4. In the Direct reports section, select the direct reports you want to transfer and click Next.

Transfer direct reports

Supervisors Direct reports Review

Which direct reports do you want to transfer?

3 direct reports selected.

David White - dwhite@test.com
Site technician - Genetec

Joel Black - jblack@test.com
Site technician - Genetec

Sharon Brown - sbrown@test.com
Site technician - Genetec

Close Back Next

5. In the Review section, verify the details of the direct reports that you want to transfer.

Transfer direct reports

Supervisors Direct reports Review

Review direct report transfer

Direct reports will be transferred to the following supervisors:

ClearID Supervisor2

Reason for transfer:

Change of job role.

The following (3) direct reports will be transferred:

David White - dwhite@test.com
Site technician - Genetec

Joel Black - jblack@test.com
Site technician - Genetec

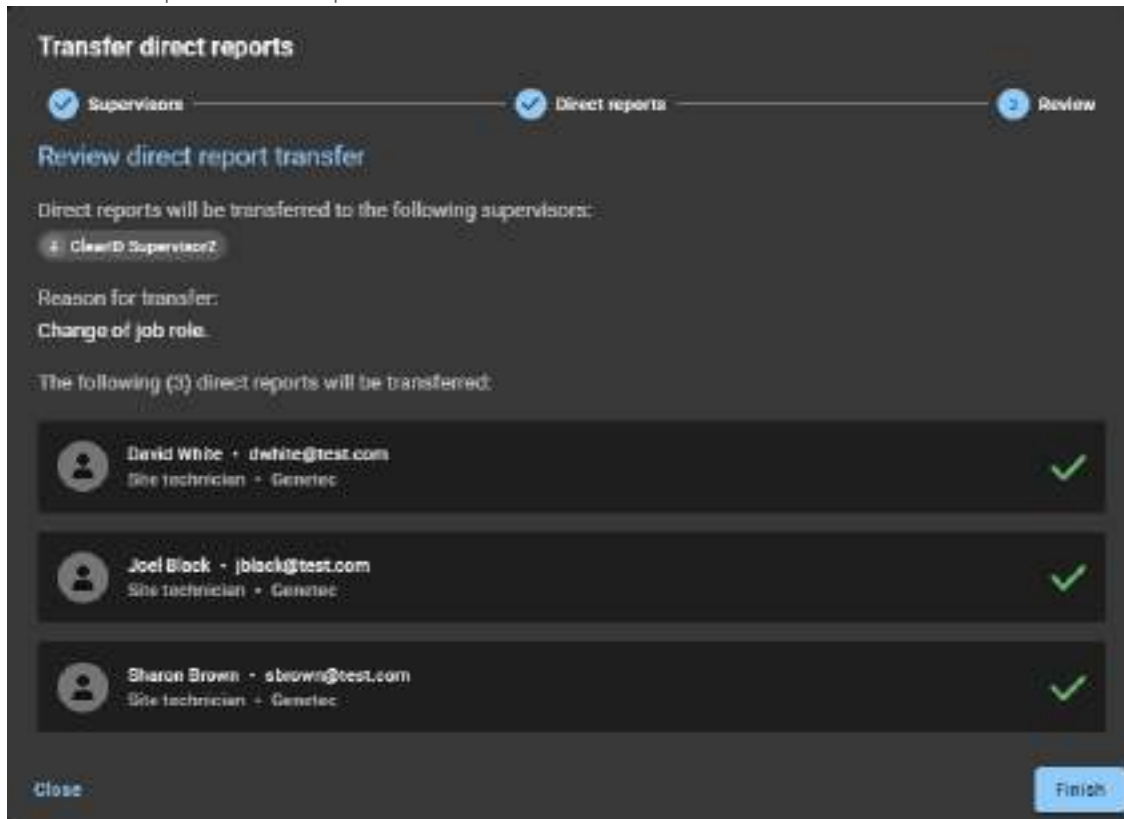
Sharon Brown - sbrown@test.com
Site technician - Genetec

Close Back Transfer

Genetec ClearID™ User Guide

Displayed in the header

- a. (Optional) If you need to make some additions or changes, click Back to return to previous steps.
 - b. If no further changes are required, click Transfer to initiate the transfer.
6. Click Finish to complete the transfer request.



Example



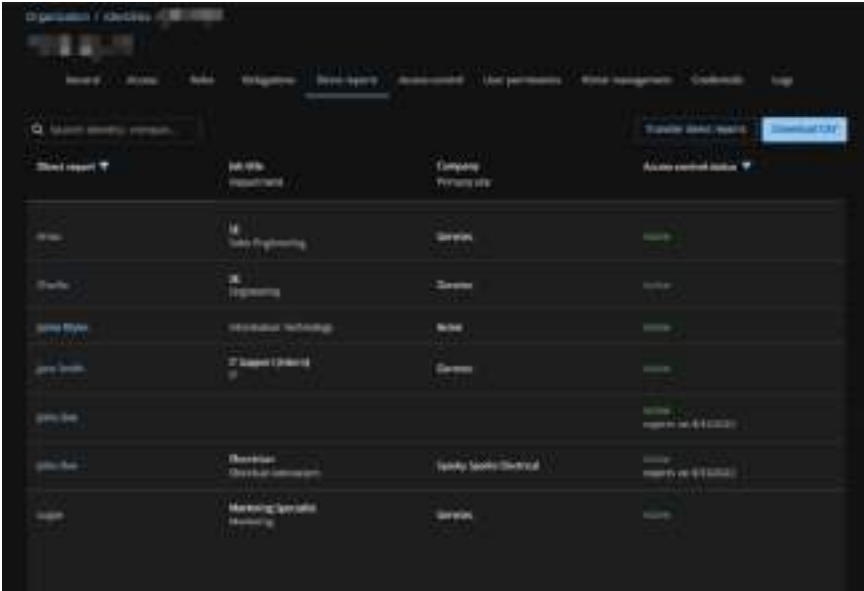
After you finish

View the new supervisors identity to check that the direct reports were transferred successfully.
Browse

- Granting additional permissions for identities and roles in ClearID
- Granting additional permissions for supervisors in ClearID

5.25 | About direct reports report in ClearID

In Genetec ClearID™, a direct reports report is a list of identities of employees that report to a supervisor. The report includes information about direct reports, delegated direct reports, job titles, companies, and access control status.



Direct reports report

The direct reports report is used by supervisors to view their direct reports to check their access control status and general identity information. The report can also be used to provide direct reports information to auditors.

Filters can be used to help refine the search results by direct reports (or delegated direct reports) and access control status (active or inactive).
Browse

- [Viewing direct reports in ClearID](#)

5.26 | Resetting user passwords in ClearID

If you're unable to authenticate while signing in to an account managed by Genetec ClearID™, you can reset your password.

What you should know

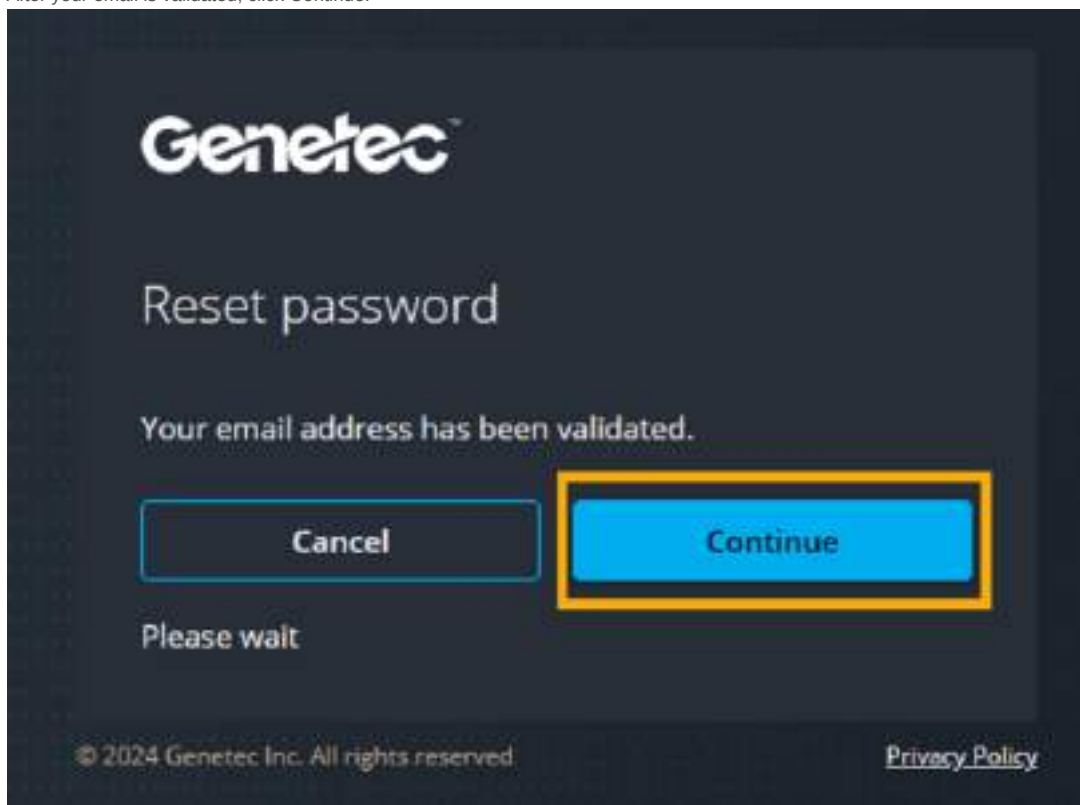
Password reset is only available for users with accounts managed by ClearID. Use industry best practices for creating strong passwords.
NOTE: This procedure isn't applicable to corporate single sign-on.

Procedure

1. In a web browser, do one of the following:
 - If you have a production account, go to <https://portal.clearid.io>.
 - If you have a demo or test account, go to <https://demo.clearid.io>.
2. Enter your email address and click Sign in.
You're redirected to the new Genetec™ sign in page.



3. Click Forgot password?.
You're redirected to the Reset password page.
4. On the Reset password page, click Send code to receive an email with a verification code.
 - a. Enter the verification code in the Verification code field on the Reset password page.
 - b. Click Verify code.
 - c. After your email is validated, click Continue.



5. Enter and confirm your new password, then click Continue.

Results

You can now access ClearID using the password you created.

5.27 | About email notifications in ClearID

Genetec ClearID™ sends email notifications to inform users about specific system events related to access, identities, roles, and visits.

Email notifications are sent from noreply@clearid.io. If you don't receive email notifications in either your Inbox or Spam (Junk) folders, contact your *account administrator*.

To opt out of or resubscribe to email notifications, see [Configuring your ClearID email notification preferences](#)

The following events can trigger email notifications:

Trigger event for notification	Possible notification recipients
Activity Summary	
Weekly activity summary NOTE: - The weekly activity summary summarizes all pending tasks or requests related to visit events, identity requests, or area access requests that require approval. You don't receive these notifications if you have no tasks or requests. - Weekly activity summary emails are sent every Monday at 9:00 am based on the identity's primary site. If no primary site is set, the email is sent at 9:00 am GMT.	- Requesters - Visit approvers - Supervisors - Identity approvers - Area owners - Area managers - Role managers
Access for an identity	
Account is created for an identity IMPORTANT: If a corporate log on (single sign-on using Microsoft Office 365 or similar) is used, the account is automatically activated and no activation email is received.	- Identity - Account administrators
Area access request for an identity is submitted	Identity requester
Area access request for an identity is canceled	- Identity requester - Area managers - Area owners
Area access request for an identity requires approval or denial Tip: - No email is sent if the request is auto-approved. - The email recipient depends on the system's workflow settings.	- Supervisors - Area managers
Area access request for an identity is approved or denied NOTE: If the person who submits an access request and the identity the access request is for are different, both receive the email.	- Identity - Area owners
Area access for an identity is granted	- Identity - Identity supervisors
Area access for an identity is revoked (or expired) NOTE: Access expired emails are sent at midnight based on the time zone specified for the site.	- Identity - Identity supervisors
Access for a role	
Access request submitted for a role NOTE: Both <i>role owners</i> and <i>role managers</i> can request access for roles. The user who made the request receives the email.	- Role managers - Role owners
Area access request for a role requires approval or denial	- Supervisors - Area managers
Area access request for a role is approved or denied	Approved:

Genetec ClearID®; User Guide

Displayed in the header

Trigger event for notification	Possible notification recipients
NOTE: <i>Supervisors</i> or <i>area managers</i> must approve or deny the request.	• <i>Area managers</i> Denied: • <i>All Role managers</i>
Area access granted for role NOTE: <i>Area managers</i> can approve area access requests for roles, or the requests can be auto-approved. A role can also be manually granted access to an area.	• <i>All Role managers</i>
Area access revoked for a role	• <i>All Role managers</i>
Identity added to role membership	• Identity
Identity removed from role membership	• Identity
Identity requests	
Identity requested NOTE: If one of the requested identities is canceled, all configured approvers are added to the Cc list of the identity request approval and completion email. The subject of the email is: "Identity request for <i>identity</i> has been updated".	• Requester • <i>Supervisors</i> (if configured in the identity template) • <i>Identity approvers</i> (if configured in the identity template)
Visit events	
Visit created	• Requester • Hosts
Visit requires approval or denial NOTE: No email is sent if the request is auto-approved.	• <i>Supervisors</i>
Visit approved or denied	• Requester • Hosts
Visitor confirmation	• Visitor
Visit request requires approval or denial NOTE: No email is sent if the visit is auto-approved.	• <i>Area managers</i> (depending on workflow) • <i>Visit approvers</i> (depending on workflow)
Visitor checked-in	• Hosts
Visitor watchlist alert (notify or block)	• <i>Watchlist managers</i>
Access reviews	
Access review pending	• <i>Area managers</i> • <i>Role managers</i>

Browse

- [Configuring your ClearID email notification preferences](#)
- [Configuring email notification preferences in ClearID \(administrator\)](#)

5.27.1 | Customizing the email banner for sites in ClearID

You can customize the email banner image that is used for access requests and visitor requests email notifications sent for the site.

Before you begin

Configuring the ClearID Self-Service Kiosk iPad

Tip: Ensure that your email banner image meets the requirements described in the  tooltip on the Images page of the Genetec ClearID™ web portal.

What you should know

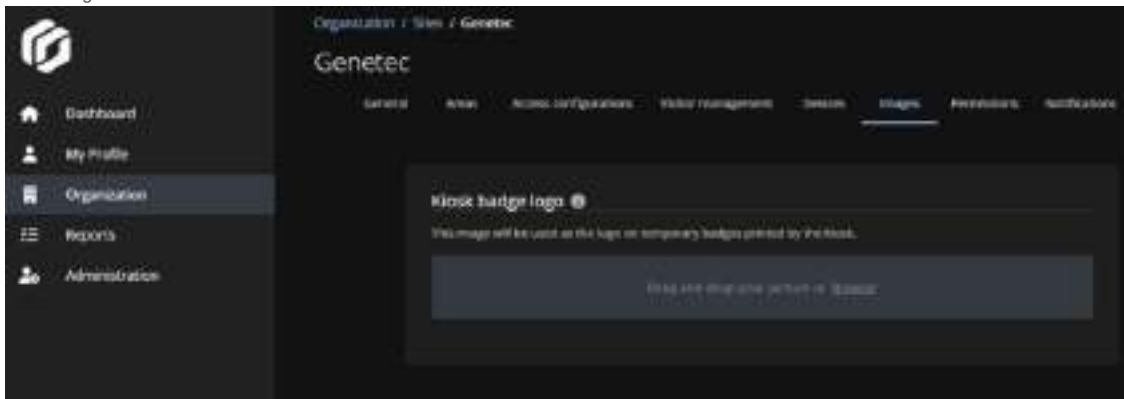
Only a site owner or account administrator can customize email banners.

- Customized email banner changes are synchronized with your site every 60 seconds.

Best Practice: For optimum results, use transparent .PNG images when customizing your email banner.

Procedure

- In the ClearID web portal, click Organization > Sites.
- Search for and select a site.
- Click Images.



- In the Email banner section, drag and drop your picture or browse to select the Email banner image.
- Click Save.

The following example shows an email banner with a custom image.



Parent topic: About email notifications in ClearID

5.27.2 | Configuring email notification preferences in ClearID (administrator)

Genetec ClearID™ portal users receive email notifications for visit requests, access requests, activity summaries, and more. *Account administrators* can decide which notifications users receive by default and whether users can opt out of email notifications.

What you should know

Only *Account administrators* can configure which email notifications are sent out and which stakeholders receive them, where applicable.

Procedure

1. In the ClearID portal, click Administration > Notifications.
2. In the Emails and recipients section, configure your preferences as needed:

Enabled

Turn on the Enabled option to send an email notification to users by default.

Can opt out

Turn on the Can opt out option to allow users to opt out of a notification in their personal email notification preferences.

NOTE: You can only allow users to opt out of a notification type if the Enabled option for that notification is turned on.

3. Where applicable, choose which stakeholders receive the notification email.



4. Click Save.

Parent topic: [About email notifications in ClearID](#)

Browse

- [About email notifications in ClearID](#)

5.27.3 | Configuring your ClearID email notification preferences

You receive email notifications for visit requests, access requests, various activity summaries, and more from Genetec ClearID™. You can decide which notifications you want to receive and configure your notification preferences accordingly.

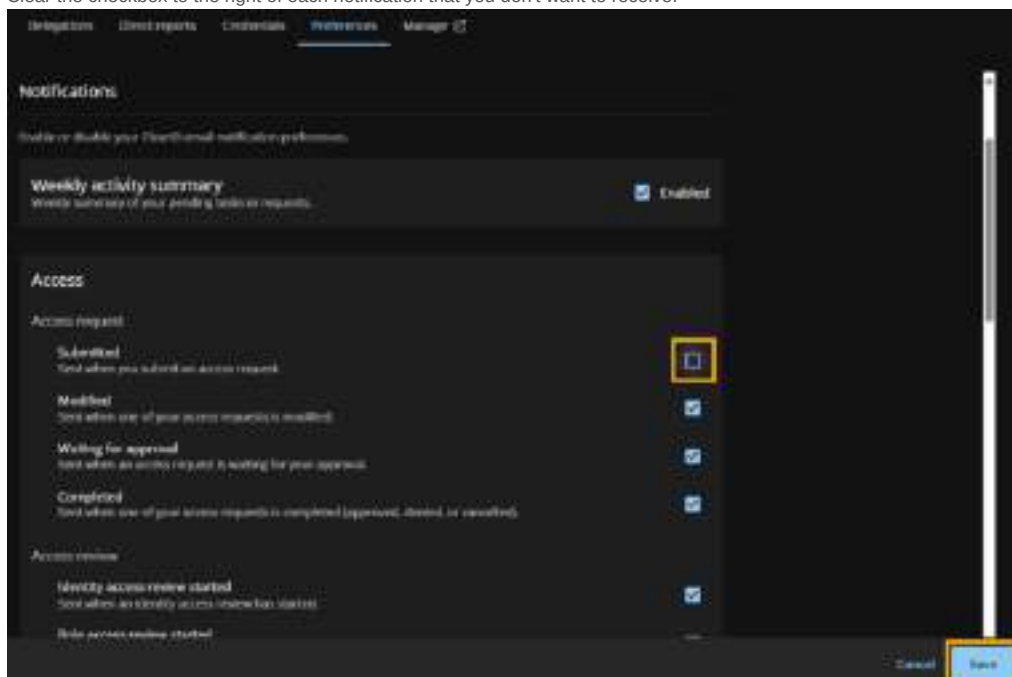
What you should know

Your notification preferences only apply to your user profile. All email notifications are turned on by default.

Tip: Use the Weekly activity summary email to keep track of your pending tasks and requests.

Procedure

1. In the ClearID web portal, click My Profile > Preferences.
2. In the Notifications section, configure your notification preferences as needed.
 - a. Clear the checkbox to the right of each notification that you don't want to receive.



3. Click Save.

Parent topic: [About email notifications in ClearID](#)
[Browse](#)

- [About email notifications in ClearID](#)

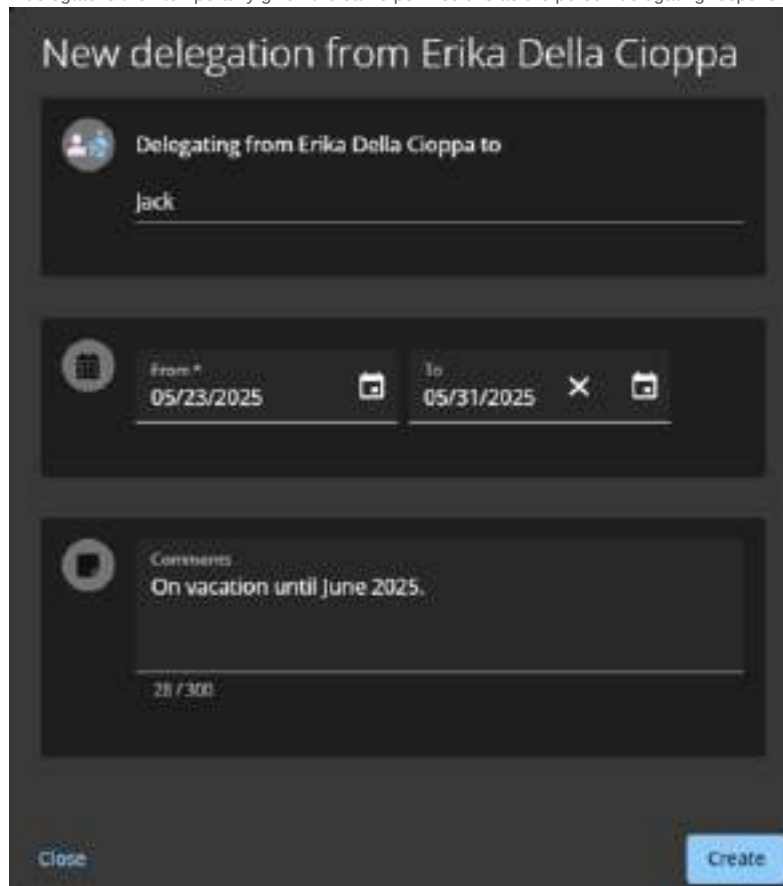
5.28 | About delegation in ClearID

In Genetec ClearID™, delegation is the process of transferring Genetec ClearID™ tasks within your organization, for example, due to a vacation or sabbatical. Tasks may be transferred among site owners, area owners, area managers, role owners, role managers, supervisors, and visit event approvers.

Planned delegation

In this situation, the delegation requirement is known about in advance and is planned for by the permission owner. For example, a planned vacation, sabbatical, or maternity leave.

A delegate is then temporarily given the same permissions as the person delegating responsibility so that they can manage the delegated tasks.



For example, if an area manager delegates to you, you are temporarily given permissions to perform that area manager's tasks. The delegated tasks are then displayed in the My tasks section of your Dashboard.

Permissions for *user* delegated to others

- If required, you can delegate to more than one person. This can be useful when tasks are performed by multiple people. For example, different supervisors or shift workers.
- You cannot delegate tasks that have been delegated to you because this would potentially create a trust conflict. When you create a delegation you are only delegating your own tasks.
- The delegation period can be modified (✎) or turned off (✖) early if your delegation requirements change.



Permissions delegated to user

Permissions can also be delegated to you from another person.

NOTE: You cannot delegate permissions to a user that is already delegating to you. In this situation, the following error message is displayed: The specified user is already delegating permissions to you. That delegation must be removed before you can delegate to them.

Unplanned delegation

From time to time, an unplanned delegation might be required because the delegator is not available to set the delegation. For example, in the event of an unplanned absence or period of unavailability. In this situation, an account administrator can perform a delegation on behalf of an unavailable delegator. The account administrator can also modify or remove a delegation if required.

IMPORTANT: Administrator permissions cannot be delegated. You can only assign administrator permissions through the normal official channels.

Delegation email notifications

Any email notifications associated with delegated tasks are sent to both the original permission owner and the delegate. Using these email notifications or the My tasks page, the delegate can access and perform the delegated tasks.

Email notifications sent to delegates include contact details in the email notifications footer so that the delegate can contact the permission owner if they want to request changes to the delegation configuration.



5.29 | Delegating ClearID tasks to another user

Site owners, area owners, area managers, role owners, role managers, supervisors, and visit event approvers can temporarily transfer their Genetec ClearID™ task responsibilities to someone else in their organization by delegating their tasks to another user. For example, during a planned vacation, sabbatical, and so on.

Before you begin

[Learn about delegation.](#)

Best Practice: Before delegating your tasks, consider contacting the potential delegate to make them aware of the delegation and confirm their availability.

What you should know

- Only the logged in user can delegate their ClearID tasks to one or more users.
- The delegation period can be modified (📅) or turned off (❌) early if your delegation requirements change.
- An account administrator can also perform an unplanned delegation on the behalf of an unavailable delegator. For example, in the event of an unplanned absence or period of unavailability.

IMPORTANT: Administrator permissions cannot be delegated. You can only assign administrator permissions through the normal official channels.

Procedure

1. From the Dashboard, click My Profile > Delegations.
2. Click Add delegation.
3. Complete the fields

New delegation from Erika Della Cioppa

Delegating from Erika Della Cioppa to

Search for a name...

From * 05/23/2025 To MM/DD/YYYY

Comments

0 / 300

Close Create

- a. Search for or enter the name of the user that you want to delegate your ClearID tasks to.
- b. Enter the From and To dates for the period of time that you want the delegation in place.
- c. In the Comments field, add an explanation about why your tasks are being delegated to other users.

New delegation from Erika Della Cioppa

Delegating from Erika Della Cioppa to

Jack

From * 05/23/2025 To 05/31/2025 X

Comments

On vacation until June 2025.

28 / 300

Close Create

4. Click Create.



5. (Optional) In the Permissions for *user name* delegated to others section, click  to modify an active delegation.

- Enter the From and To dates for the period of time that you want the delegation in place.
- In the Comments field, add an explanation about why your tasks are being delegated to other users.
- Click Update to save your changes.

Your delegation is now active and will automatically expire on the date specified.

6. (Optional) Click  to remove a delegation.

- In the Remove delegation dialog, click Remove to confirm the delegation is no longer required.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.



5.30 | About user activity report in ClearID

In Genetec ClearID™, a user activity report is an audit trail of all activities related to users. The report includes timestamp information, activity type, who activity was performed by, and a details section including reason information.

User activity report

As an account administrator, you can use this report to view all data corresponding to the following activities:

- Area owner added or removed
- Area manager added or removed
- Identity access granted or removed
- Role access granted or removed
- Role owner added or removed
- Role manager added or removed
- Role member added or removed
- Supervisor added or removed
- Identity created, updated, or deleted
- Custom field created, updated, or deleted
- Custom field section created, updated, or deleted

You can use filters to help refine the report search results by timestamp, activity type, performed by, and details.

Browse

- [Viewing a user activity report in ClearID](#)

5.31 | Viewing a user activity report in ClearID

You can consult the User activity report to review all user-related activities. Use the report for auditing purposes, download a copy to attach to an audit request to review offline, or manipulate or consolidate data in a spreadsheet for other audiences.

Before you begin

To view the User activity report and review audit trail information, ensure that you're an account administrator.

NOTE: The User activity report is empty if there is no activity logged by area owners or managers, role managers, or role members in your Genetec ClearID™ system.

Procedure

1. From the Home page, click Reports > User activity.

Timestamp	Activity type	Performed by	Details
April 2, 2021 at 11:52 AM	Area manager added	Mike Della Cappa	Mike Della Cappa added as area approver for Main Entrance.
April 2, 2021 at 11:51 AM	Area owner added	jack	Mike Della Cappa added as area owner for Main Entrance.
April 2, 2021 at 11:51 AM	Area manager removed	jack	Mike Della Cappa removed as area approver from Main Entrance.
April 2, 2021 at 11:50 AM	Role member added	Mike Della Cappa	Mike Della Cappa added to role Identity Requests. Identity Requests role approver Identity Requests.
April 2, 2021 at 11:51 AM	Role member added	Mike Della Cappa	Mike Della Cappa added to role Customer managers. Manager: Mike Della Cappa (operator manager).
April 2, 2021 at 11:51 AM	Role member added	Mike Della Cappa	Mike Della Cappa added to role Defined...

2. In the User activity report tab, select the display time setting that you require.

Display time in local

Report times are displayed using the system time from the computer of the logged-in user.

Display time in UTC

Report times are displayed using Coordinated Universal Time (UTC).

3. Filter the report based on your required criteria:

Timestamp

In the Timestamp column, click  to filter the results by date. Select a pre-defined date range from the choices available or enter a specific date range using the date range picker.

(Optional) Use the sort icons ( and ) to display the results in descending or ascending order.

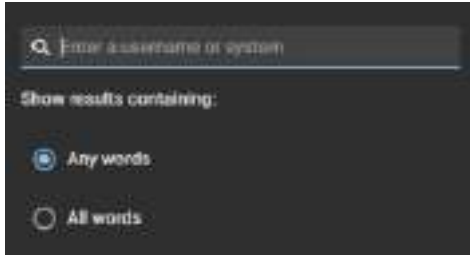
Activity type

In the Activity type column, click  to filter the results by activity type:

- o Area owner added or removed
- o Area manager added or removed
- o Identity access granted or removed
- o Role access granted or removed
- o Role owner added or removed
- o Role manager added or removed
- o Role member added or removed
- o Supervisor added or removed
- o Identity created, updated, or deleted
- o Custom field created, updated, or deleted
- o Custom field section created, updated, or deleted

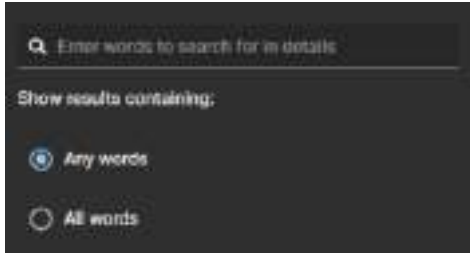
Performed by

In the Performed by column, click  to open a search dialog and filter the results by who performed an activity. For example, search for tasks performed by a particular user, or tasks performed automatically by the system.



Details

In the Details column, click  to open a search dialog to search the details or reason using a search criteria.



(Optional)

Click  to reset filter selections.

- Click Download CSV to download a copy of the User activity report.

Follow your browser prompts to complete downloading the exported file.

The file is exported as a .CSV file to the default download location for your browser. By default the exported file is created using the report name and download date. For example, UserActivities_2022-02-14.csv.

NOTE: The columns and entries in the CSV file can vary depending on the filters you selected when you downloaded the report.

Browse

- About user activity report in ClearID

5.32 | User levels in ClearID

The following information can be used to help you understand which actions the users or roles in Genetec ClearID™ can perform.

Identity management

Actions	Account owners (and API key)	Site owners	Area owners	Area managers	Identity supervisors	Authenticated users
Create identities	✓ ¹					
Update identities	✓ ¹					
View private information about identities	✓ ¹					
List identities when adding to an area or role	✓ ¹	✓	✓	✓	✓	✓
Create sites	✓ ¹					
Delete identities	✓ ¹					

Genetec ClearID™ User Guide

Displayed in the header

Actions	Account owners (and API key)	Site owners	Area owners	Area managers	Identity supervisors	Authenticated users
View direct reports	✓ ¹				✓	
Manage direct reports	✓ ¹				✓	
Transfer direct reports	✓ ¹				✓	

¹ Users assigned as a delegate for another user do not inherit the permission.

Area management

Actions	Account owners (and API key)	Site owners	Area owners	Area managers	Identity supervisors	Authenticated users
Create and delete sites	✓ ¹					
Edit site details	✓ ¹	✓				
Assign site owners	✓ ¹	✓ ¹				
Create and delete areas	✓ ¹	✓				
Edit area automatic provisioning attributes	✓ ¹	✓				
Edit area name	✓ ¹	✓				
View all private areas of a site	✓ ¹	✓				
Assign area owners	✓ ¹	✓				
Assign area managers	✓ ¹	✓	✓ ¹			
Edit area visibility (Public or Private)	✓ ¹	✓	✓			
Edit approval workflow	✓ ¹	✓	✓			
Edit area schedules	✓ ¹		✓			
View area configuration and access list	✓ ¹	✓	✓	✓		
Add people or roles to areas	✓ ¹		✓	✓		
Remove people or	✓ ¹		✓	✓		

Actions	Account owners (and API key)	Site owners	Area owners	Area managers	Identity supervisors	Authenticated users
roles from areas						
Approve access request for an area	✓ ¹			✓	✓	
Edit period and schedule before approving access request	✓ ¹			✓	✓	
Schedule area access reviews	✓	✓				
Receive and complete area access reviews	✓ ¹	✓	✓	✓		
View area access reviews report	✓	✓				

¹ Users assigned as a delegate for another user do not inherit the permission.

Role management

Actions	Account owners (and API key)	Site owners	Role owners	Role managers	Identity Supervisor	Any user on account
Create and delete roles	✓ ¹					
Assign role owners	✓ ¹					
Assign role managers	✓ ¹		✓ ¹			
Change automatic provisioning rules and configuration for a role	✓ ¹		✓			
Edit role name, description, notes	✓ ¹		✓			
List roles when adding to an area or access request	✓ ¹		✓	✓		
Manually add or remove a person from a role	✓ ¹		✓	✓		

Genetec ClearID®; User Guide

Displayed in the header

Actions	Account owners (and API key)	Site owners	Role owners	Role managers	Identity Supervisor	Any user on account
Submit an access request on behalf of a role			✓	✓		
Receive and complete role access reviews			✓	✓		
Remove identities from a role	✓ ¹		✓	✓		

¹ Users assigned as a delegate for another user do not inherit the permission.

Visitor management

Actions	Account owners (and API key)	Visit requester	Requester supervisor	Site owners	Visit hosts	Area managers
Visit event						
Create a visit event		✓ ¹				
Add guests to an event or remove guests from an event		✓ ¹			✓ ¹	
Approve or reject a visit event			✓			
Approve or reject specific guest access to an area						✓
Create an event (copy event) from an existing event		✓ ¹	✓		✓ ¹	
Cancel event		✓ ¹			✓ ¹	
View list of upcoming events		✓ ¹			✓ ¹	
View event details		✓ ¹	✓		✓ ¹	✓
Visitor management configuration						
Edit visitor management configuration (Area)	✓ ¹			✓		
Edit visitor management configuration (Site)	✓ ¹			✓		

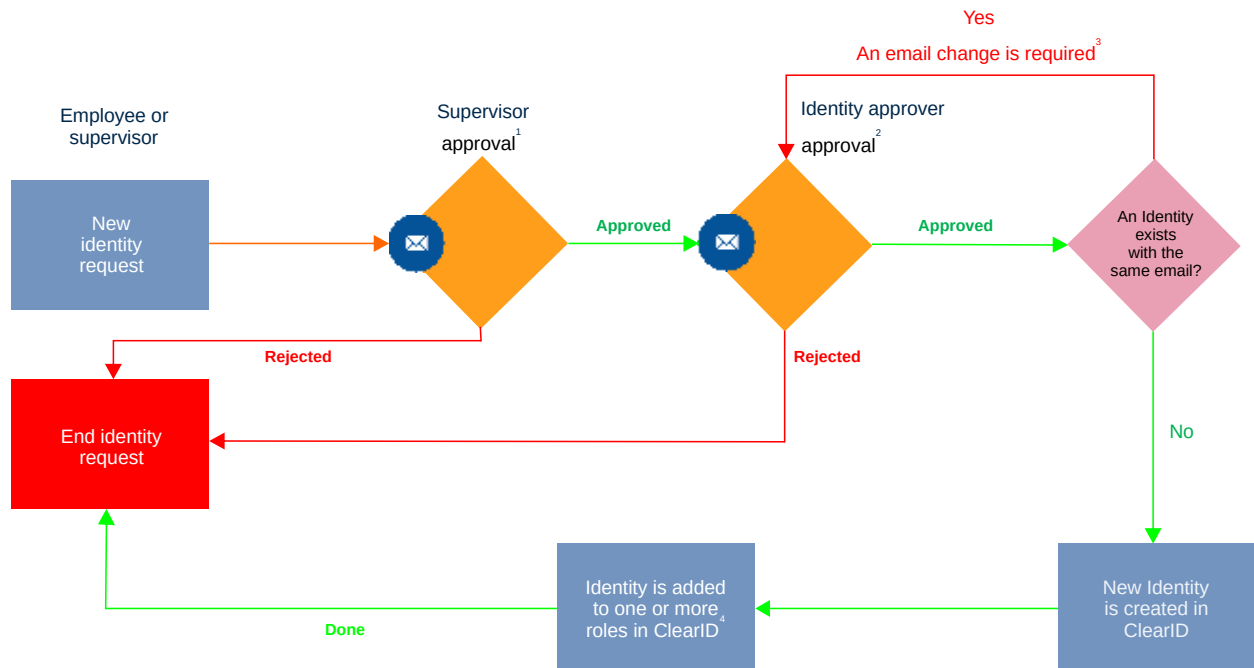
¹ Users assigned as a delegate for another user do not inherit the permission.

5.33 | About identity request workflow in ClearID

An identity request workflow is a series of activities performed by the system or authorized people during the life cycle of an identity request. The activities can create an individual identity, or multiple identities using a CSV import, and add each new identity to a role to inherit relevant access for a specified period.

The workflow helps automate identity request tasks, such as approving or rejecting identity requests, so that people involved in the review and approval process can focus on other tasks.

The following diagram illustrates the *identity request workflow* that occurs in Genetec ClearID™ and Synergis™.



¹ (Optional) Supervisor approval can be enabled and disabled for each identity template.

² (Optional) Identity approver approval can be enabled and disabled for each identity template.

³ (Optional) Email address must be unique in the system.

⁴ (Only if applicable) Cardholder is added to corresponding cardholder group in Security Center.

Browse

- [About workflows in ClearID](#)

Browse

- [Identity Request Feature Note \(2 pages\)](#)

5.34 | Creating an identity template in ClearID

Before you can submit an identity request, you must create your identity templates.

Before you begin

- Familiarize yourself with workflows.
- Create the roles that will be allowed to request identities.
- (Optional) Create roles containing the role access your identity templates will use.
- (Optional) If you want to use Supervisor approvals, add a supervisor for each identity that can request an identity.

What you should know

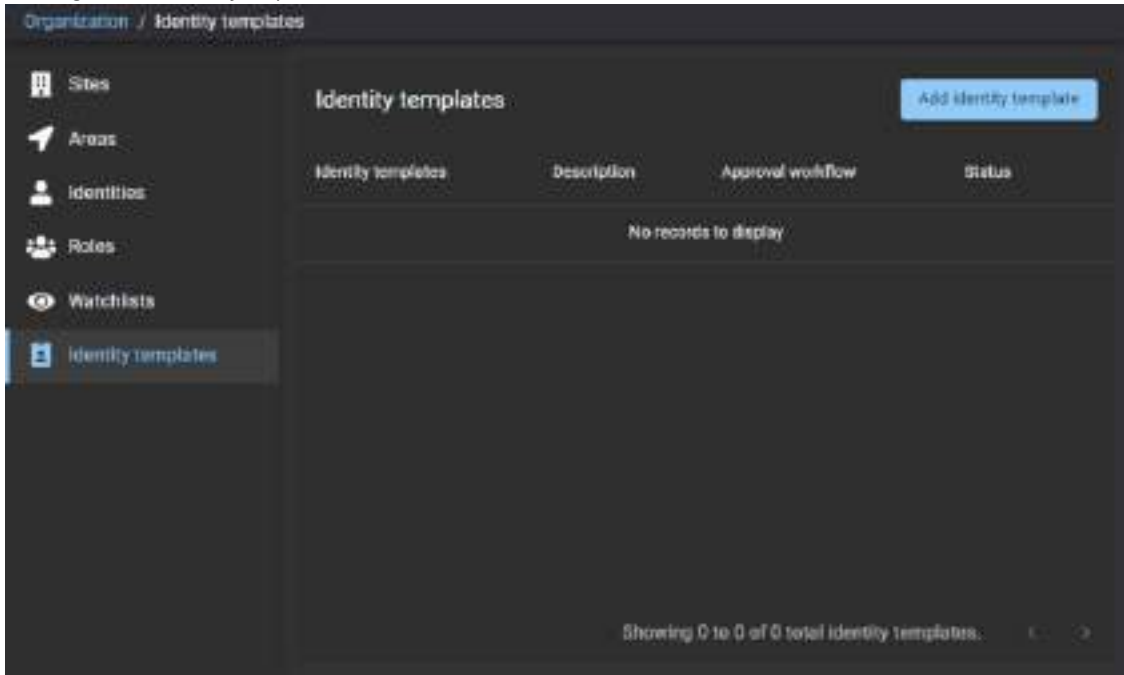
Only an account administrator can create an identity template.

Create identity templates to address the identity requests that your organization frequently encounters.

- You can create identity templates with predefined role access to suit different requirements. For example, identity requests for different types of contractors, or identity requests for large groups of specific employees who require access to a specific site or building.
- When an identity request is submitted using an identity template, the identity is added as a role member to the roles that apply to the template and inherits the associated role access.

Procedure

1. Click Organization > Identity templates.



2. Click Add identity template.
3. In the Identity template section, complete the fields or configure the settings as required:

The screenshot displays the 'New identity template' form. At the top, there's a progress indicator with three steps: 1. Identity template, 2. Permissions, and 3. Approval setting. The form fields include: 'Identity template name *' with the value 'Electrical contractors' and an 'Enabled' toggle switch; 'Description' with the value 'Electrical contractors for HQ Main Building'; and 'Form type *' with a dropdown menu set to 'Standard'. Below these are sections for 'Web portal access' (with a checked checkbox 'Enable option for web portal access') and 'Access control' (with checked checkboxes for 'An expiry date is required' and 'Enforce a maximum duration for the period of access'). A text input field shows 'Limit the maximum duration to 365 days'. At the bottom left is a 'Cancel' button, and at the bottom right is a 'Next' button.

Identity template name

Enter a name that summarizes the type of identity requests that the template is intended for. For example, Electrical contractors.

Description

Enter a meaningful description that describes the purpose of your template. For example, Electrical contractors for HQ Main Building.

Form type

Standard is the default.

Enabled

Move the slider to the Enabled position for this template to be available for selection when requesting an identity. Enabled is the default.

- a. In the Web portal access section, configure the option that you require.

Enable option for web portal access

Select the check box if you want to display the web portal access option when requesting an identity.

NOTE: When requesting multiple identities the availability of the web portal access option is dependent on your template configuration.

- If your template does not include the web portal access option, the web portal access fields are ignored.
- If your template does include the web portal access option, the web portal access fields are processed.

- b. In the Access control section, configure the options that you require.

An expiry date is required

Select the check box if you want to enforce an expiry date when creating identity requests.

Enforce a maximum duration for the period of access

Select the check box if you want to specify a maximum duration when creating identity requests.

Limit the duration to *nnn* days

Specify a maximum duration. For example, 365 days.

- c. Click Next.

4. In the Permissions section, configure the settings or add roles as required:

- a. In the Who can request this identity template? section, do one of the following:
- If you want all users to be able to select this identity template, select the All users can request identities check box.
 - If you want to select specific roles, click Add role.

NOTE: If you selected All users can request identities proceed to step 6.

5. If you clicked Add role, search for or select one or more roles and click Add.

NOTE: The roles that you add in the Who can request this identity template? section determine who can request identities using this template. For example, you might add a role, so that only *Contractor managers* can request identities. Another example could include buildings with tenants spaces, for that situation you might want to create *Tenant managers*.

6. (Optional) In the What roles do you need? section, add the roles that you require.
- a. Click Add role.
- b. Search for or select one or more roles and click Add.

Electrical contractors

Identity template Permissions Approval setting

Who can request this identity template?

☒ All roles can request identities

What roles do you need?

Identities created using this identity template are added as role members and inherit the associated role access

Add role

Role	Description
Certified Contractor Engineering	

Cancel Back Next

NOTE: The roles that you add in the What roles do you need? section determine the access that the identity inherits when an identity is requested using this template. For example, an electrical contractor role could be setup with access to rooms containing electrical infrastructure.

c. Click Next.

7. In the Approval setting section, select the Identity request approval workflow that you require.

New identity template

Identity template Permissions Approval setting

Identity request approval workflow

- No approval required
- Supervisor approval required
- Identity approvers approval required
- Supervisor and identity approvers approval required
- APT approval

No approval required
Automatically approved.

Supervisor approval required
Approved by the supervisor of the requester.
NOTE: If the requester has no supervisor (or is a trusted requester) the supervisor approval step is bypassed.

Identity approvers approval required
If selected, identity approvers must be added.
a. Click Add and choose either Add identities or Add roles.
b. Complete the steps as prompted.

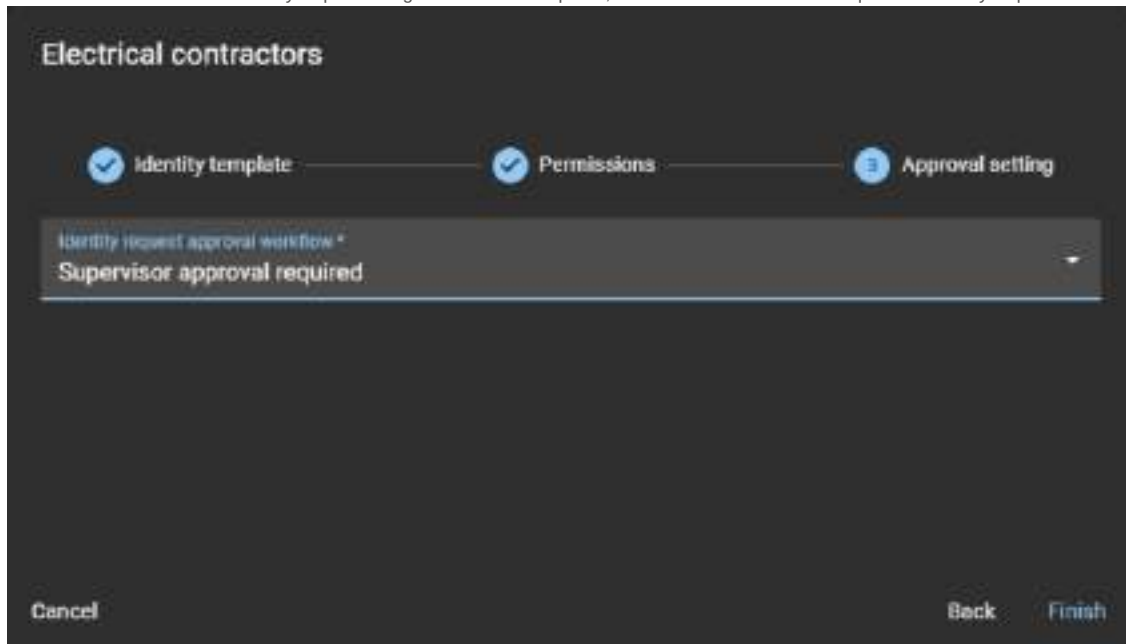
Supervisor and identity approvers approval required
If selected, supervisors are already associated with the identity, however the identity approvers must be added as described previously.
NOTE: If the requester has no supervisor (or is a trusted requester) the supervisor approval step is bypassed.

API approval

API approval is only used when the identity request approval workflow is customized to handle requests from an external service.

For example, Genetec ClearID™ LDAP Synchronization Agent, Genetec ClearID™ One Identity Synchronization Tool, or an API workflow for a plugin integration. In this situation, the request approvals are not shown in the ClearID user interface.

NOTE: If a user creates an identity request using the ClearID web portal, that user will still see their requests in the My requests dashboard.



8. Click Finish.

Results

Your template is now ready to be used.

Example



After you finish

Request an identity.

Browse

- Identity Request Feature Note (2 pages)

5.34.1 | Modifying an identity template in ClearID

After you have created your identity templates, you can modify the template settings or delete the template if required.

Before you begin

Create your identity templates.

What you should know

Only an account administrator can modify an identity template.

Procedure

1. Click Organization > Identity templates.
2. (Optional) If a template is no longer required click Delete (X) to delete the template.
3. Click a template in the list.
4. In the Identity template section, make any changes that you require and click Next.
5. In the Permissions section, make any changes that you require and click Next.
6. In the Approvals section, make any changes that you require and click Finish.

Parent topic: [Creating an identity template in ClearID](#)

5.35 | Requesting identities in ClearID

You can use the Genetec ClearID™ self-service portal to request an individual identity, or to request multiple identities using a CSV import. Using the self-service portal with optional approver workflow simplifies the approval process by only notifying the specified approvers.

Before you begin

- Familiarize yourself with workflows.

What you should know

Anyone with the required permission can submit an identity request.

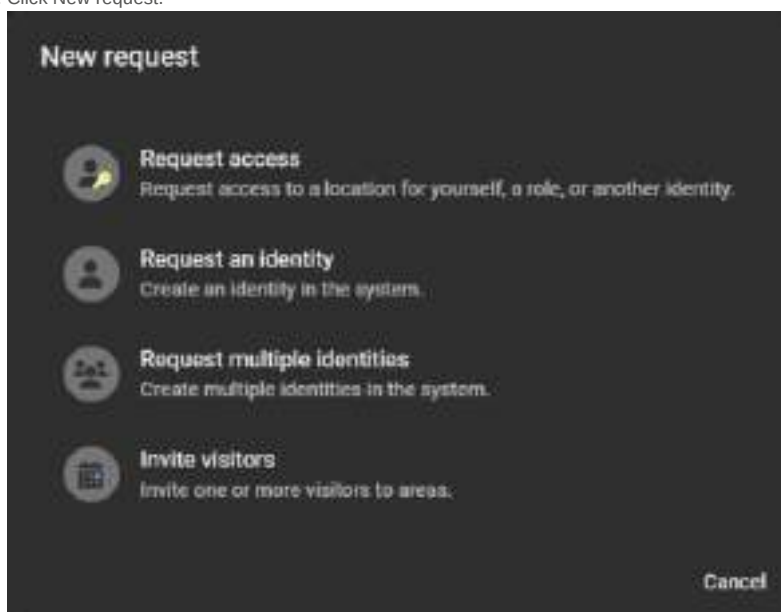
NOTE: In the past, most access control solutions would typically not track or record why an identity was required.

In ClearID the identity request includes: who requested the identity, when, and the reason for the identity request.

- Separate identity requests and approval workflows are created for each identity requested.
- After the request summary is confirmed, it is automatically assigned to the right individuals for approval.
- After the approval process occurs, the requester receives an email notifying them whether the identity request was approved or rejected.

Procedure

1. Log on to the self-service portal.
2. Click Dashboard.
3. Click New request.



4. In the New request dialog, do one of the following:
 - Requesting an identity in ClearID
 - Requesting multiple identities using a CSV import in ClearID
5. Click Finish.

Results

After you finish

Depending on the identity template that you selected, your identity requests are either approved automatically or approvers review identity requests and approve (or reject) as required.

Browse

- [Identity Request Feature Note \(2 pages\)](#)

Browse

- [Checking the status of identity requests in ClearID](#)

5.35.1 | Requesting an identity in ClearID

You can use the Genetec ClearID™ self-service portal to request an identity. This request adds someone (as an identity) that does not currently exist in the system. Using the self-service portal with an optional approver workflow simplifies the approval process by only notifying the specified approvers.

Before you begin

- [Familiarize yourself with workflows.](#)

What you should know

Anyone with the required permission can submit an identity request.

This task describes how to use the identity request wizard in the web portal to request an identity. The requester can use the wizard to add someone (as an identity) that does not already exist in the system.

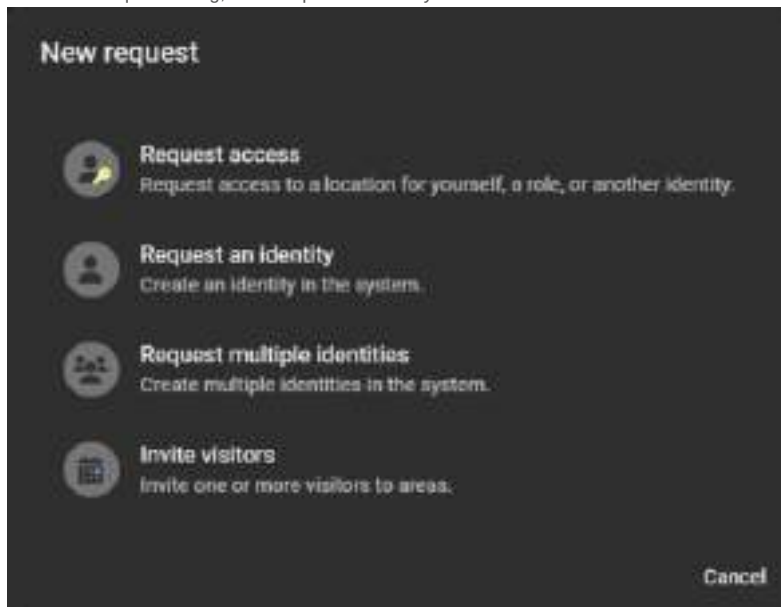
NOTE: In the past, most access control solutions for sites typically did not track or record why an identity was required.

In ClearID, the identity request includes: who requested the identity, when, and the reason for the identity request.

- Separate identity requests and approval workflows are created for each identity requested.
- After the request summary is confirmed, it is automatically assigned to the right individuals for approval.
- After the approval process occurs, the requester receives an email notifying them whether the identity request was approved or rejected.

Procedure

1. Log on to the self-service portal.
2. Click Dashboard.
3. Click New request.
4. In the New request dialog, click Request an identity.



5. In the New identity request wizard, select a template from the Identity template list and click Next.
6. In the General information section, complete the fields.

The screenshot shows a web interface for creating an identity request. At the top, a progress bar indicates four steps: 1. Identity template (completed), 2. General information (current step), 3. Work details, and 4. Review. The 'General information' section contains several input fields: 'First name' (John), 'Last name' (Doe), 'Email' (johndoe@test.com), 'Middle name' (empty), 'Mobile phone number' (123-456-7899), 'Preferred name *' (John Doe), and 'External ID' (empty). Below this is the 'Web portal access' section, which includes a slider for 'Grant user access to the web portal' set to 'N/A'. At the bottom left is a 'Save as draft' button, and at the bottom right are 'Back' and 'Next' buttons.

Tip: At any point during the creation of the request, you can click Save as draft to save an incomplete request (while waiting for missing information). Alternatively, you can click Delete if the request is no longer required. You can access your drafts from the My requests tab in the Dashboard.

7. (Optional) In the Web portal access section, move the Grant user access to the web portal slider to the Enabled position if you want to allow the identity being requested to be able to log on and use the ClearID web portal.

NOTE: The Grant user access to the web portal slider is disabled when the identity template you are using does not include the option for web portal access.

- a. If you enabled web portal access enter a user name.

NOTE: The user name must be a valid email address.

8. In the Access control section, complete the fields. Mandatory fields are highlighted with an asterisk (*).

Time zone

Select the time zone that you require.

Activation date

Select the date when the requested identity should be activated.

Expiration date

Select the date when the requested identity should be deactivated.

NOTE: Depending on the identity template selected, the expiration date might not be mandatory.

The screenshot shows the 'identity request' form. At the top, there are two input fields: 'Preferred name *' with the value 'John Doe' and 'External ID'. Below these is the 'Web portal access' section with a toggle switch for 'Grant user access to the web portal' set to 'N/A'. The 'Access control' section includes a 'Time zone *' dropdown set to 'America/Toronto (-05:00) [EST]'. A message states: 'A template policy limit is currently active, individual access is limited to 365 days.' Below this are 'Activation date *' (01/01/2022) and 'Expiration date *' (03/31/2022) fields, each with a calendar icon. A 'Duration' field shows '90 d'. At the bottom are 'Save as draft', 'Back', and 'Next' buttons.

NOTE: The identity activation and expiration times are dependent on and triggered by the access period specified in the identity request and the time in the selected time zone. If a *maximum duration* was specified and enabled in the identity template, a message is displayed to indicate the maximum period of access that you can specify.

a. Click Next.

9. In the Work details section, complete the fields.

The screenshot shows the 'New Identity request' form with a progress bar at the top indicating four steps: 'Identity template' (completed), 'General information' (completed), 'Work details' (current step), and 'Review'. The 'Work details' section contains three input fields: 'Company' (Sparky Sparks Electrical), 'Employee ID', and 'Job title' (Electrician). Below these are 'Department' (Electrical Contractors) and 'Country *' (Canada) fields. A section titled 'Supervisors of John Doe' shows a table with one entry: 'Fred Smith' with email 'fred.smith@test.com'. At the bottom are 'Save as draft', 'Back', and 'Next' buttons.

Company

Enter the company name.

Employee ID

Enter the Employee ID.

Job title

Enter the job title.

Department

Enter the department.

Country

Select a country from the list. This country setting is only used by the *Standard* form.

Tip: Enter the first letter of the country to jump to that part of the country list.

- In the Supervisors of section, click  to add supervisors.

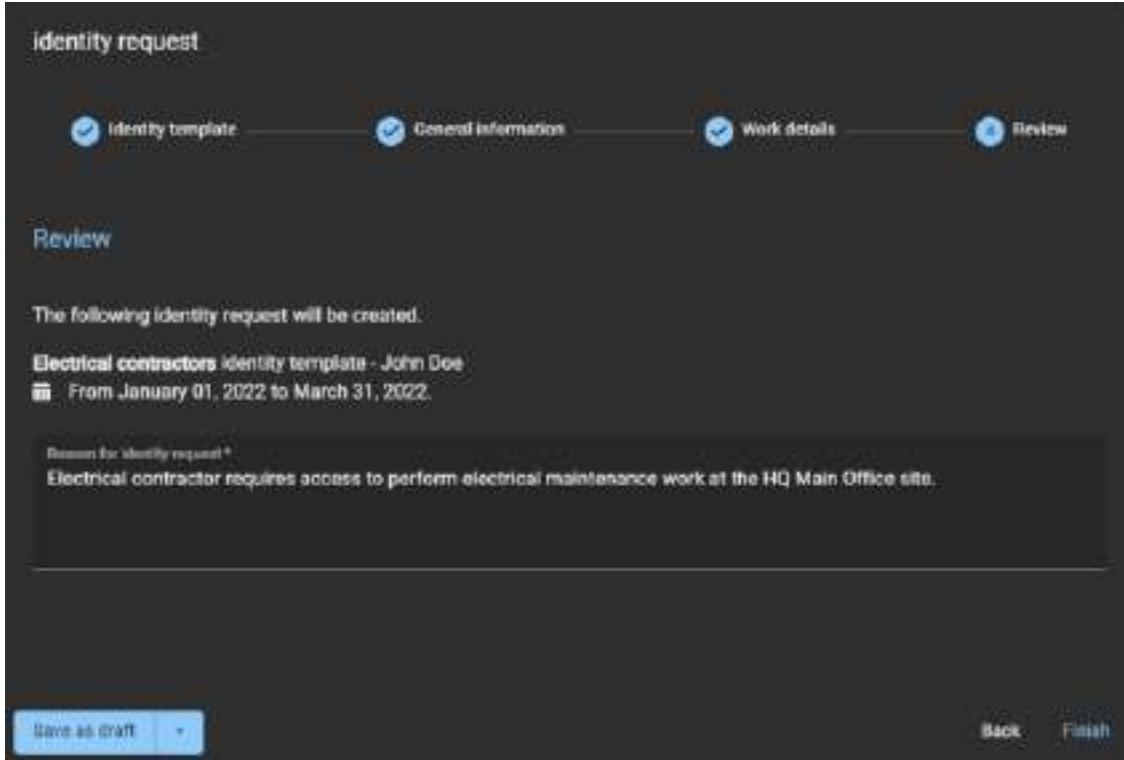
NOTE: The supervisors specified here are the supervisors of the new identity being created. The requester is automatically added to the Supervisors of list by default.

- (Optional) Add more supervisors as required.

- (Optional) Click  to remove any supervisors that are no longer required. For example, If you requested identities on behalf of someone else, you might remove yourself (if required) after the relevant supervisors are added.

- Click Next.

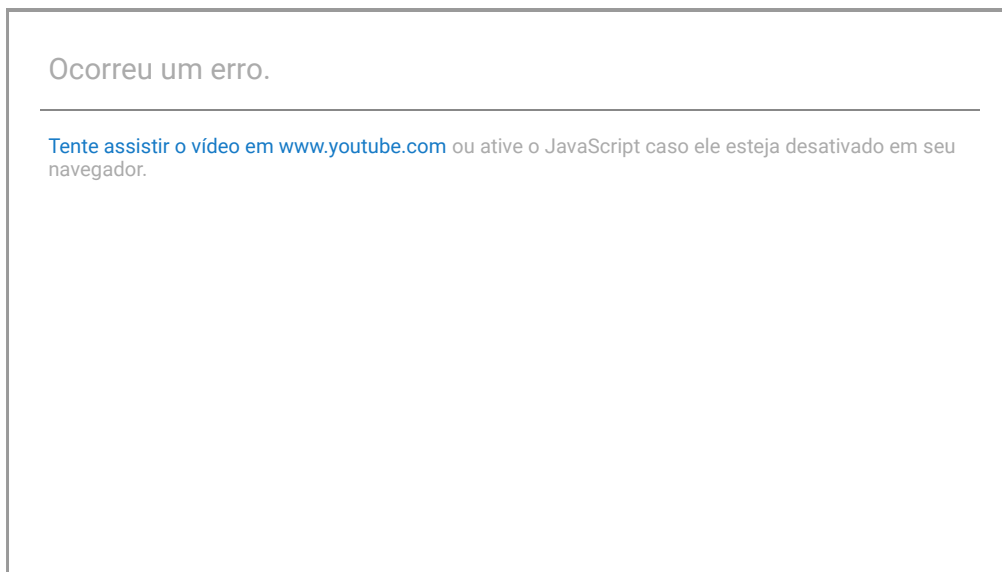
- In the Review section, verify that the identity request details are correct.



- If the details are correct, add a reason for the request and click Finish.

An email notification is sent to approvers (if applicable).

Example



After you finish

Depending on the identity template that you selected, your identity requests are either approved automatically or approvers review identity requests and approve (or reject) as required.

Parent topic: [Requesting identities in ClearID](#)

Browse

- Identity Request Feature Note (2 pages)

5.35.2 | Requesting multiple identities using a CSV import in ClearID

You can use the Genetec ClearID™ self-service portal to request multiple identities. This request adds multiple people (as identities) that do not currently exist in the system. Using the self-service portal with the optional approver workflow simplifies the approval process by only notifying the specified approvers.

Before you begin

- Familiarize yourself with workflows.

What you should know

Anyone with the required permission can submit an identity request.

This task describes how to use the identity request wizard in the web portal to request multiple identities using a CSV import. The requester can use the wizard to add people (as identities) that do not already exist in the system.

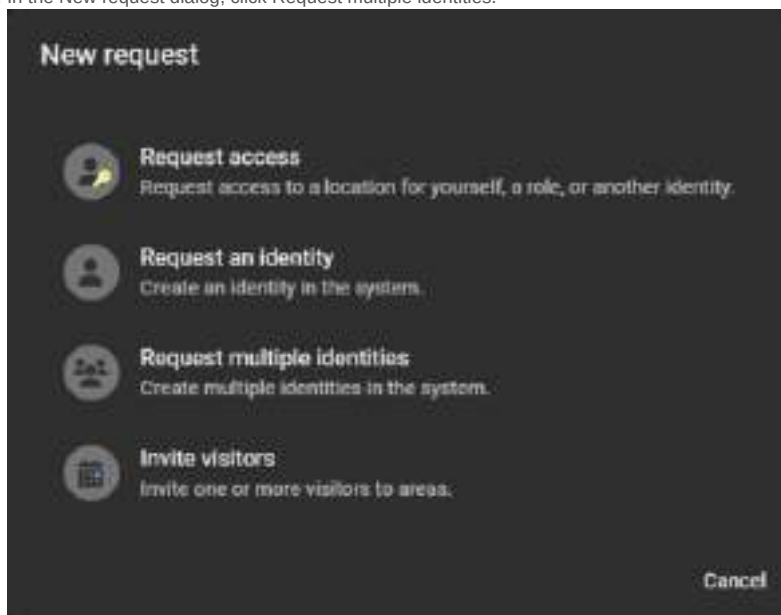
NOTE: In the past, most access control solutions would typically not track or record why an identity was required.

In ClearID, the identity request includes: who requested the identity, when, and the reason for the identity request.

- Separate identity requests and approval workflows are created for each identity requested.
- After the request summary is confirmed, it is automatically assigned to the right individuals for approval.
- After the approval process occurs, the requester receives an email notifying them whether the identity request was approved or rejected.

Procedure

1. Log on to the self-service portal.
2. Click Dashboard.
3. Click New request.
4. In the New request dialog, click Request multiple identities.



5. In the Request multiple identities wizard Basic information section, complete the fields.
 - a. In the Request name section Name field, enter a meaningful name for your request.

This meaningful name ensures that your request can be easily identified in the My requests or My tasks dashboards later.
 - b. In the Supervisors section, search for and select one or more identities to assign as supervisors for the imported identities. You can assign a maximum of 20 supervisors.

NOTE: The supervisors specified here are the supervisors of the new identities being created. The requester is automatically added to the Supervisors list by default.
 - c. In the Identity request template section, select a template from the list.
 - d. In the Reason for request section, add a reason for the request and click Next.

The screenshot shows the 'Request identities' form at the 'Basic Information' step. The progress bar at the top indicates three steps: 1. Basic Information (active), 2. Import, and 3. Review. The form contains the following sections:

- Request name:** A text field with the value 'Renovation contractors (4th floor)'. A note above the field states: 'Enter a meaningful name for your request so that it can be easily identified in the "My requests" or "My team" dashboards later.'
- Supervisors:** A section with a search bar labeled 'Identities' containing '+ Add One' and a dropdown arrow. Below the search bar, it shows '1 / 38'.
- Identity request template:** A dropdown menu with the selected value 'Electrical contractors'.
- Reason for request:** A text area with the value 'Electrical contractors for 4th floor renovations'.

At the bottom of the form, there are 'Cancel' and 'Next' buttons.

6. In the Import section, click Import from CSV.

The screenshot shows the 'Request identities' form at the 'Import' step. The progress bar at the top indicates three steps: 1. Basic Information, 2. Import (active), and 3. Review. The form contains the following sections:

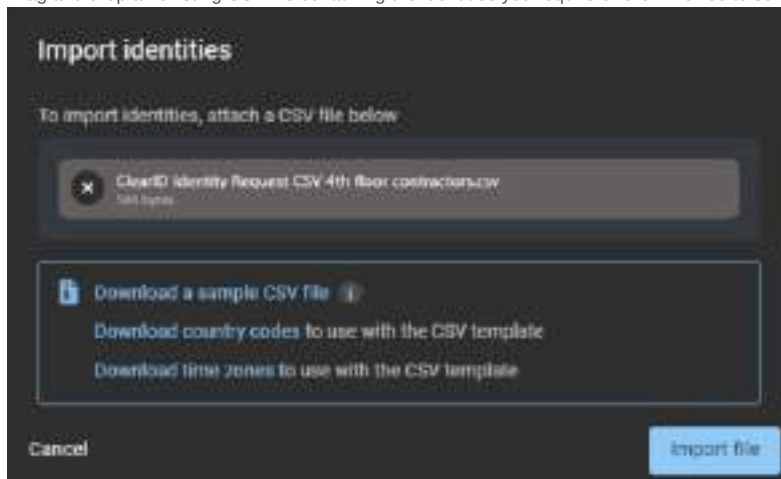
- Import identities:** A section with a note: 'Import your identities for this request below. If any data errors are encountered during the identities import, fix the issues in the CSV file then import the file again. CAUTION: Importing the file again overwrites any data already imported into the grid.'
- Import from CSV:** A prominent blue button.
- No records to display:** A message indicating that no identities have been imported yet.
- 0 total results:** A status indicator at the bottom right.

At the bottom of the form, there are 'Cancel', 'Back', and 'Next' buttons.

NOTE: You can import a maximum of 1000 identities per identity request.

7. Choose one of the following:

- Use an existing CSV file.
 - Download a sample CSV file.
8. If you chose to use an existing CSV file, do the following:
- a. Drag and drop an existing CSV file containing the identities you require or click Browse to select the file you require.



- b. Click Import file to import the identities list.
9. Review the imported identities data and check for any errors.
- NOTE: When requesting multiple identities, the availability of the web portal access option depends on your template configuration.
- If your template does not include the web portal access option, the web portal access fields are ignored.
 - If your template does include the web portal access option, the web portal access fields are processed.

The following example shows imported identities that do not include web portal access.

Request identities

1

Identity Information

2

Import

3

Review

Import identities

Import your identities for this request below. If any data errors are encountered during the identities import, the messages in the CSV file show import the file again. Do not edit the template for the request information and data already imported into the grid.

Import from CSV

First name	Last name	Middle name	Email	Mobile phone number	Preferred name	First name	Activation date	Expiration date	Company	Employee ID	Job title	Department	Job country	Internal ID
John	Smith	A.	johnsmith@corp.com	12345	John A. Smith	American Express	1/15/2023, 7:44 PM	3/31/2025, 7:44 PM	Corp Co.	123456	Manager	Sales	Canada	1000011
John	Doe	A.	john.doe@corp.com	555-1234	John A.D.	American Express	1/15/2023, 7:44 PM	3/31/2025, 7:44 PM	Corp Co.		Admin	Sales	United States of America (US)	

0/1000 identities

Cancel

Back

Next

The following example shows imported identities that include web portal access.

The following example shows imported identities that include web portal access:

Request identities

Step 1: Identity Information

Step 2: Import

Step 3: Review

Import identities

Import your identities for this request below. If any data errors are encountered during the identities import, the messages in the CSV file show import the file again. Do not edit the template for the request information and data already imported into the grid.

Import from CSV

First name	Last name	Middle name	Email	Mobile phone number	Preferred name	First name	Activation date	Expiration date	Company	Employee ID	Job title	Department	Job country	Internal ID
John	Smith	A.	johnsmith@corp.com	12345	John A. Smith	American Express	1/15/2023, 7:44 PM	3/31/2025, 7:44 PM	Corp Co.	123456	Manager	Sales	Canada	1000011
John	Doe	A.	john.doe@corp.com	555-1234	John A.D.	American Express	1/15/2023, 7:44 PM	3/31/2025, 7:44 PM	Corp Co.		Admin	Sales	United States of America (US)	

0/1000 identities

Cancel

Back

Next

If any errors are encountered in the imported CSV file, they are highlighted in red. Any corrections must be applied in the CSV file and then imported again.

CAUTION:

Correcting any errors will overwrite identities data already imported into the grid.

- a. (Optional) If your identities list is long, consider using the Show errors only slider.
- b. Click Next.

10. In the Review section, review the information to ensure that everything is correct.

Request identities

Basic information Import Review

Review
Ensure that all information is correct before completing the request.

Request name	Renovation contractors (4th Floor)
Supervisors	John Doe
Identity request template	Electrical contractors
Reason for request	Electrical contractors for 4th floor renovations.
Identities	2 identities will be requested

Cancel Back Finish

- a. If the details in the Review section are correct, click Finish.

11. If you chose Download a sample CSV file, do the following:

- a. Click Download a sample CSV file.

Import identities

To import identities, attach a CSV file below

Drag and drop a CSV file here or [Browse](#)

[Download a sample CSV file](#)

[Download country codes to use with the CSV template](#)

[Download time zones to use with the CSV template](#)

Cancel Import file

- b. Select and open the downloaded CSV file.

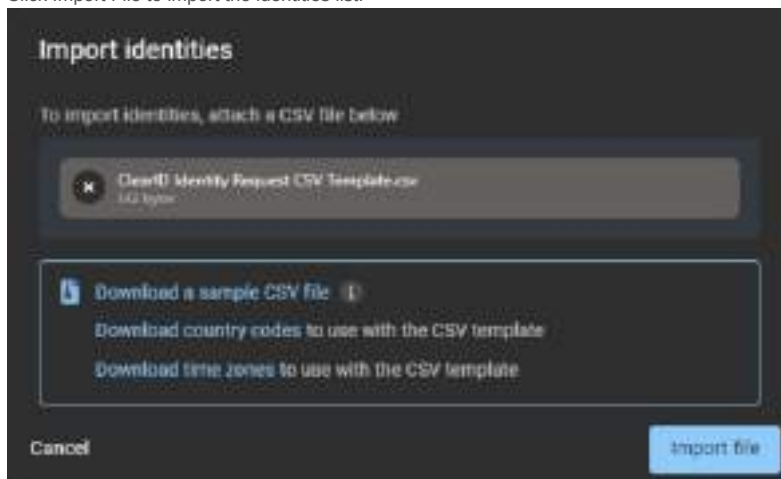
Tip: Download the *country codes* and *time zones* samples for reference if the *country codes* and *time zones* you require are not shown in the downloaded sample.

- c. For each identity, complete a row of identity information in the CSV template file.

first name	last name	middle name	email	mobile phone number	preferred time zone	activation date	expiration date	company	employee id	job title	department	job count	external id	enable id	web portal username	password
John	Smith	B.	john@smith.com	12345	John (U.S. America)	1/1/2021	12/31/2021	Smith Co.	1012345	Manager	Sales	CAN	0000001	TRUE	john@smith.com	
Jane	Doe	A.	jane@smith.com	67890	Jane (U.S. America)	1/1/2021	12/31/2021	Smith Co.		Sales rep	Sales	USA		FALSE		

NOTE: The columns in the CSV template can vary depending on the settings in your site configuration.

- Save the identities list as a CSV file.
- Return to the Import identities dialog, to drag and drop or click Browse to select the file you created.
- Click Import File to import the identities list.



- Review the imported identities data and check for any errors.

First name	Last name	Middle name	Email	Mobile phone number	Preferred time zone	Activation date	Expiration date	Company	Employee ID	Job title	Department	Job count	External ID	Internal ID
John	Smith	B.	john@smith.com	12345	John (U.S. America)	1/1/2021, 7:44 PM	12/31/2021, 7:44 PM	Smith Co.	1012345	Manager	Sales	Canada	0000001	
Jane	Doe	A.	jane@smith.com	67890	Jane (U.S. America)	1/1/2021, 7:44 PM	12/31/2021, 7:44 PM	Smith Co.		Sales rep	Sales	United States of America (EST)		

If any errors are encountered in the imported CSV file, they are highlighted in red. Any corrections must be applied in the CSV file and then imported again.

CAUTION:

Correcting any errors will overwrite identities data already imported into the grid.

- (Optional) If your identities list is long, consider using the Show errors only slider.
- Click Next.

- In the Review section, review the information to ensure that everything is correct.

Request identities

Basic information Import Review

Review
Ensure that all information is correct before completing the request.

Request name	Renovation contractors (4th Floor)
Supervisors	John Doe
Identity request template	Electrical contractors
Reason for request	Electrical contractors for 4th floor renovations.
Identities	2 identities will be requested.

Cancel Back Finish

a. If the details in the Review section are correct, click Finish.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Depending on the identity template that you selected, your identity requests are either approved automatically or approvers review identity requests and approve (or reject) as required.

Parent topic: [Requesting identities in ClearID](#)

Browse

- [Identity Request Feature Note \(2 pages\)](#)

5.36 | Canceling identity requests in ClearID

To cancel identity requests, the identity requester must review the pending requests and then decide which requests to cancel.

Before you begin

Ensure that some identity requests have already been submitted.

What you should know

Only identity requesters can cancel identity requests.

- Only pending requests can be canceled.
- Completed requests cannot be canceled.

NOTE: If one of the requested identities is canceled, all the configured approvers are added to the .cc list in the email notification for identity request approval and completion titled: "Identity request for *identity* has been updated".

Procedure

To cancel an identity request:

1. Click Dashboard > My requests.
2. From the Status list, filter the requests that are displayed:

Status

Select a status from the following:

All

Displays all pending or completed tasks.

Pending

Displays tasks waiting for approval.

Completed

Displays completed tasks and their status. For example, approved, completed, denied, or canceled.

3. In the My requests list, click an identity request to display additional details about the request.

Identity request for Jim Brown

? Identity requested by: Fred Smith on December 16, 2021 9:52 AM
fsmith@test.com

Waiting for approval from 1 approver

Identity template: Electrical contractors

General information

First name	Middle name	Last name
Jim		Brown
Preferred name	Email	Phone number
Jim Brown		
External ID		

Work details

Company	Employee ID	
Job title	Department	Country
		Canada

Access control

Activation date	Expiration date	Time zone
December 16, 2021	March 31, 2022	America/Toronto

Supervisors

Name	Email
Fred Smith	fsmith@test.com

Web portal access

Grant user access to the web portal: N/A

History

- Dec 16 Genetec ClearID™ service edited the request.
- Fred Smith created the request.

Close Cancel request

NOTE: The buttons that are available in the identity request details vary depending on whether you are the requester, supervisor, or an approver.

4. Review the identity request details for accuracy and completeness.
5. If the identity request is no longer required click Cancel request.
 - a. Enter the reason for cancellation and click Confirm.

To cancel multiple identities requested using a CSV import:

1. Click Dashboard > My requests.
2. From the Status list, filter the requests that are displayed:

Status

Select a status from the following:

All

Displays all pending or completed tasks.

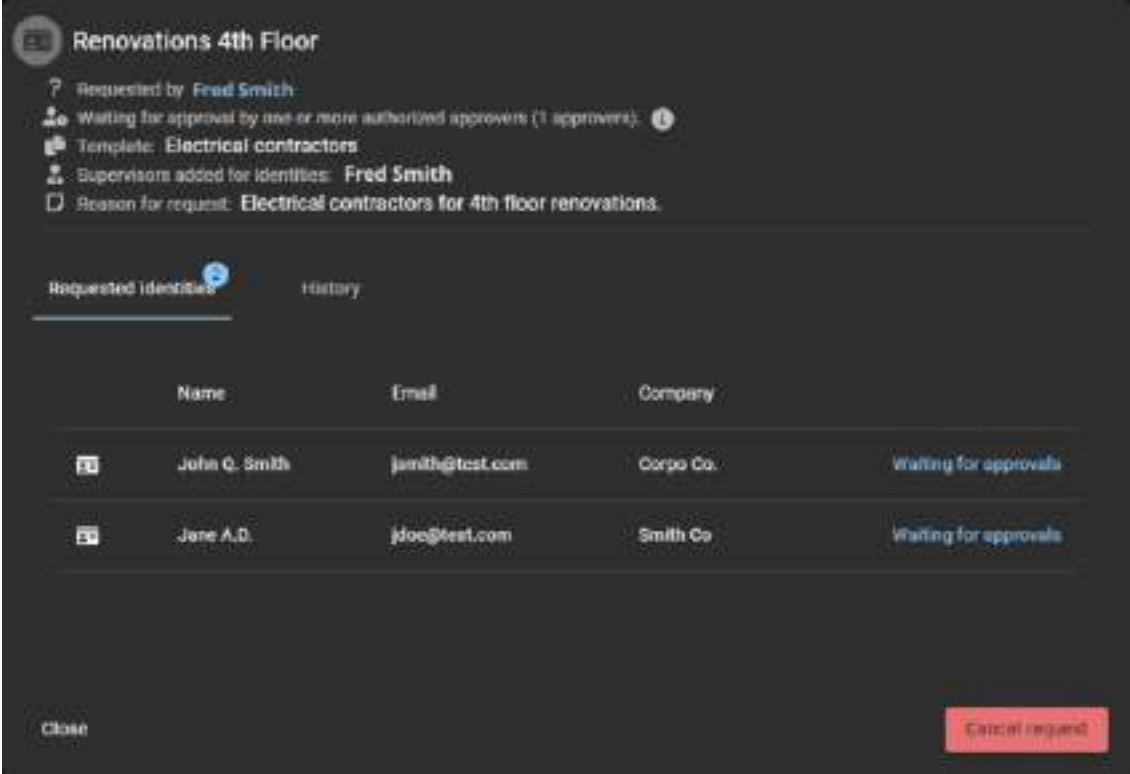
Pending

Displays tasks waiting for approval.

Completed

Displays completed tasks and their status. For example, approved, completed, denied, or canceled.

3. In the My requests list, click an identities request awaiting approval to display additional details about the request.



NOTE: The buttons that are available in the identities request details vary depending on whether you are the requester, supervisor, or an approver.

4. Review the identity request details for accuracy and completeness.
5. If the identity request is no longer required click Cancel request.
a. Enter the reason for cancellation and click Confirm.

Results

The identity request is now canceled.

5.37 | Approving identity requests in ClearID

To approve identity requests, a supervisor or identity approver must review the pending approvals and then decide which requests to approve.

Before you begin

Ensure that some identity requests have already been submitted.

What you should know

Only supervisors or identity approvers can approve identity requests.

Procedure

To approve an identity request:

1. Click Dashboard > My tasks.
2. From the Status list, filter the tasks that are displayed:

Genetec ClearID®; User Guide

Displayed in the header

Status

Select a status from the following:

All

Displays all pending or completed tasks.

Pending

Displays tasks waiting for approval.

Completed

Displays completed tasks and their status. For example, approved, completed, denied, or canceled.

3. In the My tasks list, click an identity request to display additional details about the request.

Identity request for Jim Brown

Identity requested by: Fred Smith on December 14, 2021 9:52 AM
Email: fsmith@quest.com

Waiting for approval from 1 approver

Identity template: Electrical contractors

General information			Work details		
First name: Jim	Middle name:	Last name: Brown	Company:	Employee ID:	
Preferred name: Jim Brown	Email:	Phone number:	Job title:	Department:	Country: Canada
External ID:					

Access control			Supervisor	
Activation date: December 14, 2021	Expiration date: March 31, 2022	Time zone: America/Toronto	Name: Fred Smith	Email: fsmich@quest.com

Web portal access: Grant user access to the web portal: Yes / No

History:

- Dec 14 Genetec ClearID™ service edited the request.
- Dec 14 Fred Smith created the request.

Buttons: Edit, Deny, Approve

NOTE: The buttons that are available in the identity request details vary depending on whether you are the requester, supervisor, or an approver.

4. Review the identity request details for accuracy and completeness.
5. (Optional) If you need to modify the identity request, click Edit and make any changes that are required.
 - a. Click Save.
6. If the request is not valid or contains incorrect information, click Deny.
 - a. Enter the reason for denial and click Confirm.
7. If the request is valid and correct, click Approve.
8. In the Reason for approval field, enter the reason for approval and click Confirm.

Identity request for Jim Brown

Requested by: **Jim Brown** | Status: **Open** | Request ID: **123456789** | Job title: **Electrical Contractor** | Department: **Facilities** | Country: **Canada**

Access control

Activation date: **December 14, 2021** | Expiration date: **March 31, 2022** | Time zone: **America/Toronto**

Supervisors

Name	Email
Fred Smith	fsmith@test.com

Web portal access

Grant user access to the web portal: **Yes** (N/A)

Reason for identity request

Access required for electrical contractor work.

History

- Dec 14** Genetec ClearID® service edited the request.
- Dec 14** Fred Smith created the request.

Reason for approval

Reason: **Access granted for new electrical contractor**

48 / 300

Custom

To approve identities imported using a CSV import:

1. Click Dashboard > My tasks.
2. In the My tasks list, click an identities request to display additional details about the request.

Renovation contractors (4th Floor)

Requested by: **Fred Smith**

Waiting for approval by one or more authorized approvers (1 approver).

Template: **Electrical contractors**

Supervisors added for identities: **Fred Smith**

Reason for request: **Electrical contractors for 4th floor renovations**

Requested identities | History

Show errors only (0)

Name	Email	Company	Deny all	Approve all
John Q. Grey	jgrey@test.com	Corpo Co.	X	✓
Jane A.D.	jasmith@test.com	Smith Co	X	✓

Close | **Cancel request** | **Save**

NOTE: The buttons that are available in the identity request details vary depending on whether you are the requester, supervisor, or an approver.

3. Review the identities request details for accuracy and completeness.
 - a. If all the identities in the request are correct, click Approve all then click Save.
 - b. If all the identities in the request are not correct, click Deny all then click Save.
4. (Optional) If you need to modify an identity, click View identity request details (🔍) on the row for the identity to review the details of that request.
 - a. Click Edit to make any changes that you require.

- b. Click Save.
5. If the request is not valid or contains incorrect information, click Deny () on the row for the identity.
 - a. Enter the reason for denial and click Confirm.
6. If the request is valid and correct, click Approve () on the row for the identity.
 - a. Click Save.
 - b. In the Reason for approval field, enter the reason for approval and click Confirm.

Results

The identity request is now approved. The identity is now created and if applicable inherit the role access to associated areas during the periods specified in their identity request.

NOTE: (Optional) Additional communications might also be provided by your organization regarding where and how to retrieve a badge access card (if required) for the new identity.

Example



After you finish

Browse

- [Identity Request Feature Note \(2 pages\)](#)

5.37.1 | Modifying an identity request in ClearID

To modify identity requests, a supervisor or identity approver must review the pending approvals and then decide which requests to modify.

Before you begin

Ensure that some identity requests have already been submitted.

What you should know

Only supervisors or identity approvers can modify identity requests.

Procedure

To modify an identity request:

1. Click Dashboard > My tasks.
2. From the Status list, filter the tasks that are displayed:

Status

Select a status from the following:

All

Displays all pending or completed tasks.

Pending

Displays tasks waiting for approval.

Completed

Displays completed tasks and their status. For example, approved, completed, denied, or canceled.

3. In the My tasks list, click an identity request awaiting approval to display additional details about the request.

Identity request for Jim Brown

? Identity requested by: Fred Smith on: December 16, 2021 9:52 AM
✉ fsmith@test.com

👤 Waiting for approval from 1 approver: ⓘ

Identity template: Electrical contractors

General information

First name: Jim	Middle name:	Last name: Brown
Preferred name: Jim Brown	Email:	Phone number:
External ID:		

Work details

Company:	Employee ID:	
Job title:	Department:	Country: Canada

Access control

Activation date: December 16, 2021	Expiration date: March 31, 2022	Time zone: America/Toronto

Web portal access

Guest user access to the web portal: ⓘ [View](#)

Supervisors

Name	Email
Fred Smith	fsmith@test.com

History

👤 Dec 16	Genetec ClearID™ service edited the request.
👤	Fred Smith created the request.

Close

[Edit](#) [Deny](#) [Approve](#)

4. Review the identity request details for accuracy and completeness.
5. To modify the identity request, click Edit and make any changes that are required.
 - a. Click Save.

To modify multiple identities requested using a CSV import:

1. Click Dashboard > My tasks.
2. From the Status list, filter the tasks that are displayed:

Status

Select a status from the following:

All

Displays all pending or completed tasks.

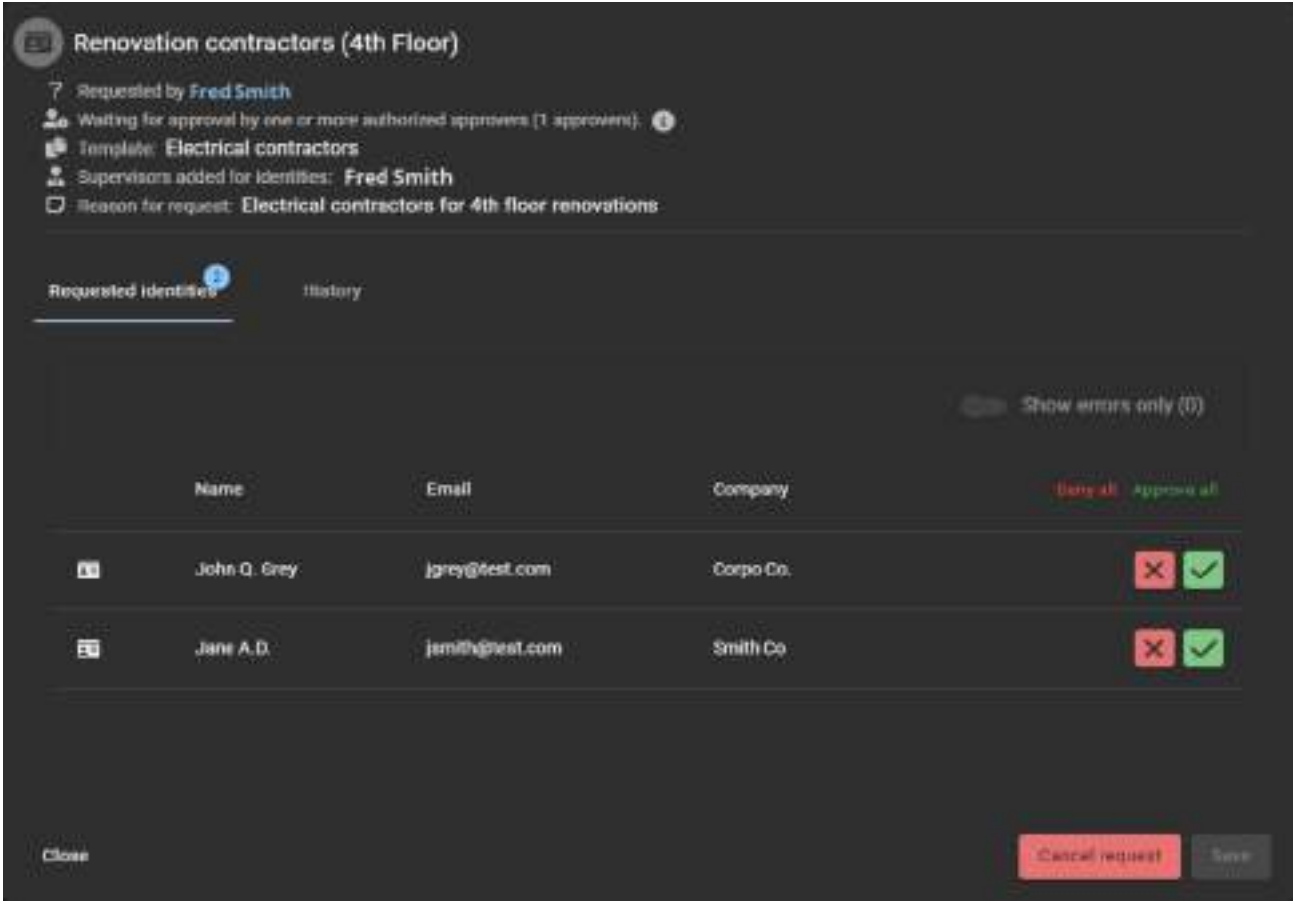
Pending

Displays tasks waiting for approval.

Completed

Displays completed tasks and their status. For example, approved, completed, denied, or canceled.

3. In the My tasks list, click an identities request awaiting approval to display additional details about the request.



4. (Optional) If you need to modify an identity, click View identity request details () on the row for the identity to review the details of that request.
- a. Review the identity request details for accuracy and completeness.
 - b. Click Edit to make any changes that you require.
 - c. Click Save.

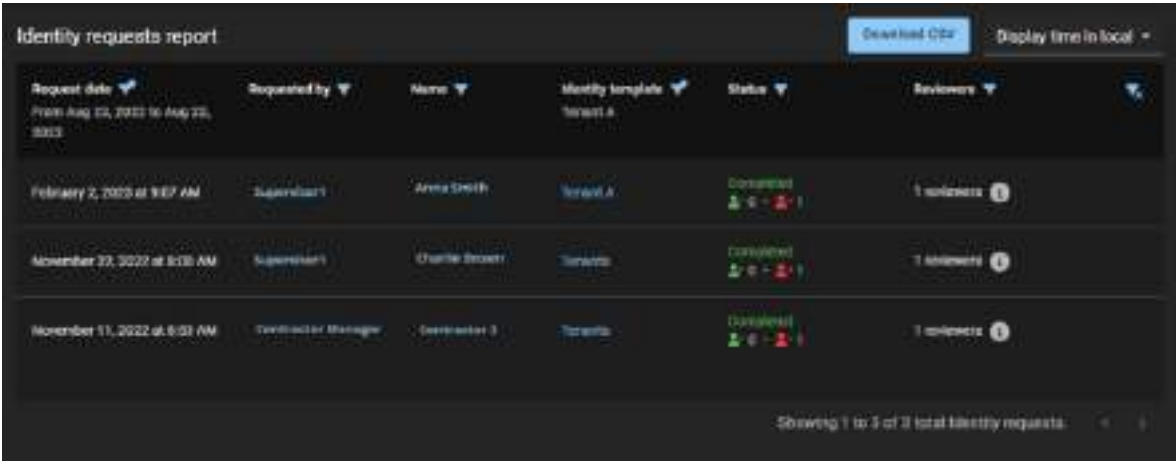
After you finish

Approve your identity requests.
Parent topic: [Approving identity requests in ClearID](#)

5.38 | About identity requests report in ClearID

In Genetec ClearID™, an identity requests report is a list of identity requests for your ClearID account. The report includes information about the identity request date, requester, name, identity template, status, and reviewers.

Identity requests report



The identity requests report is used by administrators to check the status of all identity requests at the account level. The report can also be used to provide identity requests information to auditors.

Filters can be used to help refine the search results by identity request date, requested by, name, identity template, status, and reviewers.

Browse

- [Checking the status of identity requests in ClearID](#)

5.39 | Checking the status of identity requests in ClearID

As an *Account administrator* you can check the status of identity requests to ensure that the organization is security-compliant, audit ready, and that the requests are processed in a timely fashion.

Before you begin

You must be an *Account administrator* to view the Identity requests report and check the status or progress of identity requests.

Procedure

1. From the homepage, click Reports > Identity requests.

Request date	Requested by	Name	Identity template	Status	Reviewers
February 2, 2022 at 9:07 AM	Supervisor1	Anna Smith	Template A	Completed	1 reviewers
November 22, 2022 at 1:05 AM	Supervisor1	Charlie Brown	Template	Completed	1 reviewers
November 11, 2022 at 6:03 AM	Contractor Manager	Supervisor 3	Template	Submitted	1 reviewers

2. In the Identity requests report page, select the required display time format.

Display time in local

Report times are displayed using the system time from the computer of the logged-in user.

Display time in UTC

Report times are displayed using Coordinated Universal Time (UTC).

3. Filter the report based on your required criteria:

Request date

In the Request date column, click  to filter the results by date.

If you selected Date range, use the calendar picker to select the date range that you require.

NOTE: The Request date time period is limited to a maximum of 1 year.

Requested by

In the Requested by column, click  to filter the results by identity requester.

- Enter a user name or email address in the search field.
- (Optional) Click the Requested by hyperlink to display summary details about the requester.

Name

In the Name column, click  to enter a search string and filter the results by Any words or All words.

(Optional)

Click the Name hyperlink to display the identity request.

NOTE: If you're an approver, you can Approve or Deny the pending identity request while viewing the request.

Identity template

In the Identity template column, click  to filter the results by identity template type.

Status

In the Status column, click  to filter the results by status.

- Select one or more check boxes to filter the results by the statuses that you require (Submitted, Waiting for approvals, Denied, Approved, Canceled, or Completed).

Reviewers

In the Reviewers column, click  to filter the results by identity, role, or both.

(Optional)

Click  to reset filter selections.

4. Click Download CSV, to download a copy of the identity requests report in CSV format. The report can then be used for auditing purposes, to keep a physical copy, to attach to an audit request, to review offline, or to manipulate or consolidate data in a spreadsheet for other audiences.

a. Follow your browser prompts to complete downloading the exported file.

The file is exported as a .CSV file to the default download location for your browser. By default the exported file is created using the name of your site. For example, *IdentityRequestReport_fromdate_to_todate_SiteActivityReport.csv* (IdentityRequestReport_2024-09-24.csv).

NOTE: The columns and entries in the CSV file can vary depending on the filters you've selected when you download the report.

After you finish

Approve or reject identity requests as required:

- [Approving identity requests in ClearID](#)

Browse

- [About identity requests report in ClearID](#)
- [Requesting identities in ClearID](#)

6 | Credential synchronization

6.1 | Configuring credential replication in ClearID

To replicate supported credentials across multiple Synergis™ systems, you must configure your credentials replication settings in the Genetec ClearID™ portal.

Before you begin

- [Learn about cardholder and identity relationships.](#)
- [Make sure that ClearID is managing your cardholder and credential changes.](#)

What you should know

Only an account administrator can configure credentials replication.

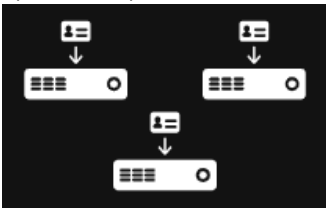
Credentials replication is intended to replicate *credentials* across two or more Synergis systems. For the replication functions to work, you must be using all the identity management functions provided by ClearID. Any credential changes that are only performed on a secondary system aren't replicated to the other systems.

NOTE: Credentials won't be sent to systems where cardholder and credential management is in read-only mode. In this situation, the access control system is highlighted in the ACS list with the Cardholder and credential management is disabled  icon.

Procedure

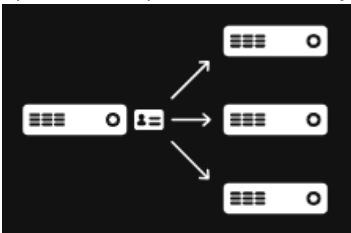
1. From the homepage, click Administration > Credentials.
2. In the Credential replication mode section, from the Mode list select a replication mode.

a. Option 1: No replication between access control systems.



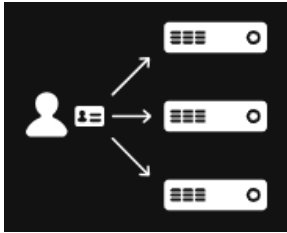
Each access control system operates independently, without synchronizing credentials with other systems. The credentials created in one system remain unique to that system, and aren't automatically synchronized or used in other systems.

b. Option 2: Use a specific access control system as the source of credentials synchronization.



Credential modifications performed in the selected access control system are synchronized to all other systems where the identity is associated with a cardholder.

c. Option 3: Use the system associated with the primary site of the identity as the source of credentials synchronization.



Credential modifications performed in the system associated with the primary site of the identity are replicated to all other systems where the identity is associated with a cardholder.

NOTE: If you selected No replication between access control systems, you can skip the following step.

3. In the Credential types and formats section, select the credential types that you want to synchronize.

NOTE: The credential options that are available for selection here varies depending on the credential information that is pulled in from your connected systems. Custom credentials are not supported.

- a. (Optional) If your organization has multiple formats, there might be situations where you only want to synchronize specific formats.

4. Click Save.

After you finish

(Optional) Do one or more of the following:

- Review the credential synchronization logs.
- Force a credentials synchronization.

6.2 | Viewing credential synchronization logs in ClearID

To check credential synchronization status or to review detailed information about the audit trail activities for all events related to credentials, view the credential synchronization logs in Genetec ClearID™.

Before you begin

Configure your credentials synchronization settings.

What you should know

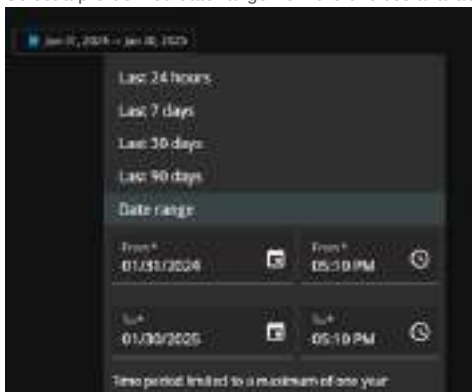
Only an account administrator can view the credential synchronization logs.

Procedure

1. From the homepage, click Administration > Credentials.
2. In the Credential replication logs section, click View logs.
3. (Optional) Use filters to help refine the log results based on one or more of the following criteria:

Date range

Select a pre-defined date range from the choices available or enter a specific date range using the date range picker.



Search field

In the search field, enter a search criteria.

Filter controls

Access control system

Search for an ACS system using its name or select one or more ACS systems from the list.

Associated identity

Search for an associated identity. For example, first name, last name, email, or a partial search string.

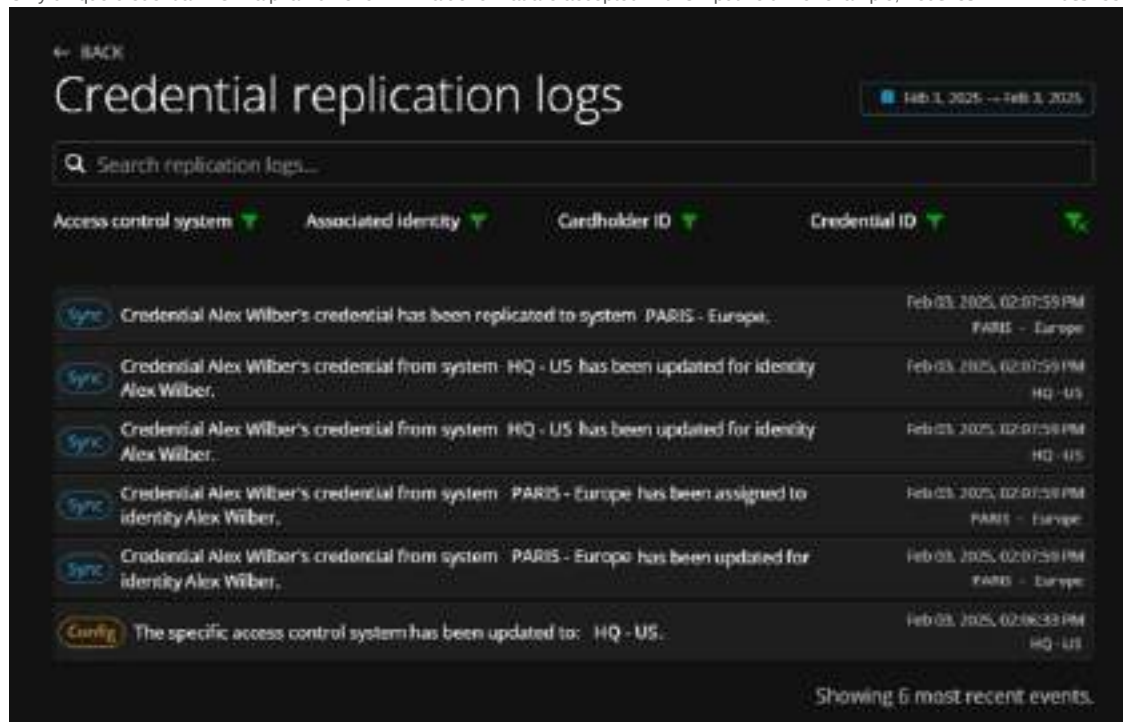
Cardholder ID

Only unique cardholder IDs in alpha-numeric HEX value format are accepted in this input field. For example, 29abdafb-f124-401a-b143-3c88556ec3c1.

NOTE: This filter is useful for users who primarily work with the information from Security Center.

Credential ID

Only unique credential IDs in alpha-numeric HEX value format are accepted in this input field. For example, fc6e4851-f429-40e5-bbe7-ba363c5cad1a.



After you finish

(Optional) Force a credentials synchronization.

6.3 | Forcing credential synchronization in ClearID

To resolve credential issues, you can force a synchronization to replace all credentials in Genetec ClearID. This force synchronization uses the latest values from your selected credential source and triggers the synchronization immediately.

Before you begin

- Configure your credential synchronization settings.
- (Optional) View the credential synchronization logs.

What you should know

Only an account administrator can force a credentials synchronization.

After credential synchronization settings have been configured, the synchronization is automatic.

- A forced synchronization can be used during initial setup as a preemptive measure to ensure that all credentials are propagated correctly.
- A forced synchronization is also used when the synchronization mode is updated from a specific system to the primary site option. Forcing the synchronization after a mode change ensures that the correct credentials are synchronized immediately to align with the selected mode.

Synchronization throughput is estimated at approximately 10 credentials a second. However, this throughput can vary depending on the machine running the Genetec ClearID™ plugin and the number of credentials assigned to identities.

If credential issues are encountered at a site contact the account administrator to view the logs, perform troubleshooting, and potentially force a synchronization.

NOTE: If you selected No replication between access control systems during your credentials synchronization configuration, the force synchronization function isn't available.

Procedure

1. From the homepage, click Administration > Credentials.
2. In the Force credential synchronization section, click Synchronize.
3. In the Synchronize dialog, click Synchronize.

The request to synchronize credentials is initiated and a Request to synchronize other systems sent successfully message is displayed.
IMPORTANT: No further progress is reported in the Credentials tab.

After you finish

Review the Credential replication logs to confirm that credentials information has been updated with the latest information.

7 | Managing sites

7.1 | About sites in ClearID

In Genetec ClearID™, a site is a logical entity. Sites include one or more areas. Each site and area can have a different owner.

A site typically represents either a building or a campus:

- If you have multiple buildings managed by one security team or one set of policies for visitors, consider setting them up using one site.
- Each site can have its own set of policies and site owners.
- If you have different buildings spread throughout a city, consider implementing one site per building.
- Multiple sites can be associated with the same Security Center access control system.

IMPORTANT: Your implementation choices can affect the Genetec ClearID™ solution costs. These costs can vary depending on the implemented functions, the number of identities, and the number of sites.

7.2 | Creating sites in ClearID

Before you can configure your areas in Genetec ClearID™, you must create the sites that you want to associate your areas with.

Before you begin

- [Add your systems.](#)

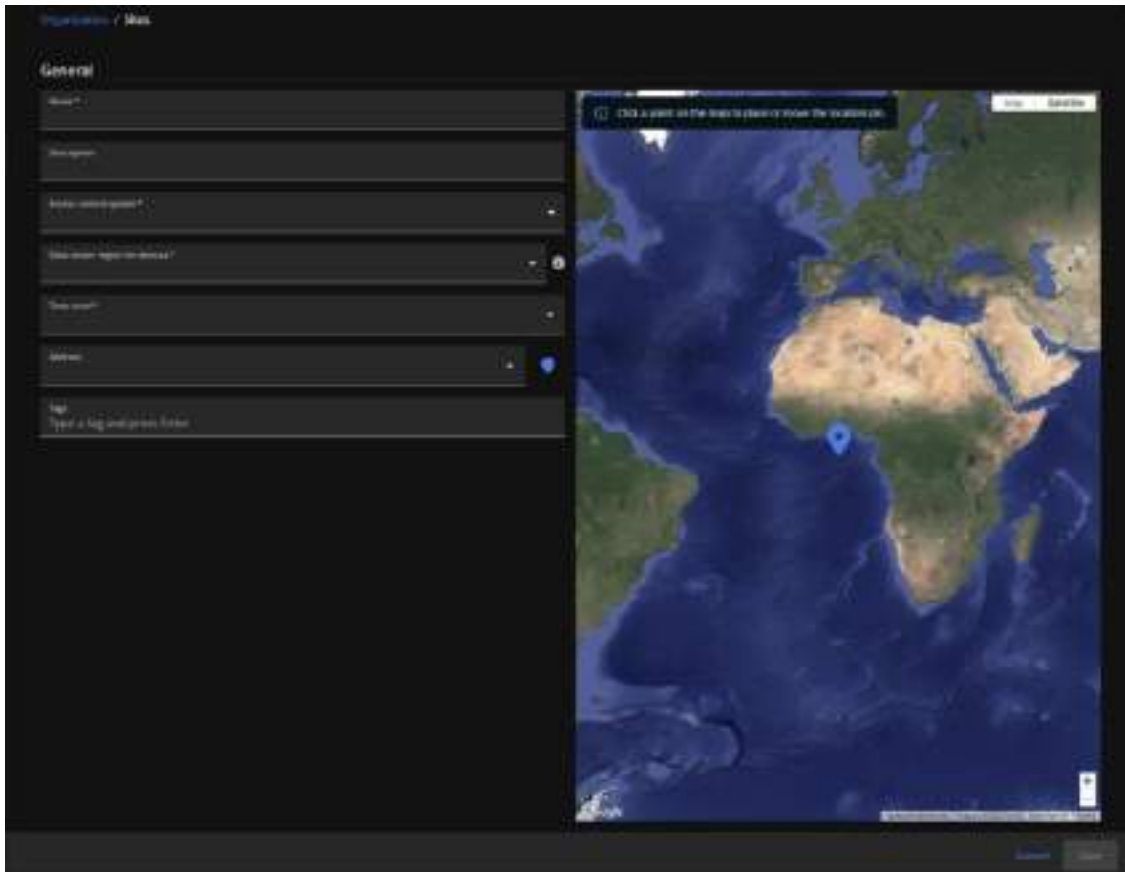
What you should know

To create sites in ClearID, you must be an *Account administrator*.

- An *Account administrator* can choose the *Site owners* and configure visitor management for the site.
- A *site* is associated with a Security Center access control system.
- Multiple sites can be associated with the same Security Center access control system.

Procedure

1. Click Organization > Sites.
2. Click Add site.



3. On the General page, complete the fields.

NOTE: Mandatory fields are highlighted in the user interface with an asterisk (*).

Name

Enter a name for your site.

Description

Enter a description that indicates the geographical location of the building or physical location of the site.

Access control system

Select the system that you require from the Access control system list.

NOTE: This access control system is used to synchronize changes in ClearID back to Security Center.

Data center region for devices

Select a data center region from the drop-down. This option is typically set to the data center region closest to where the device will be used. The data center region is used for device communications.

NOTE: This setting is permanent and can't be changed after the site is created. The data center option isn't available if your account is deployed in the Europe only architecture.

Time zone

Select a time zone from the drop-down. The time zone options are represented using the Internet Assigned Numbers Authority (IANA) format.

NOTE: When an access request or visitor request is made from anywhere in the world, the time zone of the requested site access or visit is used to ensure that the correct date and times are applied to the request.

Address

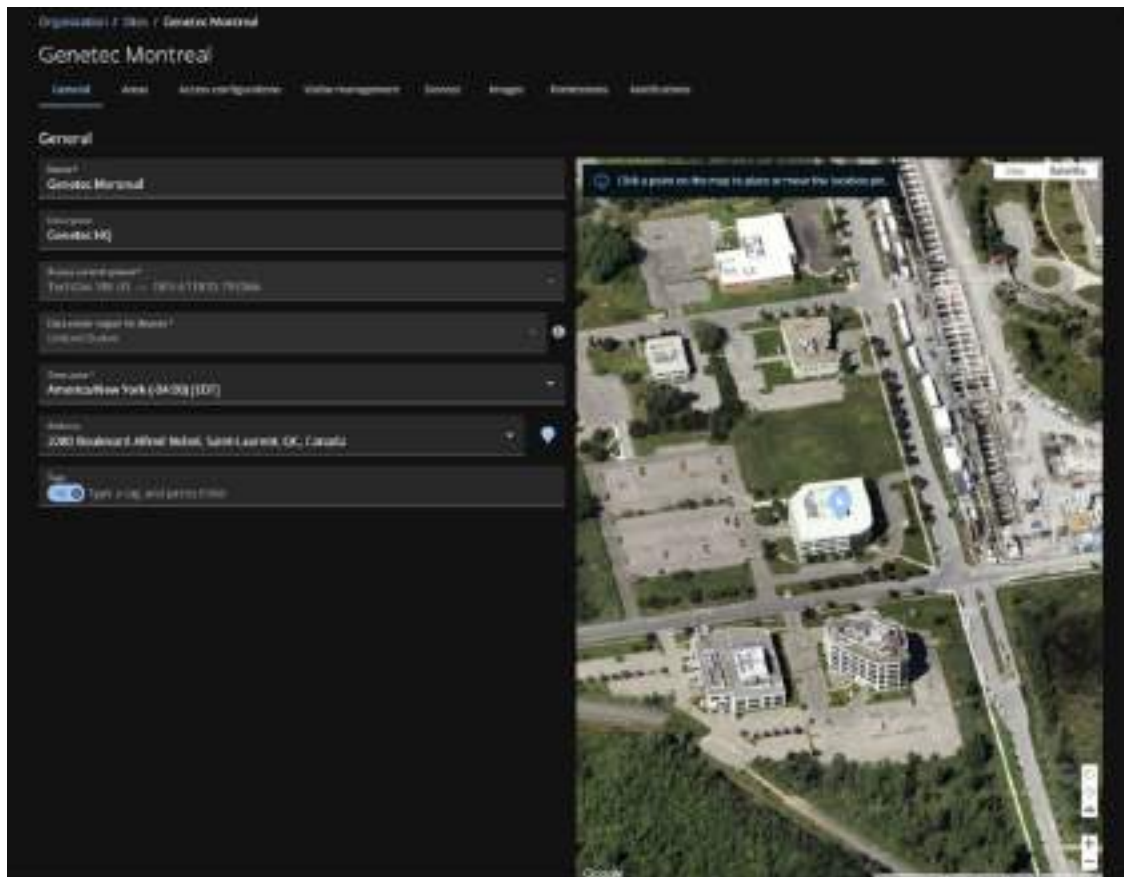
Enter an address for the site. As you type, Google Maps integration auto-complete processes the information and displays available addresses.

Center map

Click  to find the address on the map, and center the map on that address.

Tags

Enter alternative keywords or search term categorizations that might be used to find the site.



4. On the Notifications page, complete the fields.

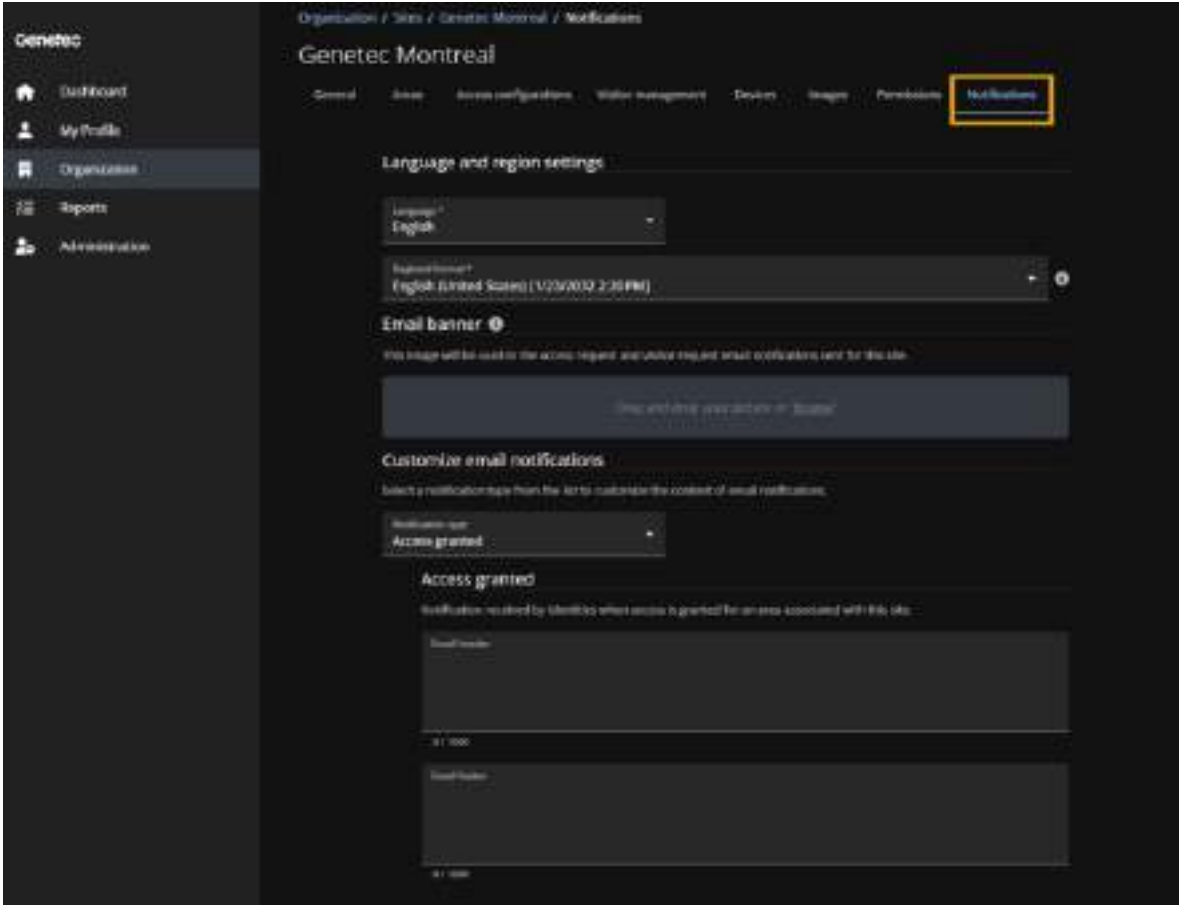
Language

Select a notification language from the drop-down. This setting is used for email notifications and SMS alerts. The notifications language selection is unique to a site and you can choose from English, French, Spanish, Portuguese, Italian, German, Dutch, and Japanese.

Regional format

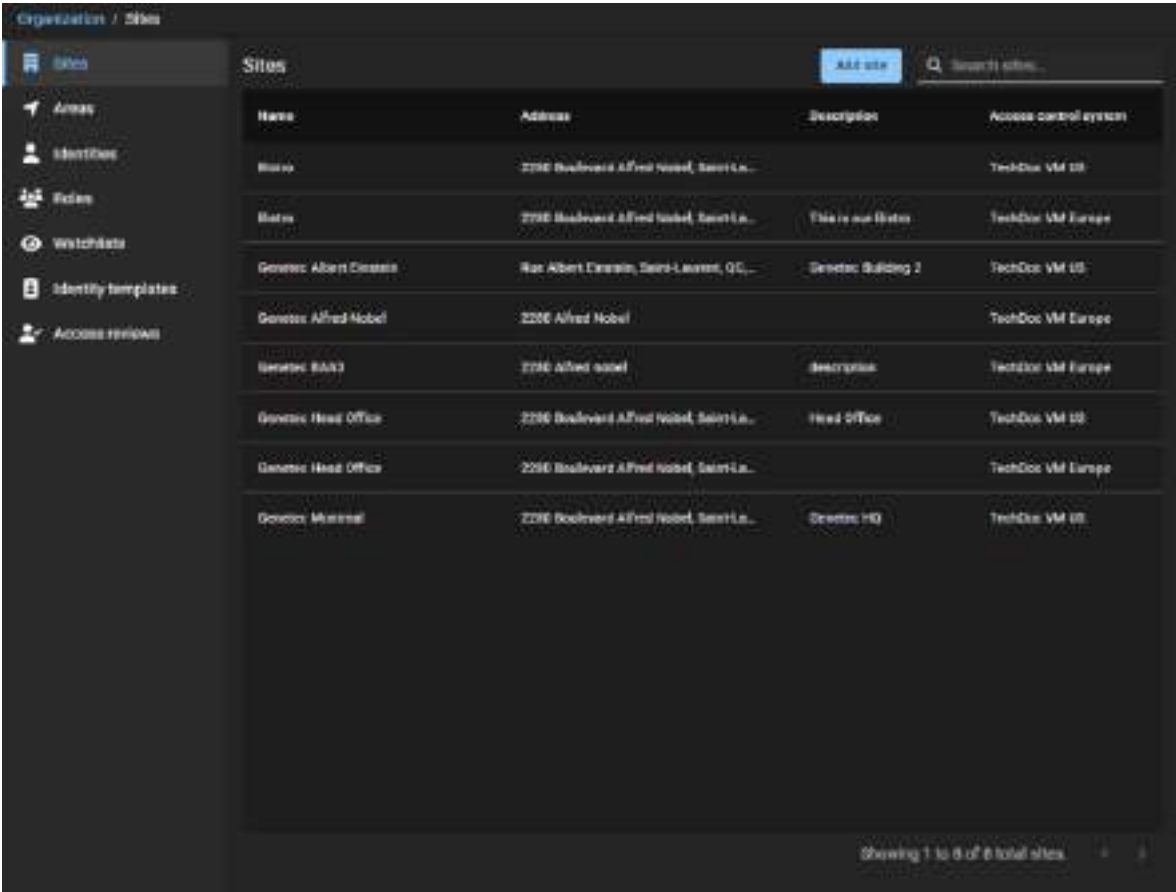
Select a regional date and time format to use in email notifications for this site. The default regional format is American English (en-us). For example, 1/23/2032 2:20 PM.

5. Click Save.



Results

Your site has been created in ClearID.



After you finish

Add your site owners.
Browse

- [Modifying sites in ClearID](#)

Browse

- [IANA Time Zone Database](#)

7.2.1 | Adding site owners in ClearID

In Genetec ClearID™, a site owner is an identity that has authority over areas associated with a specific site. Before you can assign or modify area owners, configure specific area settings that are exclusive to site owners, or manage site access reviews you must add your site owners.

Before you begin

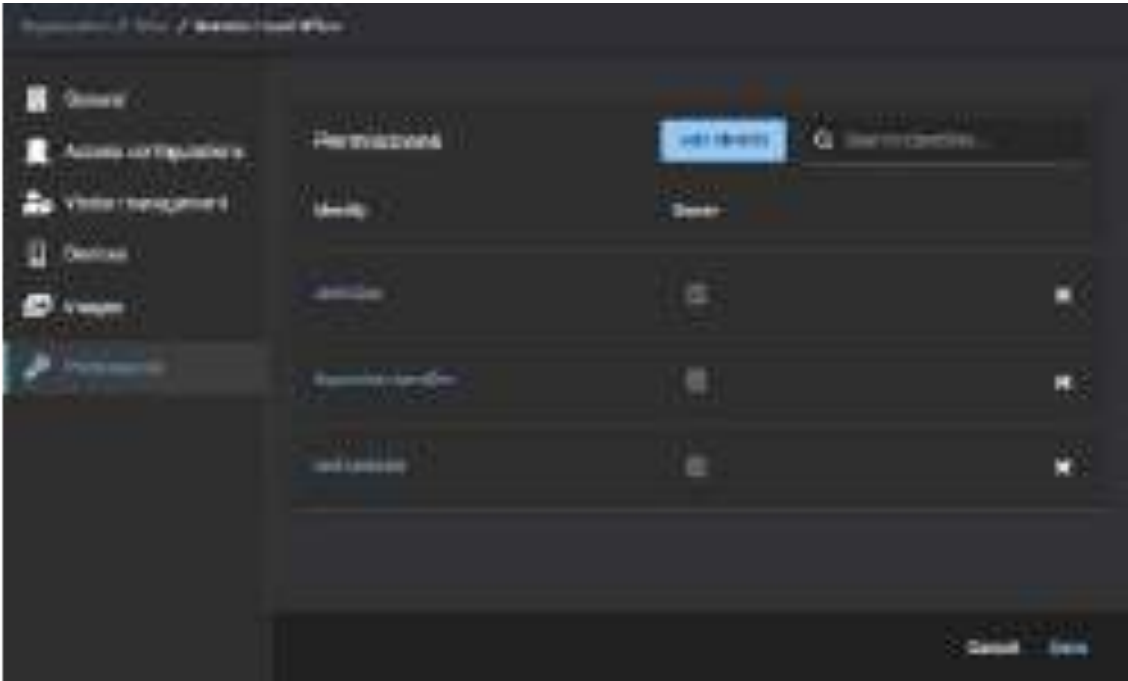
Create your sites.

What you should know

To add site owners in ClearID, you must be an account administrator.

Procedure

1. Click Organization > Sites.
2. Select your site and click Permissions.
3. Click Add identity to add site owners to the site Permissions list.



- a. Search for or select the identities that you require and click Add.
Tip: Click the identity hyperlink in the Identity column to review identity details (company, department, home site, supervisor, and email) and to verify that you have the correct identities in the list.
 - b. (Optional) Click  to remove any site owner permissions that are no longer required.
4. Click Save.

After you finish

Create your areas
Parent topic: [Creating sites in ClearID](#)

7.2.2 | Enabling visitor management for sites in ClearID

Before users can invite visitors, you must configure the visitor management settings for your site.

Before you begin

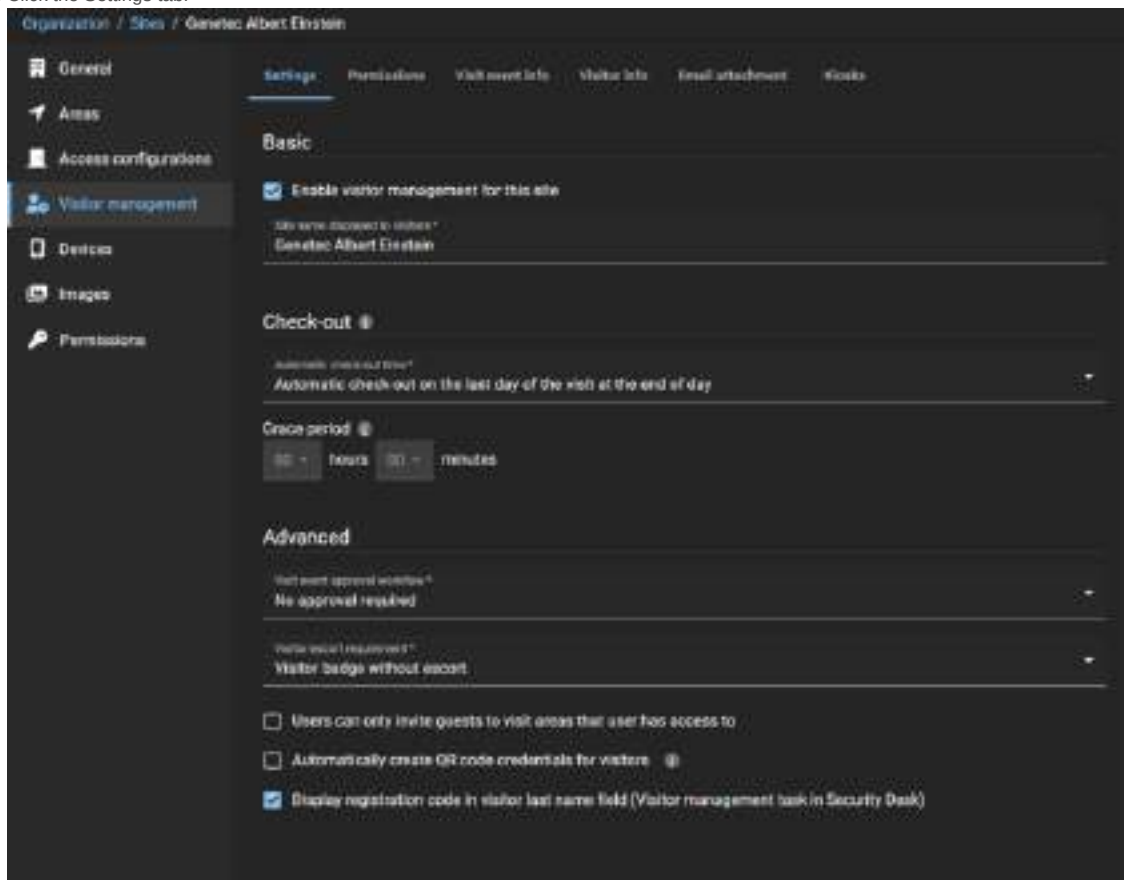
Create your sites.

What you should know

- Visitor management is disabled by default.
- Only account administrators or *site owners* can enable or configure visitor management for sites in Genetec ClearID™.
- The options displayed when a visit request is created vary depending on the users requesting access and also the settings that you configure here.
- Only account administrators can grant user permissions to invite visitors using roles.
- Users are automatically granted *Invite visitors* permissions for their home site by default.

Procedure

1. Click Organization > Sites.
2. Search for and select a site.
3. Click Visitor management to configure the visitor management options for a site.
4. Click the Settings tab.



- a. In the Basic section, configure the options you require:

Enable visitor management for this site

Select this checkbox to enable visitor management for this site.

Site name displayed to visitors

Enter the site name that you want displayed externally to visitors.

- b. In the Check-out section, configure the options you require:

Automatic check-out time

Automatic check-out on the last day of the visit at the end of the day

The visitor is checked out automatically on the last day of the visit at midnight.

Automatic check-out at the scheduled visit end time

The visitor is checked out at the specified visit end time.

NOTE: Visitor's temporary access rights and QR code credential are deactivated during automatic check-out. If a grace period is activated, visitors are checked out after the additional grace period lapses after the visit end time.

Grace period

Adds extra time to the scheduled end time of the visit event. After the grace period lapses, the visitor is checked out.

- c. (Optional) In the Advanced section, configure the options you require:

Visit event approval workflow

Select the approval workflow that you require:

No approval required

No approval is required to complete visit event approval. For example, to simplify employees inviting visitors at any time.

Supervisor approval required

Supervisor approval is required to complete visit event approval.

Visit event approver approval required

Visit event approver approval is required to complete visit event approval.

NOTE: If an area is selected during the visit event creation, it can trigger its own approval workflow.

Visit escort requirement

Select the badge type that you require:

Visitor badge without escort

Typically used for visitors who do not require an escort and who do not need door access to secure or sensitive areas.

Visitor badge with escort

Typically used for visitors who do require an escort or who need door access to secure or sensitive areas.

NOTE: The visitor escort rule must also be turned on for the areas in Synergis™ to enforce the visitor escort rule. For the escort function to work properly, the Cardholder groups can escort visitors option must also be enabled in the General settings of the Access control task in Config Tool.

Users can only invite guests to visit areas that they have access to

- If the checkbox is selected, users can only invite guests to visit areas that the requesting user has access to. This setting is enforced when a guest visit request is created.
- If the checkbox is cleared, users can invite guests to visit any area in ClearID that allows visitors.

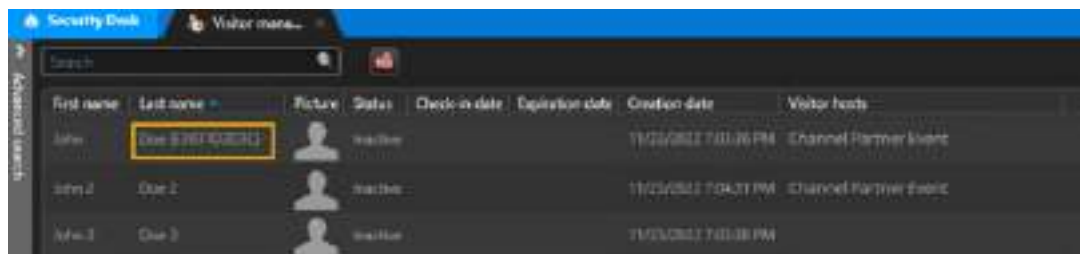
Automatically create QR code credentials for visitors

If the checkbox is selected, ClearID automatically creates a QR code credential for visitors when a visit request is created. Visitors can then use the QR code contained in the visitor confirmation email to access specific parking entrances, turnstiles, or gated facilities. The QR code can also be used during check-in with security, at a reception, or at a Genetec ClearID™ Self-Service Kiosk.

Display registration code in visitor last name field (Visitor management task in Security Desk)

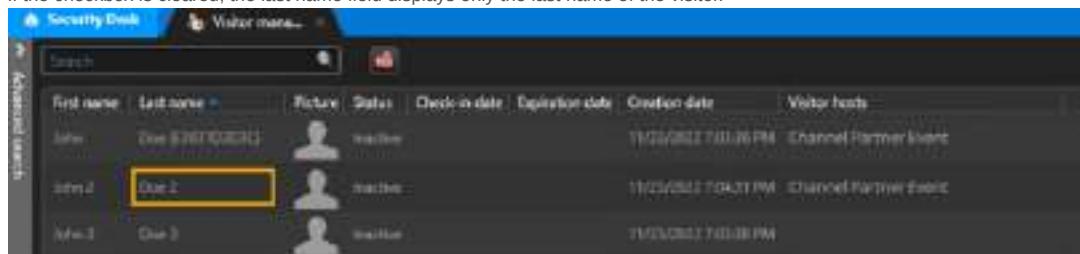
- If the checkbox is selected, the last name field displays the last name of the visitor and the QR code value. This checkbox is selected by default.

The checkbox must be selected for a QR code scanner to successfully scan and locate a pre-registered visitor in Security Desk.



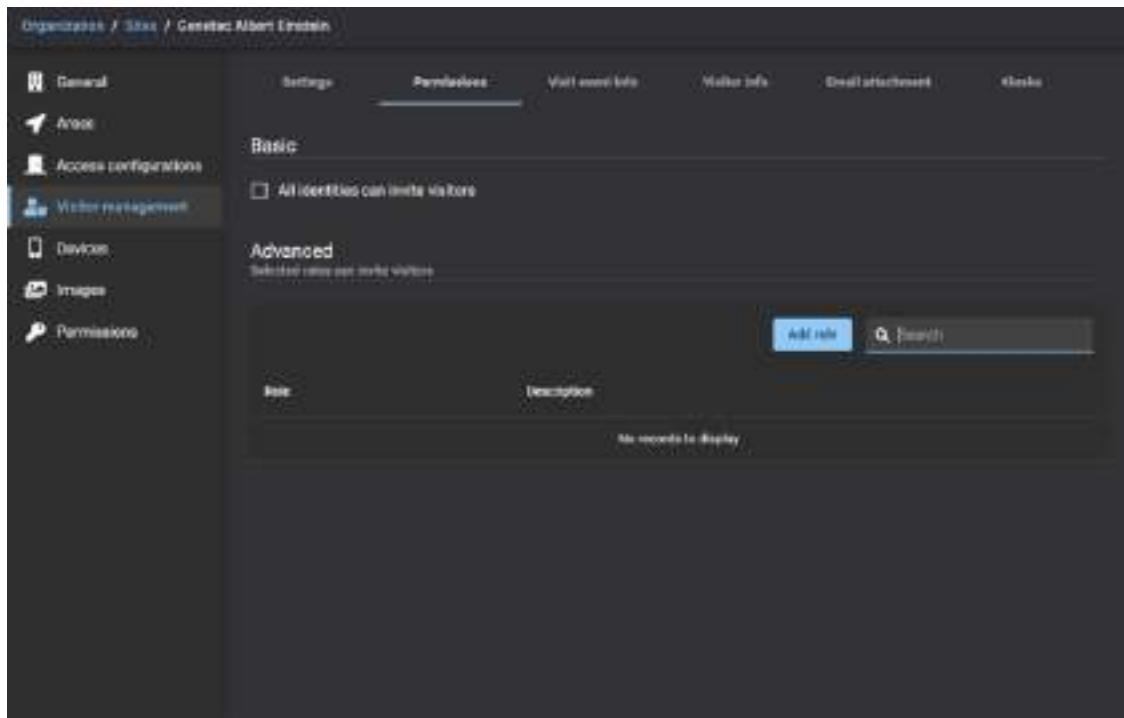
Tip: You can use a Zebra QR code scanner to enter the QR code in the Last name field for you. In the Visitor management task in Security Desk, click in the Search field, scan the QR code and press Enter.

- If the checkbox is cleared, the last name field displays only the last name of the visitor.



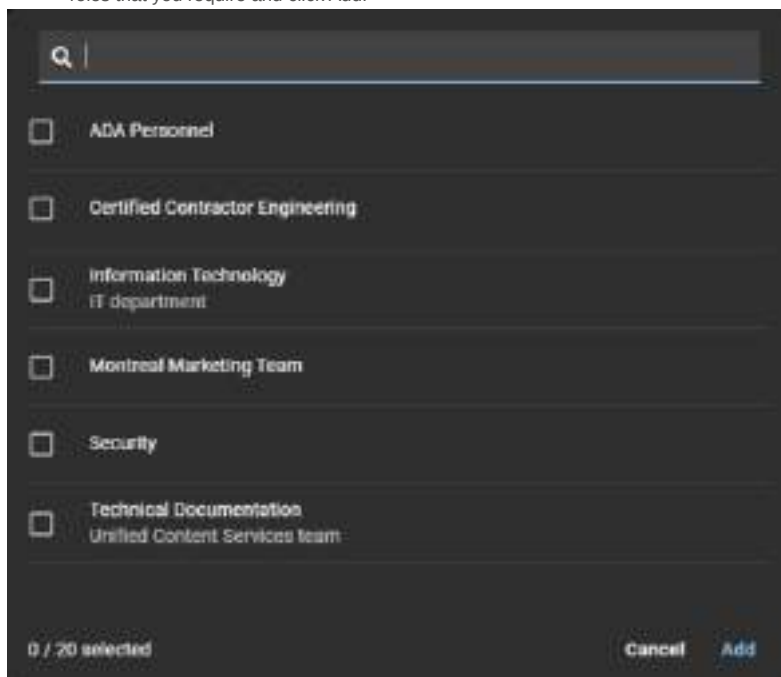
NOTE: When the registration code option is changed, only visitors created after the change are modified, previously created visitors remain unchanged.

5. (Optional) Click the Permissions tab.



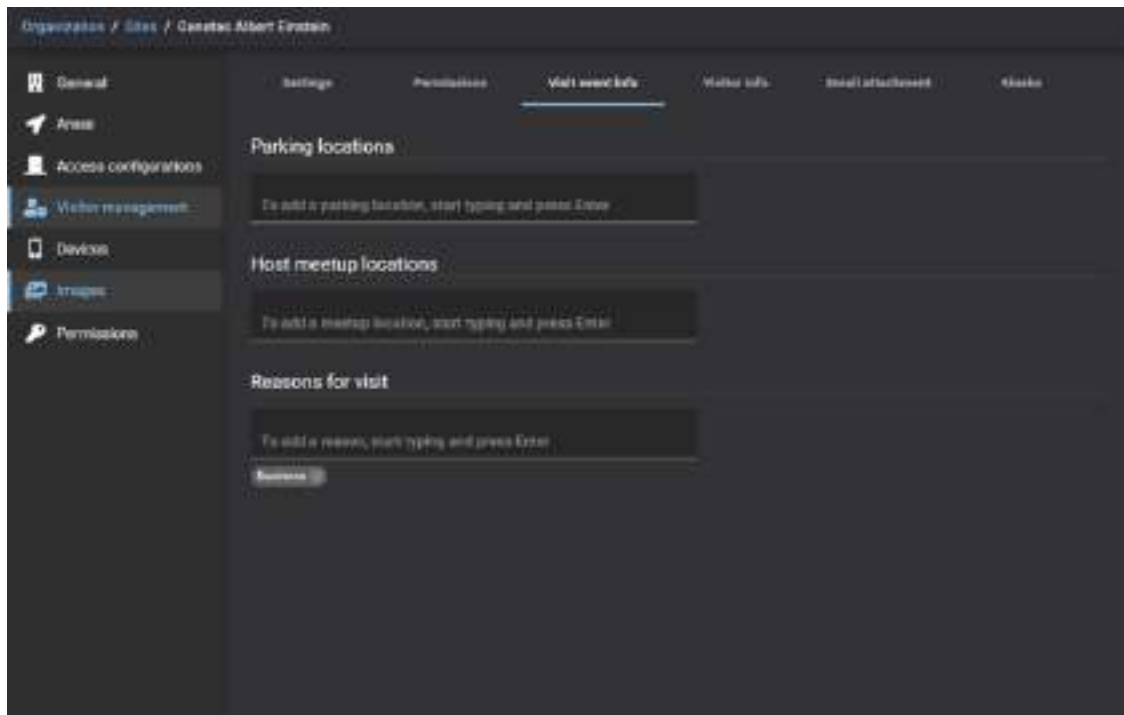
Do one of the following:

- In the Basic section, select the All identities can invite visitors checkbox if you want all identities to be able to invite visitors to this site.
- In the Advanced section, click Add role if you want to use roles to manage who can invite visitors to this site. You can then search for or select the roles that you require and click Add.



Tip: When adding new role permissions, advise role members to log off and log on, if they want to load the new visitor invite permissions immediately.

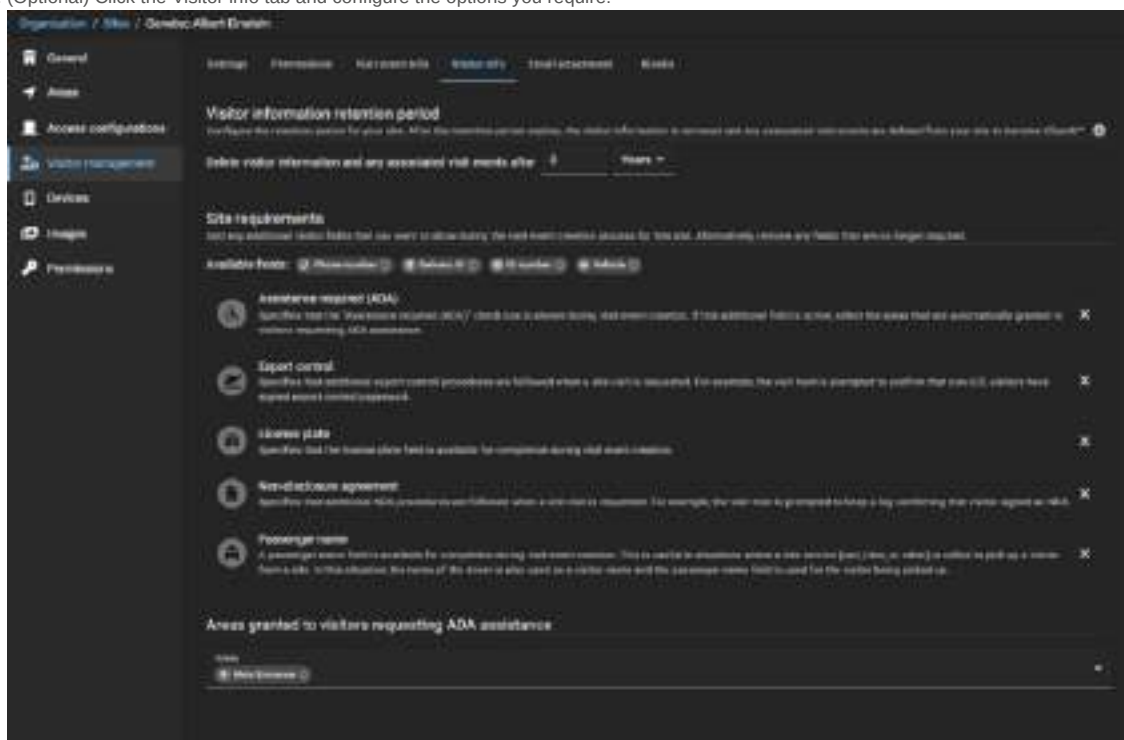
6. (Optional) Click the Visit event info tab and configure the options you require:



- a. In the Parking locations section, add parking locations.
- b. In the Host meetup locations section, add meetup locations.
- c. In the Reasons for visit section, add the typical reasons for visits to your site.

For example, customer meeting, partner meeting, job interview, delivery, taxi pickup, Uber pickup, lift pickup, and so on.

7. (Optional) Click the Visitor info tab and configure the options you require:

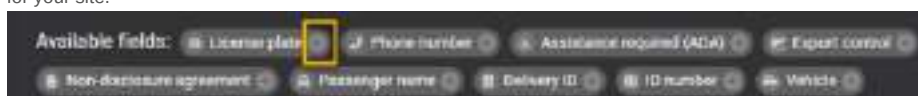


- a. In the Visitor information retention period section, select a retention period in days, months, or years.

The default retention period is 1 year and the maximum is 3 years.

NOTE: The retention period is configurable by site to comply with the different data laws that might apply in your region.

- b. In the Site requirements Available fields section, click  to add each additional field that you want to include during the visit event creation process for your site.



License plate

If selected, a license plate field is provided when a site visit is requested.

Phone number

If selected, a phone number field is provided when a site visit is requested.

Genetec ClearID®; User Guide

Displayed in the header

Assistance required (ADA)

If selected, an Areas granted to visitors requesting ADA assistance section is displayed.

NOTE: This assistance option is used to comply with the Americans with Disabilities Act (ADA).

Export control required

If selected, additional export control procedures are followed when a site visit is requested. For example, the visit host is prompted to confirm that non-U.S. visitors have signed export control paperwork.

Non-disclosure agreement

If selected, additional NDA procedures are followed when a site visit is requested. For example, the visit host is prompted to keep a log confirming that the visitor signed an NDA.

Passenger name

If selected, a passenger name field is provided when a site visit is requested. This passenger name field is useful in situations where a ride service (taxi, Uber, or other) is called to pick up a visitor from a site. In this situation, the name of the driver is also used as a visitor name and the passenger name field is used for the visitor being picked up.

Delivery ID

If selected, a delivery ID field is provided when a site visit is requested.

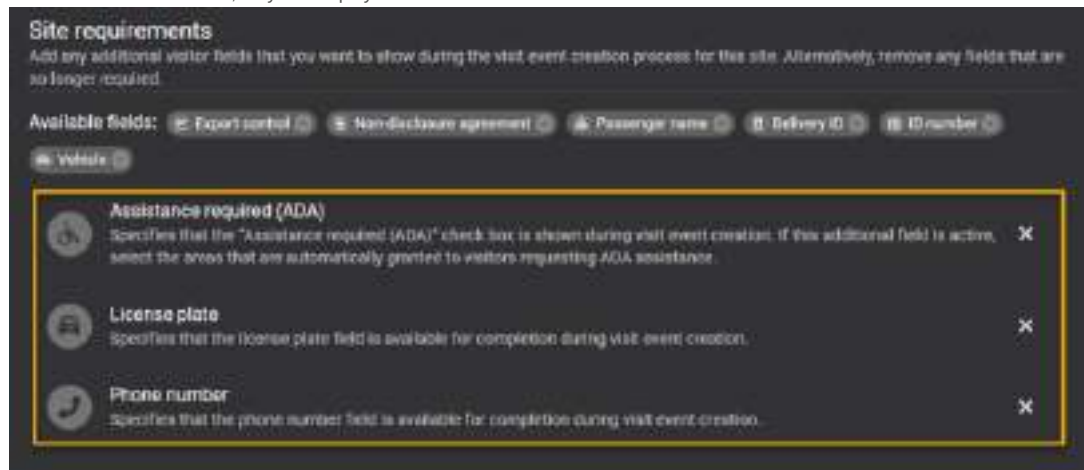
ID number

If selected, an ID number field is provided when a site visit is requested.

Vehicle

If selected, an extra expected vehicle details field is provided when a site visit is requested.

NOTE: As fields are added, they are displayed in the Available fields later in the section.



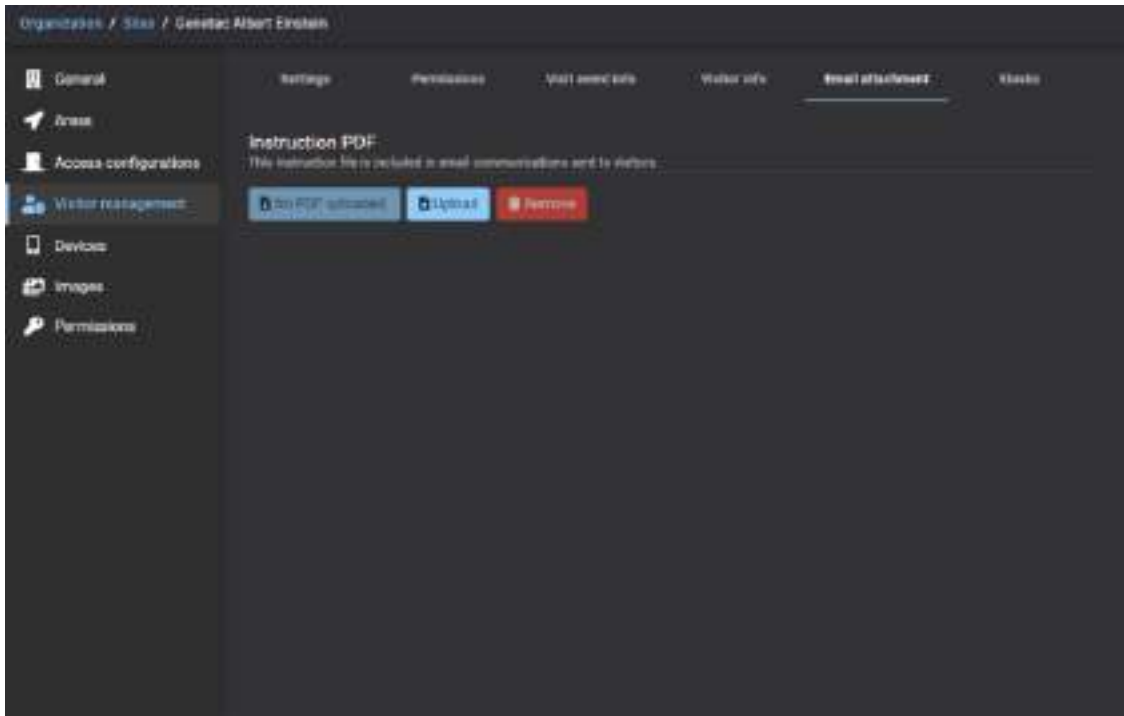
- c. (Optional) If you added Assistance required (ADA) to your site requirements, in the Areas granted to visitors requesting ADA assistance section, add areas that should automatically be granted to visitors requesting ADA assistance.

NOTE: When an employee invites a visitor that requires accessibility assistance to the site, the visitor is automatically added to the list of ADA areas.

For example, If there is a special door for wheelchair access, the people responsible for the site or facilities add that door for wheelchair access in a specific area and add the area to the list of areas granted to visitors that request ADA assistance. If a visitor checks in with ADA enabled, ClearID grants the visitor access to this door, but not other visitors.

- d. (Optional) Click  to remove any visitor fields that are no longer required.

8. Click the Email attachment tab and select the options you require:



Instruction PDF

This instruction file is used if you want to automatically include a Visit Instructions File PDF in email communications with visitors. For example, location details, site map, travel instructions, and so on. Regardless of the uploaded file name, the downloadable instruction file is saved as VisitInstructionsFile.pdf.

No PDF uploaded

Indicates that no Instruction PDF has been uploaded yet.

VisitInstructionsFile.pdf

Click to download a copy of the VisitInstructionsFile.pdf.

NOTE: This button is only visible and active after an Instruction PDF has been uploaded.

Upload

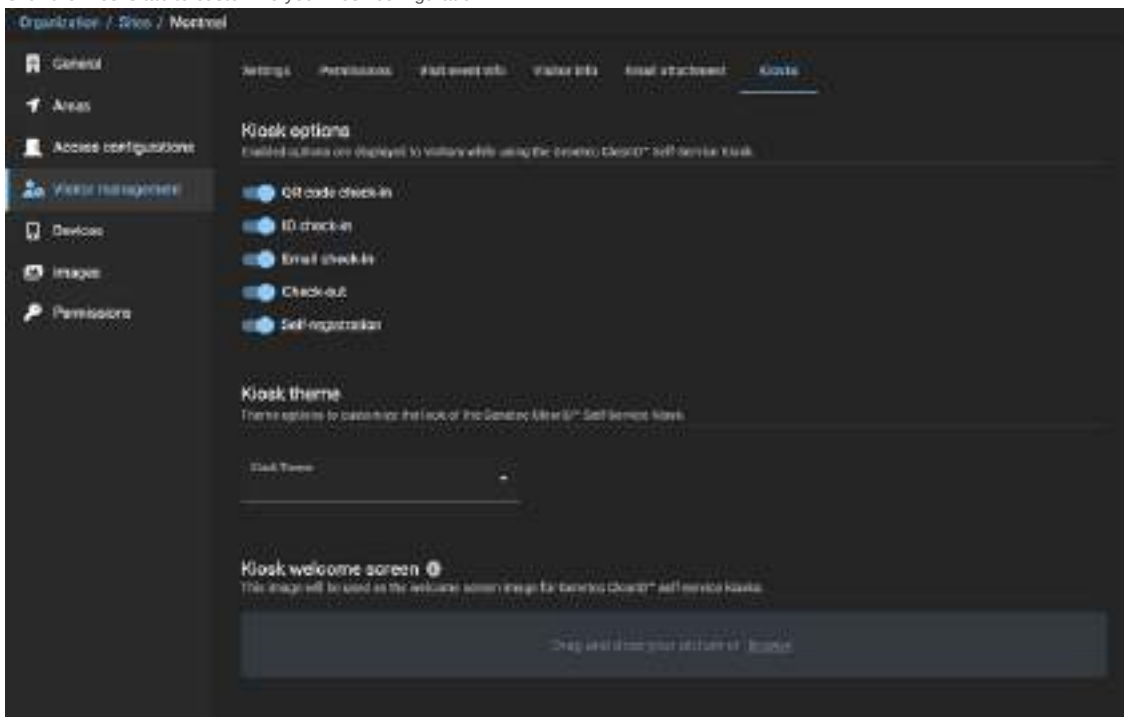
Click to upload a PDF instruction file.

Best Practice: If your instruction file is a word document, click Save as Adobe PDF before uploading to ensure that visitors cannot modify the procedure.

Remove

Click to remove a Visit Instructions File PDF from email communications with visitors.

9. Click the Kiosks tab to customize your kiosk configuration.

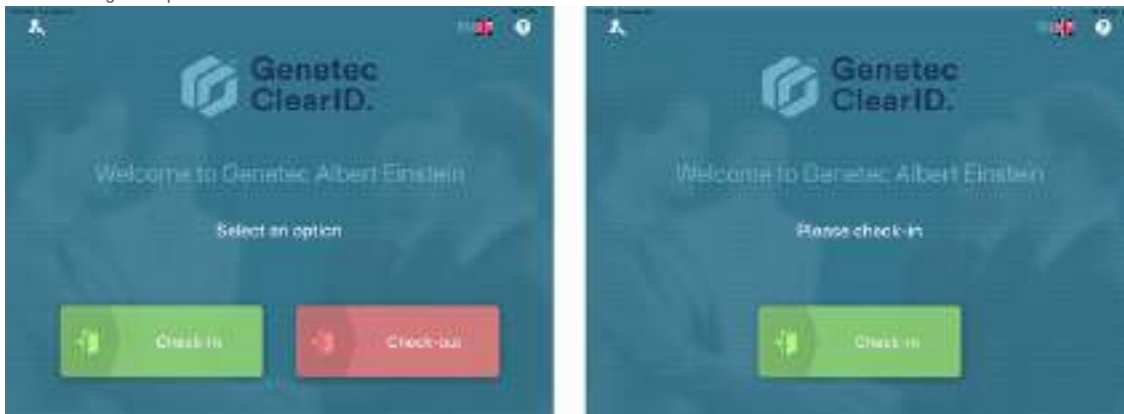


10. (Optional) Customize the Kiosk options.

These options customize the choices that are displayed to your visitors on your ClearID Self-Service Kiosk during the check-in or check-out process.

NOTE: The self-registration option is only displayed when all other check-in options are not applicable.

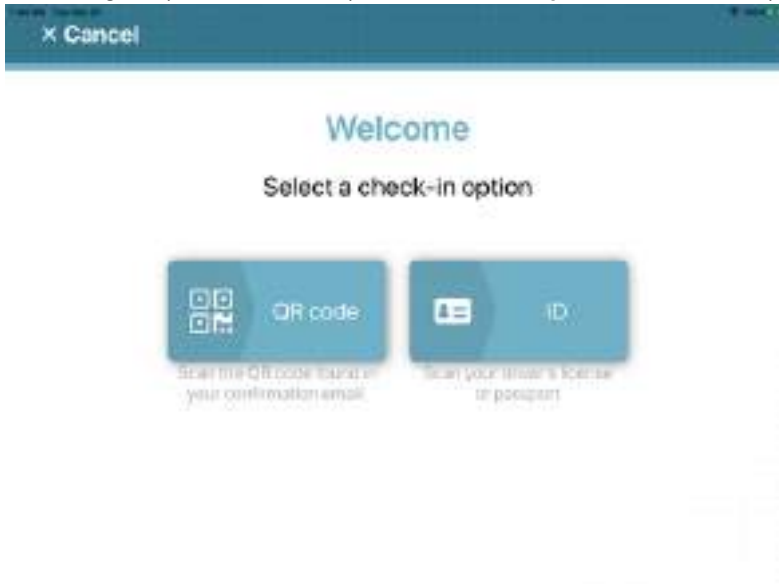
The following example shows the initial check-in or check-out screen customized for two different scenarios.



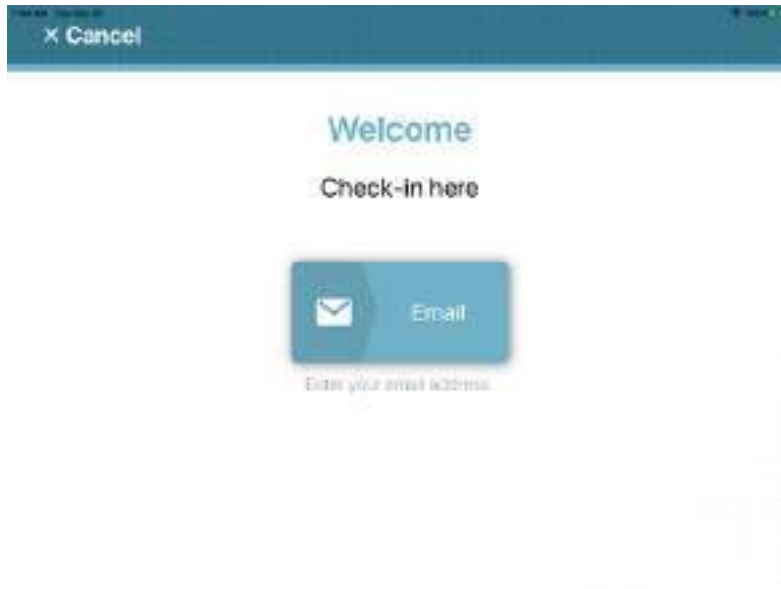
The following example shows the Kiosk options customized with QR code, ID, and Email check-in options enabled.



The following example shows the Kiosk options customized with QR code and ID check-in options enabled.



The following example shows the Kiosk options customized with only the Email check-in option enabled.



11. (Optional) Customize the Kiosk theme.

a. In the Kiosk theme section, choose a theme from the following:

ClearID

The ClearID theme (HEX color code 35768D) has no accent color.

White

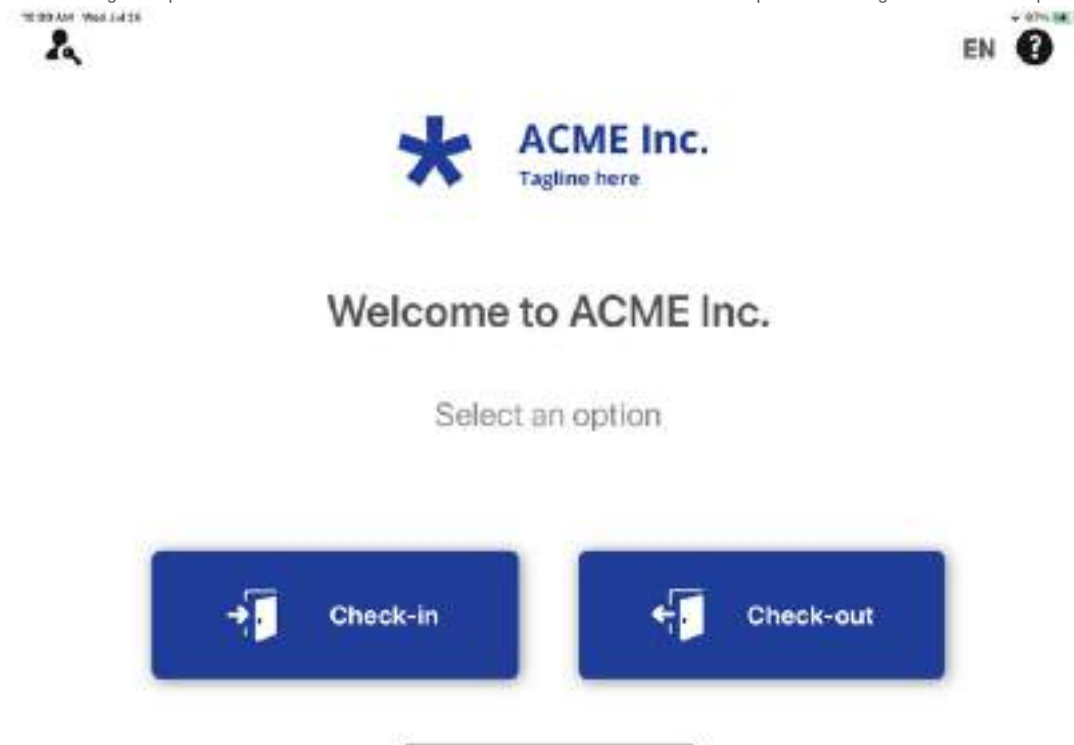
The white theme includes extra controls to pick an accent color. For example, to align with your corporate branding.

b. If you chose the White kiosk theme, select an accent color.

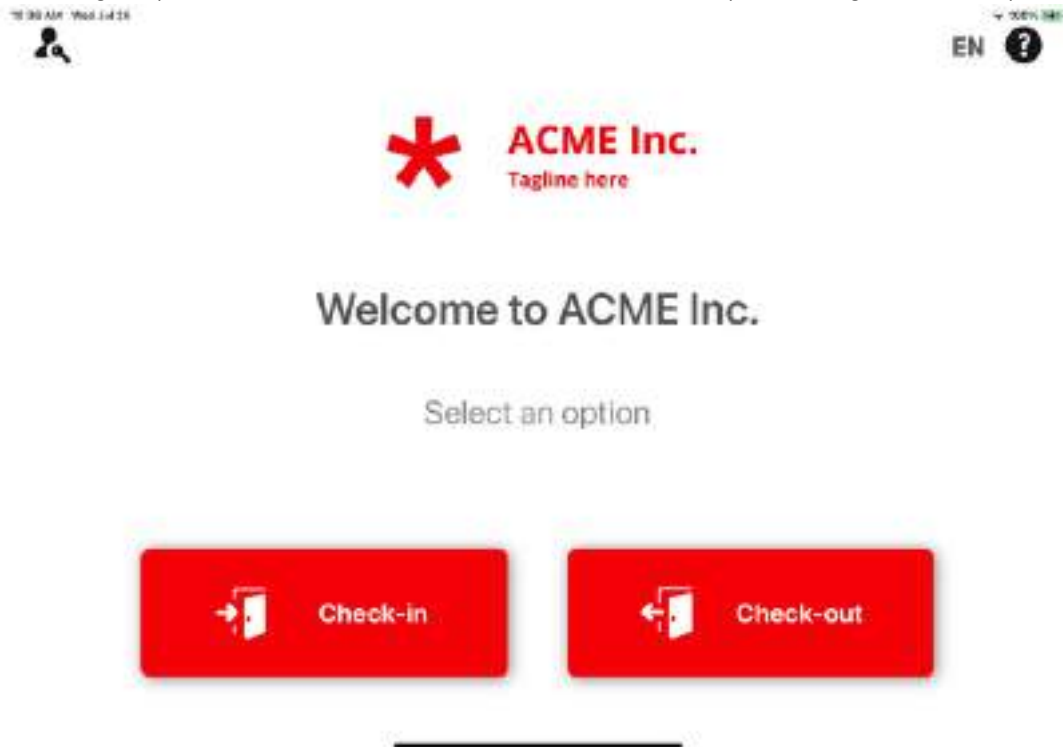


The accent color is applied to the buttons displayed on the ClearID Self-Service Kiosk.

The following example shows the white theme with blue accent color to match the blue corporate branding seen in the example.



The following example shows the white theme with red accent color to match the red corporate branding seen in the example.



12. (Optional) Customize the Kiosk welcome screen.

- a. In the Kiosk welcome screen section, drag and drop your picture or browse to select a Kiosk welcome screen image. This image is used as the welcome screen *company name* or *logo* for the kiosk.

The following example shows the welcome screen with a custom logo image.



13. Click Save.

NOTE: Kiosk options changes are synchronized with your kiosk every 60 seconds.

Results

Visitor management is enabled for the site.

After you finish

Submit an access request or visit request for this site.

Parent topic: Creating sites in ClearID

Browse

- [Introduction to the ADA](#)
- [Visit Instructions file \(Example PDF\)](#)

Browse

- [About workflows in ClearID](#)
- [Inviting visitors in ClearID](#)
- [About ClearID Self-Service Kiosk check-in](#)
- [Enabling QR code credentials for visitors in ClearID](#)

7.2.2.1 | [Viewing sites where a user can invite visitors](#)

[Creating sites in ClearID](#) >

An account administrator might need to view the list of sites where a user can invite visitors so that they can verify or update access if required.

Before you begin

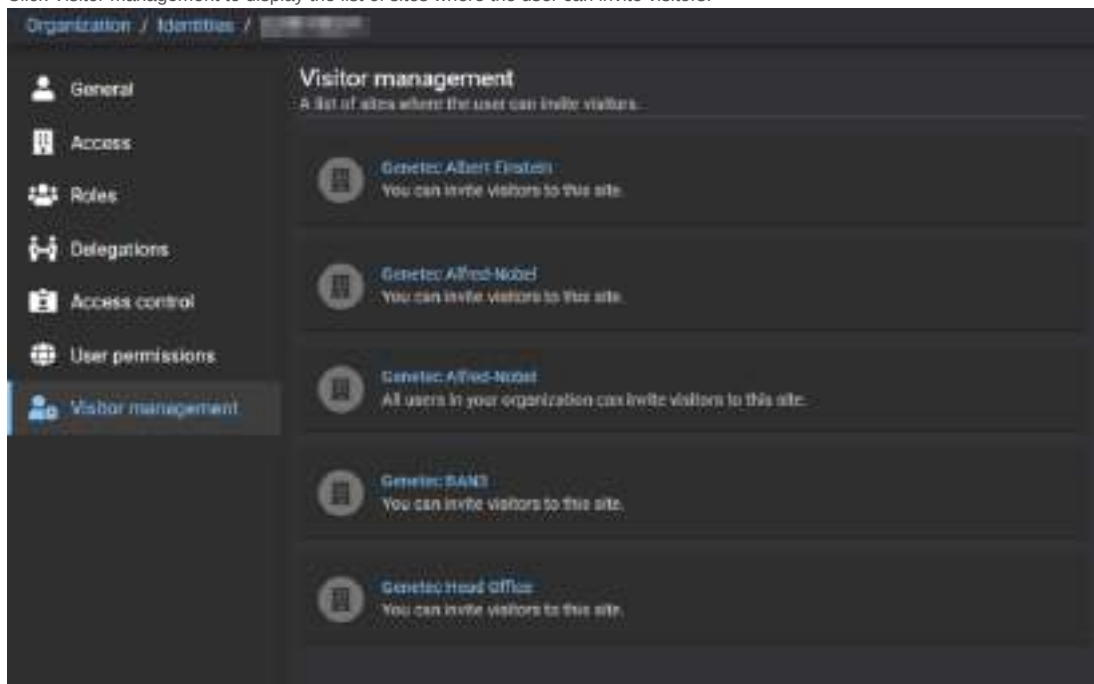
- [Configure your visitor management settings.](#)
- [Add your role members.](#)

What you should know

- Only account administrators can view the list of sites where a user can invite visitors or grant user permissions to invite visitors using roles.
- Users are automatically granted *Invite visitors* permissions for their home site by default.

Procedure

1. From the Home page, click [Organization](#) > [Identities](#).
2. Search for or select a user.
3. Click [Visitor management](#) to display the list of sites where the user can invite visitors.



Parent topic: [Enabling visitor management for sites in ClearID](#)

Browse

- [Granting access to the ClearID web portal](#)

7.3 | [Modifying sites in ClearID](#)

After you add your sites, you can modify the settings of each site individually. An *Account administrator* or *Site owner* can modify the *Site owners*, site properties, and change visitor management options for the site.

Before you begin

Create your sites.

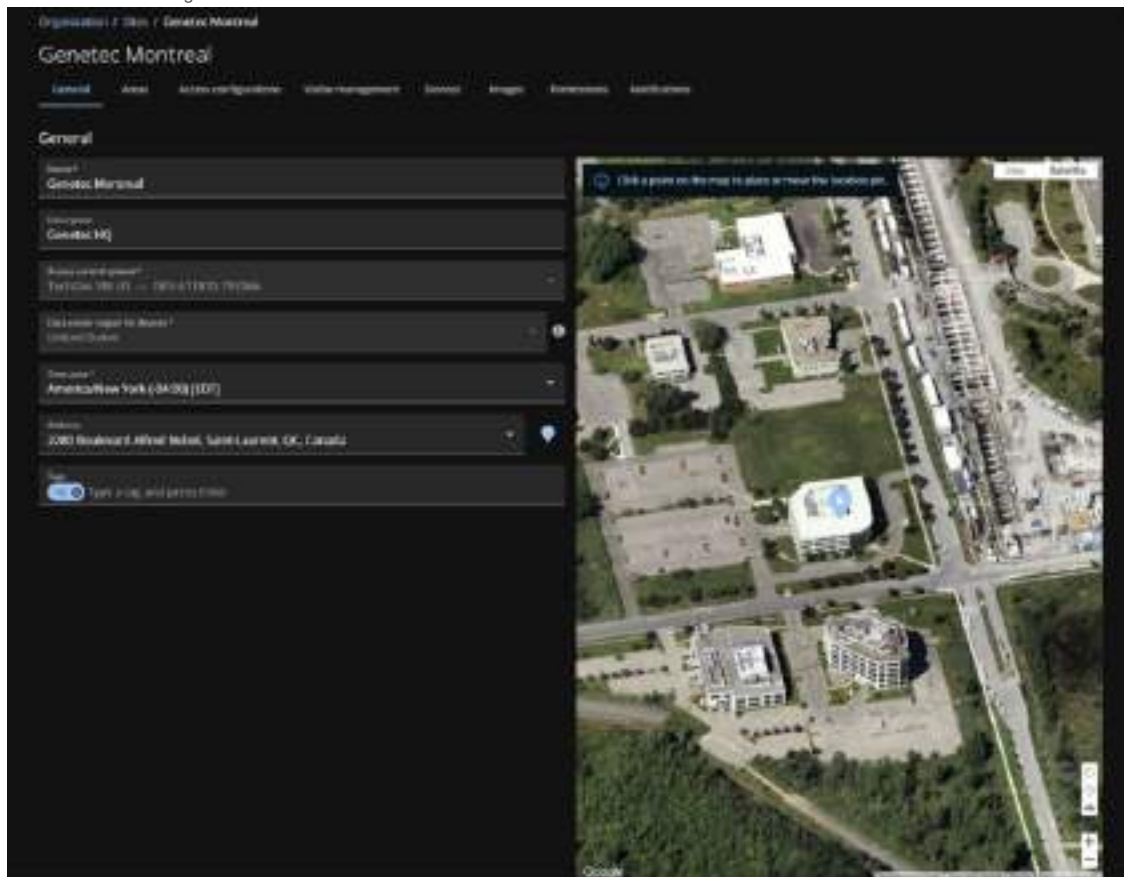
What you should know

To modify sites in Genetec ClearID™, you must be an *Account administrator* or *Site owner*.

- A *site* is associated with a Security Center access control system.
- Multiple sites can be associated with the same Security Center access control system.

Procedure

1. Click Organization > Sites.
2. Search for a site using the search field or select a site from the Site list.



3. On the General page, modify the fields as required.
4. On the Notifications page, modify the fields as required.
5. Click Save.

Results

Your site settings have been changed.

Browse

- [Creating sites in ClearID](#)

7.4 | Setting a maximum duration for site access in ClearID

To enforce a limit for identities with temporary access, you can set a site access duration. When the maximum duration limit is reached, their access expires.

What you should know

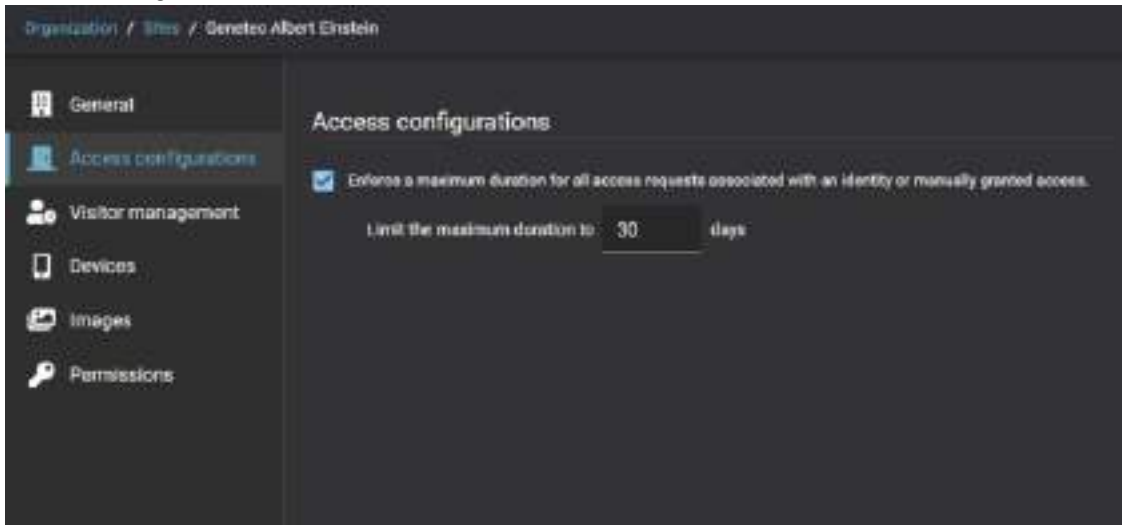
If the maximum duration for site access function has been activated for your account, the maximum duration limit for site access is enabled by default.

- To set a maximum duration period for site access in Genetec ClearID™, you must be a site owner.
- This access duration period only applies to individual identities or access that was manually granted.
- This access duration period does not apply to role access.

Tip: Use role groups when you have people who require permanent access to a site.

Procedure

1. Click Organization > Sites.
2. Search for and select a site.
3. Click Access configurations.



- a. Select the Enforce a maximum duration for all access requests associated with an identity or manually granted access checkbox.
- b. In the Limit the maximum duration to field, enter the maximum duration in days.
You can enter a value in days from 1 to 365. The default value is 30 days.

Browse

- [Adding roles in ClearID](#)
- [Adding role members in ClearID](#)
- [Requesting access in ClearID](#)

7.5 | Configuring access request documents for sites in ClearID

For sites with extra security measures or requirements, *Site owners* can make it mandatory for employees to upload supporting documents like copies of drivers licenses or certifications when requesting access to areas.

Before you begin

Familiarize yourself with [access request workflows](#).

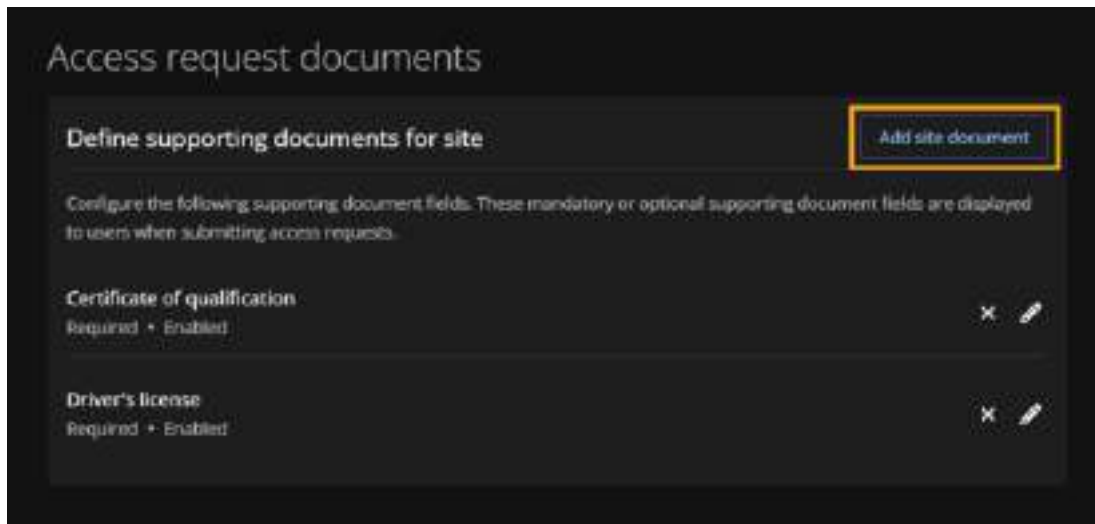
What you should know

- You must be a *Site owner* to configure mandatory or optional supporting documents for access requests at the site level.
- You can configure up to 20 supporting document types per site.

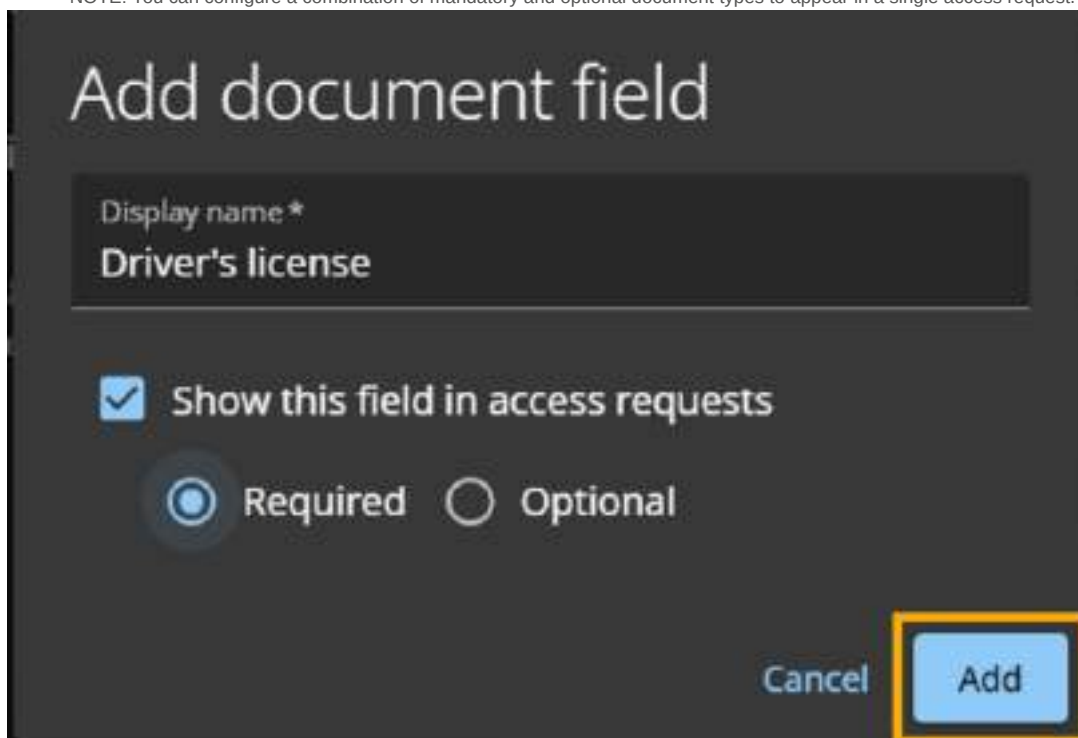
IMPORTANT: All areas inherit supporting documents configured at the site level. If needed, site owners can remove site level supporting document configurations from an area by accessing [area access request settings](#).

Procedure

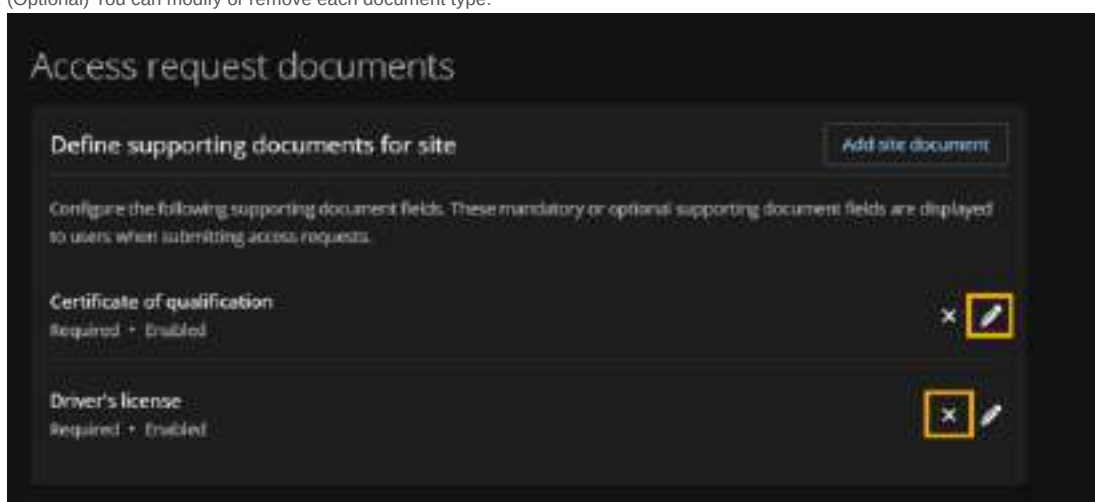
1. In the Genetec ClearID™ web portal, click Organization > Site > Access configurations.
2. Under Define supporting documents for site, click Add site document.



- a. In the Display name field, enter a name for the document type.
 - b. Select Show this field in access requests to display the document field in access requests for the site.
Tip: When the checkbox is cleared, the document type remains available in draft mode.
 - c. Choose whether or not uploading the document is mandatory when submitting an access request by clicking the Required or Optional radio button.
- NOTE: You can configure a combination of mandatory and optional document types to appear in a single access request.



3. Click Add.
4. (Optional) You can modify or remove each document type:



- a. Click  to modify the configuration of a supporting document.

- b. Click  to remove a configured supporting document.

7.6 | Customizing email notifications for sites in ClearID

To communicate specific requirements with email recipients, *Account administrators* and *Site owners* can customize the header and footer text of email notifications sent out by Genetec ClearID™.

What you should know

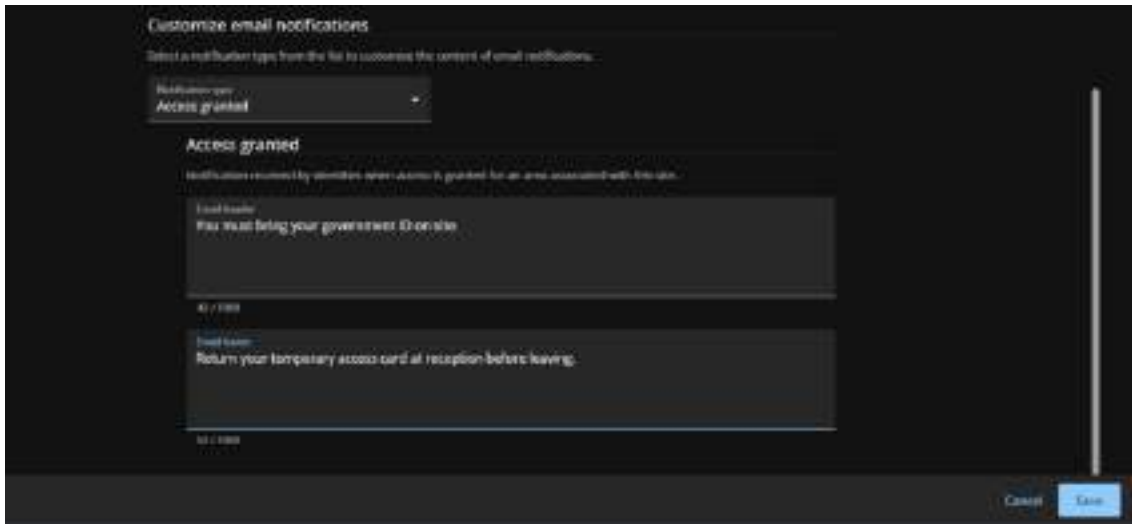
You can customize the header and footer text for two types of email notifications:

- Access granted notifications
- Visitor confirmation notifications

Procedure

1. Click Organization > Sites > Notifications.
2. From the Notification type list in the Customize email notifications section, select the type of email you want to customize.
 - a. In the Email header field, type the header text. For example, use the custom text fields to communicate equipment or documentation requirements to visitors or steps to complete before accessing an area.
 - b. In the Email footer field, type the footer text.

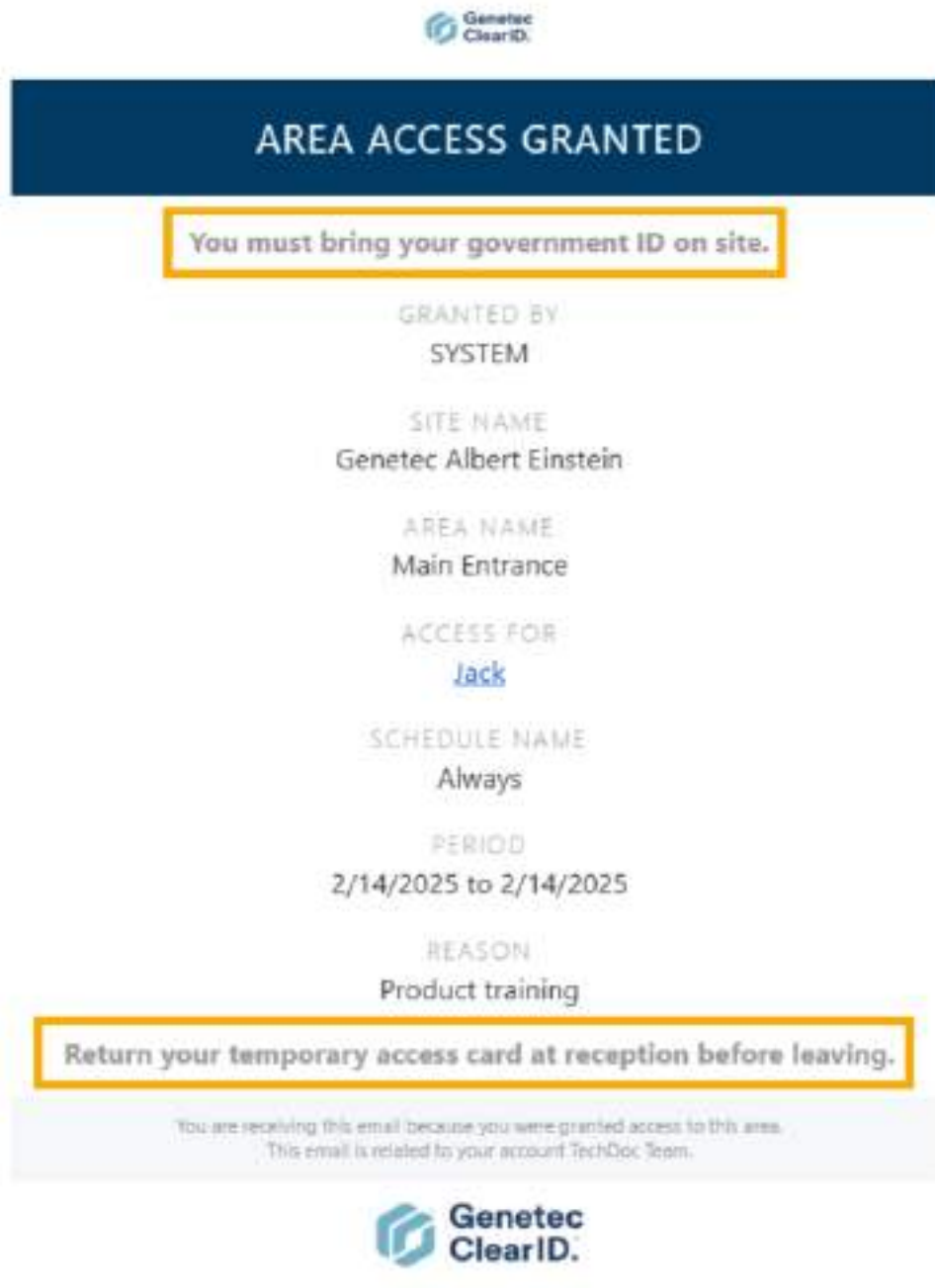
NOTE: Custom text in the header and footer of notification emails is limited to 1,000 characters.



The screenshot shows a web interface titled "Customize email notifications". Below the title, it says "Select a notification type from the list to customize the content of email notifications." A dropdown menu labeled "Notification type" has "Access granted" selected. Below this, the "Access granted" section is shown. It includes a "Email header" field with the text "You must bring your government ID on site" and a "42 / 1000" character count. Below that is an "Email footer" field with the text "Return your temporary access card at reception before leaving." and a "42 / 1000" character count. At the bottom right, there are "Cancel" and "Save" buttons.

3. Click Save.

Email notifications sent out by ClearID use your customized text in the header and footer.



7.6.1 | Customizing ClearID email notification branding

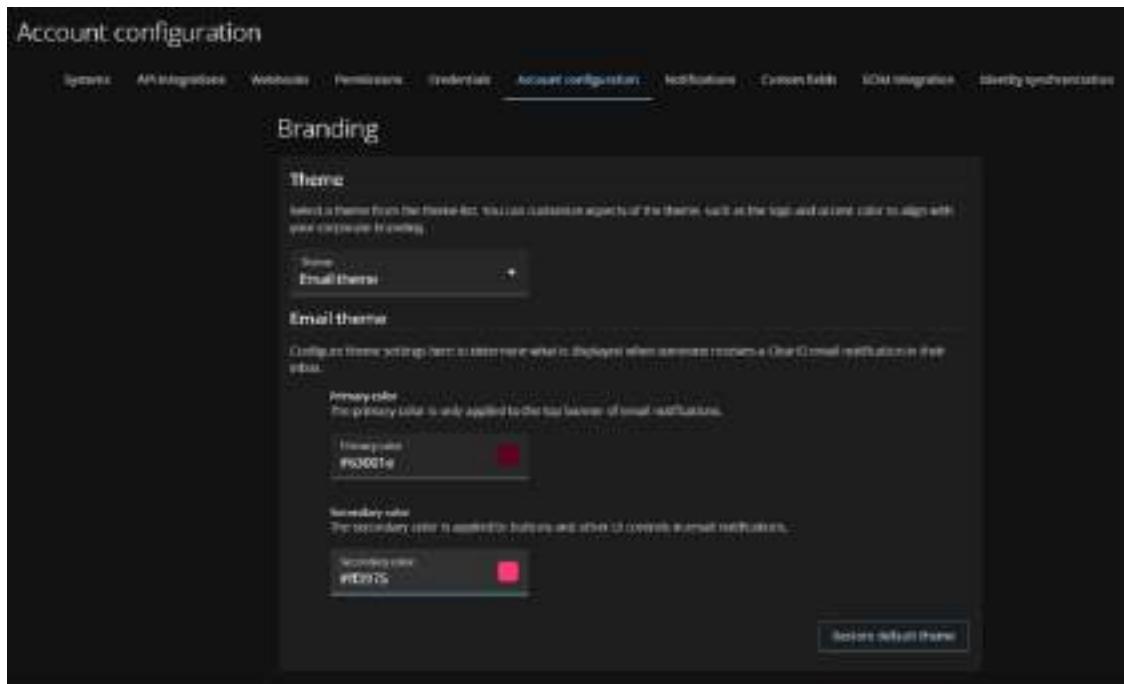
As an *Account administrator*, you can customize the color scheme of Genetec ClearID™ email notifications to align with your company's branding.

What you should know

You must be an *Account administrator* to customize email notification branding.

Procedure

1. In the ClearID web portal, click Administration > Account configuration.
2. In the Branding section, select Email theme from the Theme list.

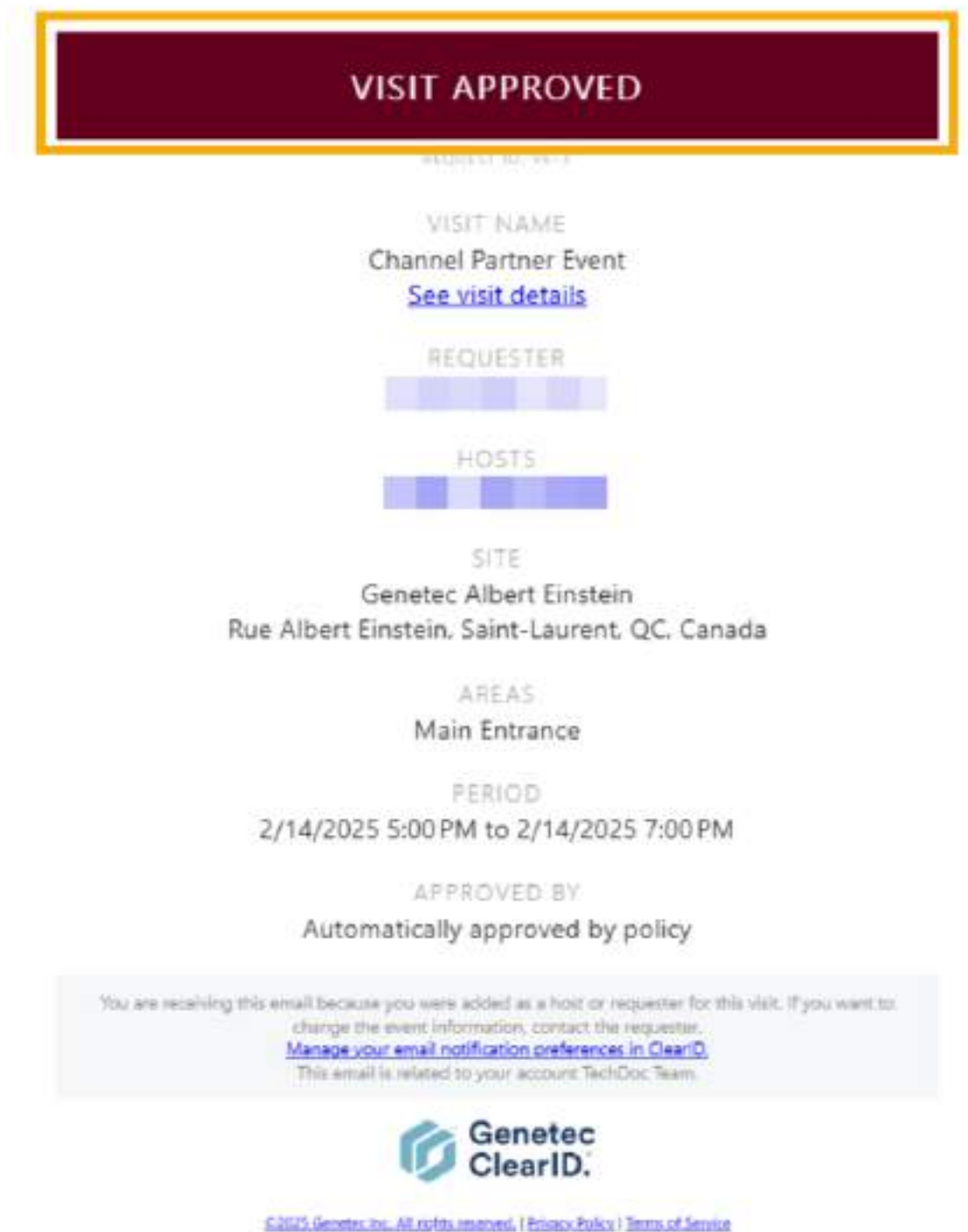


3. In the Email theme section, configure the colors for email notifications:
 - a. In the Primary color field, use the color picker to select a primary color to apply to the top banner of email notifications.
 - b. In the Secondary color field, use the color picker to select a secondary color to apply to buttons and other UI controls in email notifications.

Tip: You can reset the email theme colors to default by clicking the Restore default theme button.
4. Click Save.

Results

Customized branding is applied to the top banner, buttons, and UI controls of email notifications sent by ClearID.



Parent topic: Customizing email notifications for sites in ClearID

7.7 | About access reviews in ClearID

An access review is the process of performing an access review for an area, role, or identity to confirm that the access is still required and valid. To ensure security compliance and audit readiness you can schedule your access reviews to occur automatically.

Traditionally, security personnel manually export list of access and send to area owners to review twice a year, or every quarter.

In Genetec ClearID™ these access reviews can be scheduled (automated) or initiated manually. A site manager or owner is responsible for configuring access review frequency or manually initiating access reviews to ensure that the review process occurs on time.

- Site owners: Access reviews are displayed in the Access reviews report.
- Area managers or role managers: Area access reviews are displayed in My Tasks and notification emails.
- Supervisors: Identity access reviews are displayed in My Tasks and notification emails.

NOTE: Only site owners can access the Access review reports. Area managers can only access reviews for areas that they manage. Supervisors can only access reviews for their direct reports.

You cannot schedule a review for a site that has no areas. If a role or group is associated with an area or room, the role or group becomes part of the area review automatically. All Completed reviews are retained for audit and tracking purposes.



Scheduled access reviews

You can schedule site access reviews to occur yearly, monthly, weekly, or now to suit your needs.

- A site access review for a *Server Room* area could be scheduled to occur Yearly. For example, at quarterly intervals, on the first day of the month at 08:00.
- A site access review for a *Data Center* area could be scheduled to occur Monthly. For example, on the first day of every month at 08:00.

Manual access reviews

You can start an access review manually using the Now schedule when required, to ensure security compliance and audit readiness. Typically manual access reviews are used to test reviews in preparation for an annual review or scheduled reviews to check that all participants are properly set, or to force a review after an incident.

Access review email notifications

Access review email notifications are sent to relevant approvers to indicate that an area or role access review is pending. Site owners do not receive any email notifications.



Access review pending email notification

- When the COMPLETE THE REVIEW hyperlink is clicked, the access review detailed in the email notification is displayed and ready for review.
- When an area manager or role manager clicks the See all your access reviews hyperlink, the My access reviews page is displayed. This view only displays access reviews relevant to the approver.

Access review email notification reminders are sent every 7 days. Access review email notifications are sent from noreply@clearid.io. Check your spam or junk folder if email notifications are not received.

The status of incomplete access reviews are automatically updated to the Expired state when the incomplete access review is replaced by a newer scheduled review with the same name or when the Enforce an expiration for access reviews option is active and the expiration period has been exceeded.

All Completed reviews are retained for audit and tracking purposes. No changes can be made to an access review after it has been completed.
Browse

- [Access Reviews Feature Note \(2 pages\)](#)

7.8 | Setting up automatic expiration for access reviews

To ensure that reviewers only review current access information, you can specify an expiration period for access reviews. Failure to set an expiration could result in reviewers reviewing outdated information.

Before you begin

[Learn about access reviews.](#)

What you should know

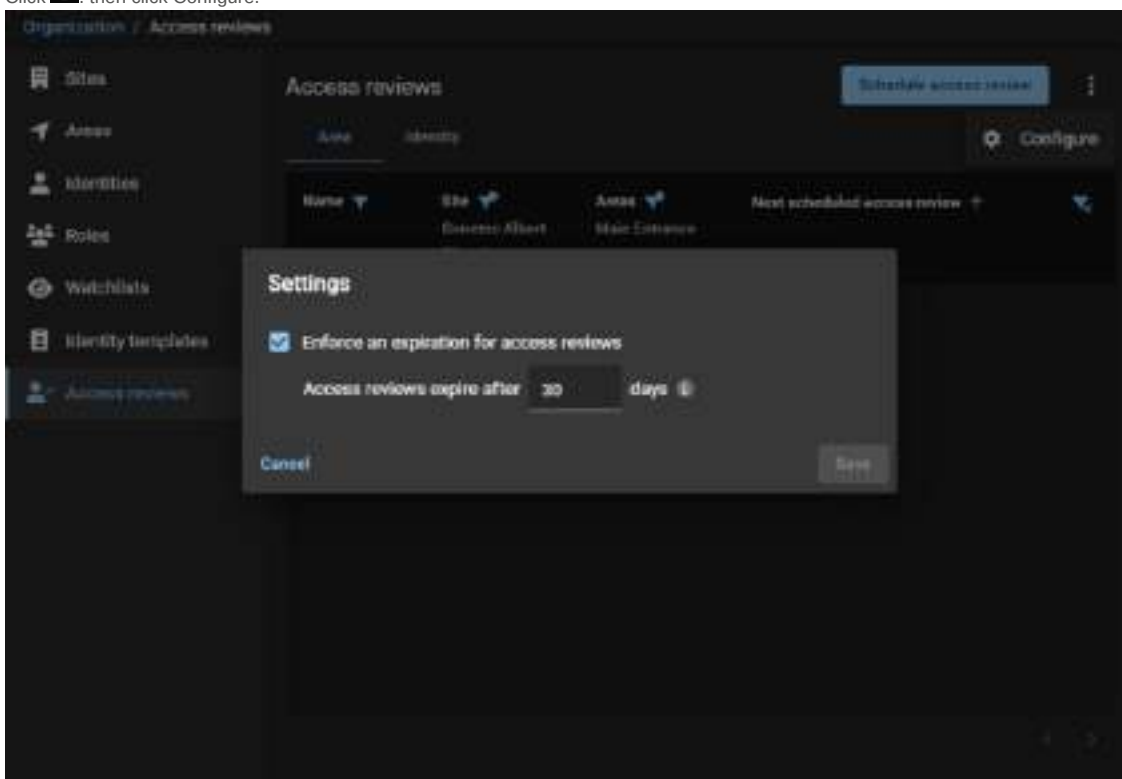
Only an account administrator can configure the expiration settings for access reviews.

Best Practice: The access reviews expiration setting is enabled by default and the default expiration period is set at 30 days.

- The expiration duration set for access reviews applies to all access reviews in the system.
- The new expiration setting is only applied to access reviews created after the setting is enabled or modified.
- When the access reviews expire, their status is set to Expired.
 - Access reviews displayed in My tasks are then changed to Completed with the status Expired.

Procedure

1. From the homepage, click Organization > Access reviews.
2. Click , then click Configure.



3. In the Settings dialog, select or enter the expiration duration that you require for your organization.
Tip: Pick an expiration interval that matches the access reviews requirement for your organization. Also bear in mind any audit or legal requirements that might be applicable.
4. (Optional) If your organization does not want to enforce expiration for access reviews, clear the Enforce an expiration for access reviews checkbox.
5. Click Save to confirm your changes.

After you finish

[Set up your access reviews.](#)

7.9 | Setting up area access reviews in ClearID

To ensure security compliance and audit readiness, you can set up area access reviews to occur at scheduled intervals. You can also start an area access review manually if required.

Before you begin

- Make sure that the site has areas defined.
- Make sure that the site is not already part of another review.

What you should know

- Only a site owner can set up area access reviews.

Best Practice: Schedule your site access reviews so that they are automatically triggered the day, week, or month before corporate audits or site safety checks to ensure your security compliance and audit readiness.

Procedure

In the Genetec ClearID™ web portal, do the following:

- [Schedule your area access reviews](#)

Results

Your area access reviews have now been set up.

After you finish

Do one or more of the following to complete your area access reviews when required:

- [Complete an area access review \(site owner\)](#)
- [Complete an area access review \(area owner\)](#)

Browse

- [Reviewing area access in ClearID](#)

Browse

- [Access Reviews Feature Note \(2 pages\)](#)

7.9.1 | Scheduling area access reviews in ClearID

To ensure security compliance and audit readiness, you can set up area access reviews to occur at scheduled intervals.

Before you begin

- Make sure that the site has areas defined.
- Make sure that the site is not already part of another review.

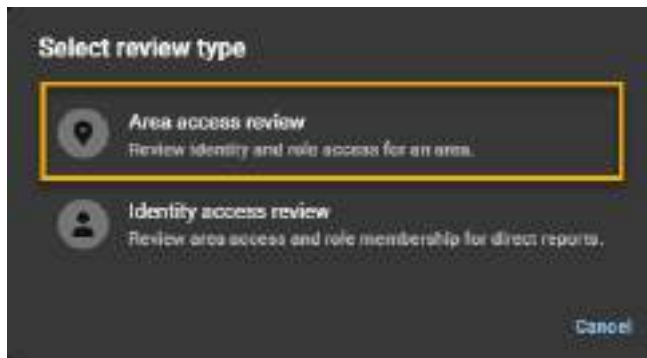
What you should know

- Only a site owner can schedule area access reviews.
- Site owners can define a review schedule for one or multiple areas under their site.

Best Practice: Schedule your site access reviews so that they are automatically triggered the day, week, or month before corporate audits or site safety checks to ensure your security compliance and audit readiness.

Procedure

1. From the homepage, click Organization > Access reviews.
2. Click Schedule access review.
3. In the Select review type dialog, select Area access review.



4. In the Site access review schedule dialog, select the options that you require.

a. Enter a Name for your area access review.

b. Select the Trigger site reviews frequency that you require and configure the options.

NOTE: The options that are displayed vary depending on the Trigger site reviews frequency that you select.

Yearly

Specifies a site access review that occurs yearly.

Monthly

Specifies a site access review that occurs monthly.

Weekly

Specifies a site access review that occurs weekly.

Now

Specifies a site access review that occurs immediately.

For example, an access review could be started manually using the *Now* schedule. Typically manual access reviews are used to test reviews before an annual review or scheduled reviews to check that all participants are properly set, or to force a review after an incident.

c. If you selected Yearly, select the day and month or months that you want the site access review scheduled.

d. If you selected Monthly, select the day that you want the site access review scheduled.

e. If you selected Weekly, select the day or days that you want the site access review scheduled.

f. Select the time that you want the site access review scheduled.

NOTE: The time shown in the Site access review schedules dialog options and all scheduled review times uses the time zone of the site.

g. Search for or select the site that you want to include in your site access review.

h. Search for or select the areas that you want to include in your site access review.

i. (Optional) In the Notes field, you can add more details as needed.

The Notes field is used to enter more detailed information about the site access review. This field is typically used when the site performs security reviews. For example, an ISO 27001 review or a SOC 1 or SOC 2 audit report.

The following example shows a site access review for a *server room* area scheduled to occur Yearly at quarterly intervals, on the first day of the month at 08:00.

Server room (quarterly access reviews)

Site access review schedule

Name *

Server Room (Quarterly Access Reviews)

Trigger site reviews

Yearly

Monthly

Weekly

Now

On the

1st

▼

day of

☒ January

☒ April

☒ July

☒ October

☐ February

☐ May

☐ August

☐ November

☐ March

☐ June

☐ September

☐ December

at

08

▼

00

▼

America/Toronto

(EST -05:00)

Site *

Genetec Head Office

▼

Area *

Server Room

+ Add more

Type to search...

▼

Notes

Close

Create

The following example shows a site access review for a *data center* area scheduled to occur Monthly, on the first day of every month at 08:00.
Data center (monthly access reviews)

Site access review schedule

Name *

Data Center (Monthly Access Reviews)

Trigger site reviews

Yearly

Monthly

Weekly

Now

On the

1st

▼

day of every month

at

08

▼

00

▼

America/New York

(EST -05:00)

Site *

Genetec Montreal

▼

Area *

Data Center

+ Add more

Type to search...

▼

Notes

Close

Create

The following example shows a site access review for a *data center* and *server room* area scheduled to occur Now.

Displayed in the footer
Page 196 of 473

Data center and server room (manual access review scheduled now)

Site access review schedule

Name *

Access review test

Trigger site reviews

Yearly

Monthly

Weekly

Now

Site *

Genetec Montreal

Area *

Data Center

Server Room

Add more

Type to search...

Close

Create

NOTE: Access reviews that are configured with a schedule of Now are not displayed on the scheduled Access reviews page. Instead, they are immediately displayed in the My tasks view of the relevant reviewers.

5. Click Create.

The scheduled access reviews are displayed in the Access reviews page.

Organization / Access reviews

Access reviews

Schedule access review

Area

Security

Name	Site	Area	Next scheduled access review	
Data Center (Monthly Access Reviews)	Genetec Montreal	1 area	January 1, 2023 at 8:00 AM (Monthly)	X
Server Room (Quarterly Access Reviews)	Genetec Montreal	1 area	January 1, 2023 at 12:00 PM (Quarterly)	X

6. (Optional) Click an area access review in the list to see the schedule details.
- a. Click Go to access reviews report to display all access reviews.

Results

Your site area access reviews have now been scheduled.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Do one or more of the following to complete your access reviews when required:

- Complete an area or role access review (site owner)
- Complete an area or role access review (area owner)

Parent topic: [Setting up area access reviews in ClearID](#)

7.10 | Setting up identity access reviews in ClearID

To ensure security compliance and audit readiness, you can set up identity access reviews to occur at scheduled intervals.

Before you begin

- Make sure that the supervisor has direct report identities defined.

What you should know

- Only an account administrator can set up identity access reviews.

Best Practice: Schedule your identity access reviews so that they are automatically triggered before corporate audits or site safety checks to ensure your security compliance and audit readiness.

Procedure

In the Genetec ClearID™ web portal, do the following:

- [Schedule your identity access reviews](#)

Results

Your access reviews have now been set up.

After you finish

[Complete an identity access review \(supervisor\)](#)

7.10.1 | Scheduling identity access reviews in ClearID

To ensure security compliance and audit readiness, you can set up identity access reviews to occur at scheduled intervals. These identity access reviews are performed based on a list of selected roles.

Before you begin

- Make sure that the roles to be reviewed have already been defined.
- Make sure that all the required identities have been associated with the correct roles.

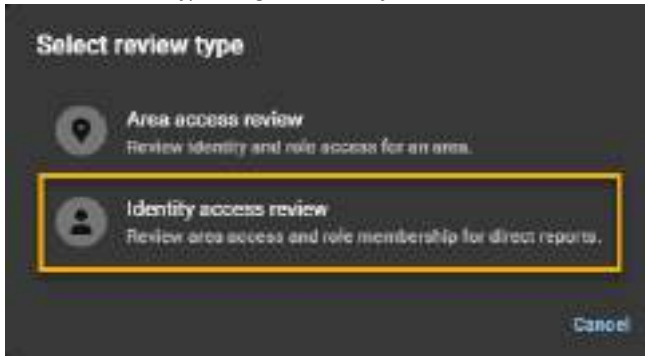
What you should know

- Only an account administrator can schedule identity access reviews.
- For Identity access reviews, only Yearly schedules are supported.
- You can schedule up to five identity access reviews at a time, and each review can include a maximum of 20 roles.

Best Practice: Schedule your identity access reviews so that they are automatically triggered before corporate audits or site safety checks to ensure your security compliance and audit readiness.

Procedure

1. From the homepage, click Organization > Access reviews.
2. Click Schedule access review.
3. In the Select review type dialog, select Identity access review.



4. In the Identity access review schedule dialog, select the options that you require.
 - a. Enter a Name for your identity access review.

For example, You might enter Contractor access review for electricians or Data center identity access review for your direct reports that need access to a data center.
 - b. Select the Trigger identity reviews options that you require.
 - Select the day and month that you want the identity access review scheduled.
 - Select the time that you want the identity access review scheduled.

NOTE: The time shown in the Identity access review schedules dialog options and all scheduled review times use the UTC time zone.
 - c. Select the Roles that you want to include in your Identity access review.

Identity access reviews will be generated for all identities in that role (active and inactive status). Inactive identities are clearly identified in the review.
 - d. (Optional) If you selected Yearly, in the Notes field, you can add more details as needed.

The Notes field is used to enter more detailed information about the identity access review. This field is typically used when a supervisor performs security reviews. For example, an ISO 27001 review or a SOC 1 or SOC 2 audit report.

The following example shows an identity access review for *Electrical contractors* role scheduled to occur Yearly, on the first day of January at 12:00.

Identity access review (yearly access reviews)

Identity access review schedule

None*

Electrical Contractor Identities review (1st review of the year)

Trigger identity reviews

Yearly

On the

1st +

day of

☒ January

☐ April

☐ July

☐ October

☐ February

☐ May

☐ August

☐ November

☐ March

☐ June

☐ September

☐ December

at

12 +

00 +

UTC (-05:00)

None*

Electrical contractors

+ Add more

Type to search...

1 / 30

None

Yearly identities review

Close

Create

- 5. Click Create.
- 6. (Optional) Click an identity access review in the list to see the schedule details.
 - a. Click Go to access reviews report to display all access reviews.

Results

Your identity access reviews have now been scheduled.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Do the following to complete your access reviews when required:

- Complete an identity access review (supervisor)

Parent topic: Setting up identity access reviews in ClearID

7.11 | Modifying access reviews in ClearID

After you have set up and scheduled your area or identity access reviews, you can modify or delete them if required.

Before you begin

- [Scheduling area access reviews in ClearID](#)
- [Scheduling identity access reviews in ClearID](#)

What you should know

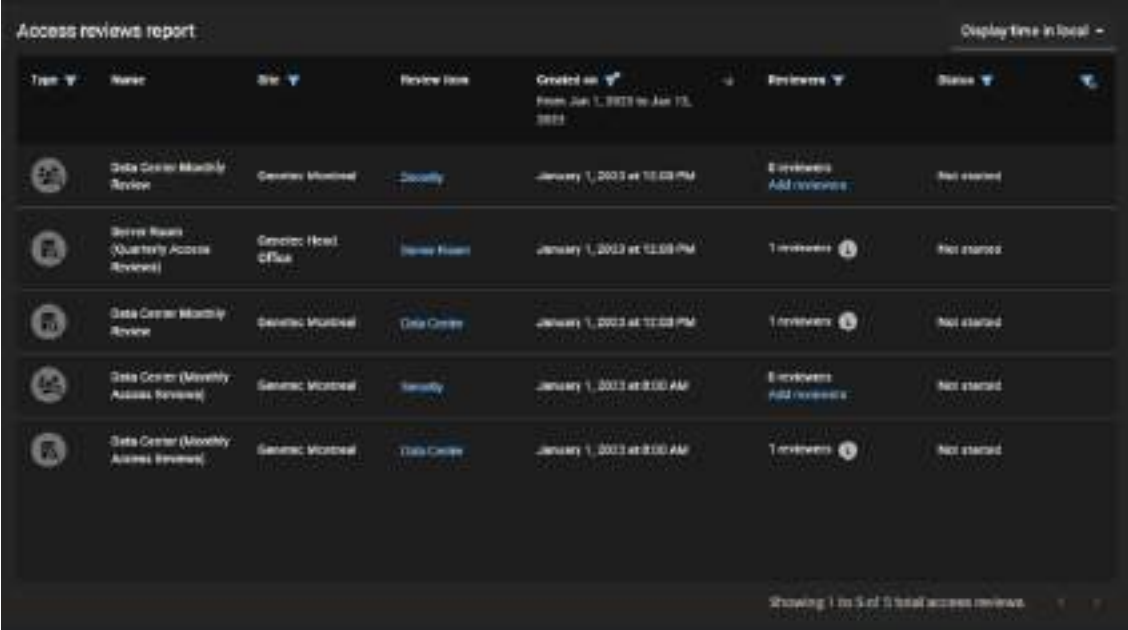
- Only a site owner can modify area access reviews.
- Only an account administrator can modify identity access reviews.

Procedure

1. If you need to make any changes or delete an identity access review schedule, click Organization > Access reviews.
2. To modify an area access review schedule, click the Area tab.
3. To modify an identity access review schedule, click the Identity tab.
4. Click a review in the list and make any changes that you require then click Save.
5. (Optional) To delete an access review, click  next to the review you want to delete then click Remove to confirm the deletion.

7.12 | About access reviews report in ClearID

In Genetec ClearID™, an access reviews report is a list of access reviews. The report includes information about area, role, or identity access reviews and the current review status (not started, started, in progress, completed, or expired).



Type	Name	Site	Review type	Created on	Reviewers	Status
Area	Data Center Monthly Review	Genetec Montreal	Monthly	January 1, 2023 at 10:00 PM	2 reviewers Add reviewers	Not started
Role	Server Room (Quarterly Access Reviews)	Genetec Host Office	Quarterly	January 1, 2023 at 12:00 PM	1 reviewer Add reviewers	Not started
Area	Data Center Monthly Review	Genetec Montreal	Data Center	January 1, 2023 at 11:00 PM	1 reviewer Add reviewers	Not started
Area	Data Center (Monthly Access Reviews)	Genetec Montreal	Monthly	January 1, 2023 at 8:00 AM	8 reviewers Add reviewers	Not started
Area	Data Center (Monthly Access Reviews)	Genetec Montreal	Data Center	January 1, 2023 at 8:00 AM	1 reviewer Add reviewers	Not started

Showing 1 of 5 of 5 total access reviews

Access reviews report

The access reviews report is used for the following:

- Site owners: To check the status of site access reviews for areas or roles.
- Supervisors: To check the status of identity access reviews (for their direct reports).
- Audits: To provide information to auditors.

Column filters can be used to help refine the report search results by review type, site, created on, reviewers, and status.

For example, you could filter for completed reviews, then select a review and choose Print (hardcopy) or Print > Destination > Save as PDF (softcopy). The hardcopy or softcopy can then be shared with auditors or other members of your organization.

Who can see what?

- Area managers or role managers only see the filters that are relevant to area or role reviews.
- Supervisors only see their direct reports.
- Administrators see everything.

Browse

- [Checking the status of access reviews in ClearID](#)

7.13 | Checking the status of access reviews in ClearID

A site owner is responsible for checking the status of access reviews to ensure that the organization is security-compliant, audit ready, and that the review processes occurs on time. A supervisor can also check the status of identity access reviews for their direct reports.

Before you begin

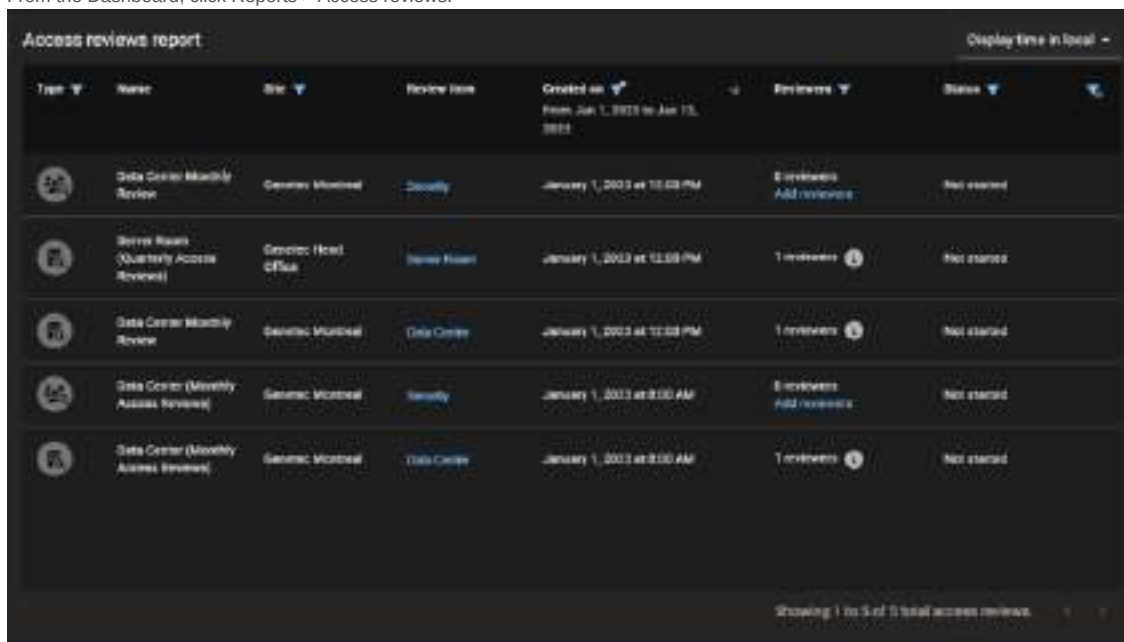
Set up your access reviews.

What you should know

- Only a site owner can view the complete Access reviews report to check the status or progress of an area or role access review for their site.
- An area manager or role manager only sees their reviews in a My access reviews version of the report.
- A site owner who is not an area owner or manager, or a role owner or manager does not see any access reviews in Dashboard > My tasks.
- Filters: When no types, sites, or reviewers are selected, all results are displayed in the report.

Procedure

1. From the Dashboard, click Reports > Access reviews.



Team	Name	Site	Review type	Created on	Reviewers	Status
	Data Center Monthly Review	Security Montreal	Security	January 1, 2023 at 10:03 PM	8 reviewers Add reviewers	Not started
	Server Room (Quarterly Access Reviews)	Security Montreal	Server Room	January 1, 2023 at 12:03 PM	1 reviewer	Not started
	Data Center Monthly Review	Security Montreal	Data Center	January 1, 2023 at 12:03 PM	1 reviewer	Not started
	Data Center (Monthly Access Reviews)	Security Montreal	Security	January 1, 2023 at 8:00 AM	8 reviewers Add reviewers	Not started
	Data Center (Monthly Access Reviews)	Security Montreal	Data Center	January 1, 2023 at 8:00 AM	1 reviewer	Not started

Showing 1 to 5 of 5 total access reviews

Tip: If any review shows 0 reviewers in the Reviewers column, you can click the Add reviewers hyperlink to add them immediately. This situation typically occurs when there are no owners or managers defined.

2. In the Access reviews report page, select the display time that you require from the following options:

Display time in local

Show report times using the local system time from the computer of the logged-in user.

Display time in UTC

Show report times using Coordinated Universal Time (UTC).

3. In the Created on column, select one of the options, or click Date range and specify a date and time range to display a list of access reviews.

☐ Last 24 hours

☐ Last 7 days

☐ Last 30 days

☐ Last 90 days

☐ Last 365 days

☒ Date range

From * 01/18/2022 To * 10:15 AM

To * 01/18/2023 To * 10:15 AM

Time period limited to a maximum of one year

4. (Optional) If the list is long, configure additional report column filters to narrow report results as required.
 - a. In the Type column, select one or more review types as required:
 - Area access review**
Displays area access reviews.
 - Role access review**
Displays role access reviews.
 - Identity access review**
Displays identity access reviews.
 - b. In the Site column, enter a search string or select one or more sites from the list.
 - c. In the Reviewers column, enter an access reviewer's name or email to show reviews that they are associated with.
 - d. In the Status column, select the status options that you want to display when checking the access review.

NOTE: The status of incomplete access reviews are automatically updated to the Expired state when the incomplete access review is replaced by a newer scheduled review with the same name or when the Enforce an expiration for access reviews option is active and the expiration period has been exceeded.
 - e. (Optional) Click  to reset filter selections.
5. In the Review item column, click a hyperlink to check the details of the access review or to complete the review.
6. (Optional) You can see the list of reviewers by clicking the info icon () next to reviewers.
7. (Optional) If you selected an area access review, click hyperlinks in the Review item column to display additional information about the access review.
8. (Optional) If you selected an access review, click Continue review to complete the access review now.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Do one or more of the following to complete your access reviews when required:

- Complete an area access review (site owner)
- Complete an area access review (area owner)
- Complete an identity access review (supervisor)

Browse

- [About access reviews report in ClearID](#)

7.14 | Completing an area access review (site owner) in ClearID

To ensure security compliance or audit readiness you can perform access reviews to check who has access to an area or role. These periodic reviews are completed by a site owner.

Before you begin

[Set up your site access reviews.](#)

What you should know

- No changes can be made to an access review after it has been completed.
- All Completed reviews are retained for audit and tracking purposes.

Procedure

To complete an area access review:

1. From the Home page, click Reports > Access reviews.
2. (Optional) Configure report column filters as required.
3. In the Access reviews report section, select the area access review that you require.

Access reviews report Display time in local -

Type	Name	Site	Review item	Created on From Jan 1, 2023 to Jan 15, 2023	Reviewers	Status
	Data Center Monthly Review	Genetec Montreal	Security	January 1, 2023 at 10:08 PM	0 reviewers Add reviewers	Not started
	Service Room (Quarterly Access Reviews)	Genetec Head Office	Service Room	January 1, 2023 at 12:08 PM	1 reviewer	Not started
	Data Center Monthly Review	Genetec Montreal	Data Center	January 1, 2023 at 11:08 PM	1 reviewer	Not started
	Data Center (Monthly Access Reviews)	Genetec Montreal	Security	January 1, 2023 at 9:00 AM	0 reviewers Add reviewers	Not started
	Data Center (Monthly Access Reviews)	Genetec Montreal	Data Center	January 1, 2023 at 9:00 AM	1 reviewer	Not started

Showing 1 to 5 of 5 total access reviews

- Click an area hyperlink in the Review item column to begin the access review.
- Click Continue review.

4. In the Details section of the area access review, check the summary details.

Access review for Data Center

Summary Access Review

0 / 9

This access review is a snapshot of identity or role access for Data Center as of September 29, 2023, 1:43 PM / any modifications (identity or role access added or removed) made after this date and time will not be reflected in this access review.

Access review summary
This access review wizard guides you through the process of reviewing identity or role access.

Created by Jamie Myles on September 29, 2023, 1:43 PM

1 reviewer

Close and continue later Next

- Click to see the reviewer details.
- (Optional) Click Close and continue later to pause the review for a later time.
- Click Next to continue to the next section of the access review wizard.

5. In the Access section of the access review, review the access.

Access review for Data Center

Summary Access Review

0/5

Access - 0/5 completed
5 identities or roles have access to this area - verify that the identity or role access is still valid. Revoked access will be revoked after the review is completed.

Approve all remaining ☐ Show already reviewed

information technology - IT department	September 19, 2023 to Forever - Always Authorized by James Myers on September 14, 2023 (General access - always)	✓ ✗
John Doe	September 19, 2023 to November 15, 2023 - Always Authorized by James Myers on September 14, 2023 (General access)	✓ ✗
Security	September 19, 2023 to Forever - Always Authorized by James Myers on September 14, 2023 (General access - always)	✓ ✗
Superman Devision	September 19, 2023 to November 15, 2023 - Always Authorized by James Myers on September 14, 2023 (General access)	✓ ✗
Test Cloud (enduser)	September 19, 2023 to November 15, 2023 - Always Authorized by James Myers on September 14, 2023 (General access)	✓ ✗

Close and continue later

Back Next

- Click Keep access (✓) to confirm that access is still valid.
Tip: Use Approve all remaining to speed up approval process when the list is long, then remove any access that is no longer required.
 - Click Remove access (✗) to remove access that is no longer required.
 - (Optional) Select Show already reviewed to go back and make modifications.
 - Click Next to continue to the next section of the access review wizard.
6. In the Review section of the access review, verify that the review details are correct.

Access review for Data Center

Summary Access Review

5/5

No changes can be made to this access review after it is completed - ensure that all information is up to date and valid before completing the review.

Additional notes
Enter any additional information or comments relevant to this access review.

Adding notes

When this access review is completed, the following changes will be made:

- No identities or roles will have their access revoked from Data Center.
- A report will be created for this access review, which can be found in the Reports section.

Close and continue later

Back Complete

- In the Additional notes section, add any notes that you require.
- Before you click Complete, review the changes summary immediately after the Additional notes section.

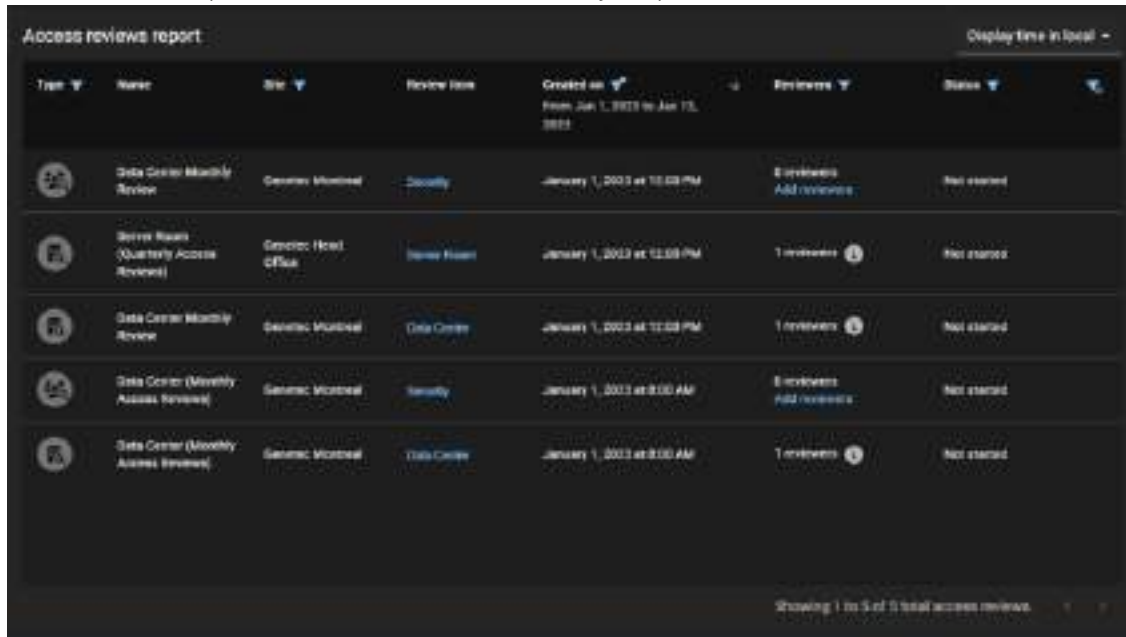
Genetec ClearID®; User Guide

Displayed in the header

- The changes summary displays information about any identity or role changes that will occur when you click Complete.
- (Optional) If any of the information looks incorrect, click Back to return to previous sections and modify your changes.
 - If the Review section details are correct, click Complete.

To complete a role access review:

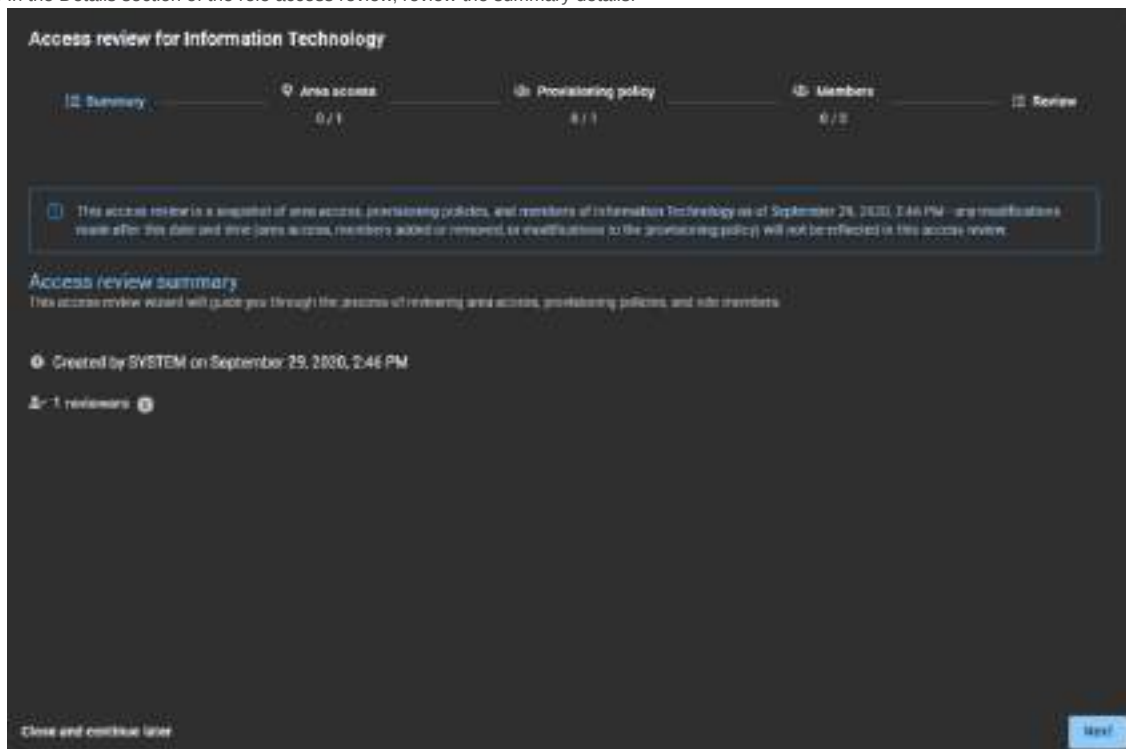
- From the Home page, click Reports > Access reviews.
- (Optional) Configure report column filters as required.
- In the Access reviews report section, select the role access review that you require.



Type	Name	Site	Review item	Created on	Reviewers	Status
	Data Center Monthly Review	Genetec Montreal	Security	January 1, 2023 at 10:03 PM	2 reviewers Add reviewers	Not started
	Server Room (Quarterly Access Reviews)	Genetec Head Office	Server Room	January 1, 2023 at 11:09 PM	1 reviewer	Not started
	Data Center Monthly Review	Genetec Montreal	Data Center	January 1, 2023 at 11:03 PM	1 reviewer	Not started
	Data Center (Monthly Access Reviews)	Genetec Montreal	Security	January 1, 2023 at 8:00 AM	2 reviewers Add reviewers	Not started
	Data Center (Monthly Access Reviews)	Genetec Montreal	Data Center	January 1, 2023 at 8:00 AM	1 reviewer	Not started

Showing 1 in 5 of 5 total access reviews

- Click a role hyperlink in the Review item column to begin the access review.
 - Click Continue review.
4. In the Details section of the role access review, review the summary details.



Access review for Information Technology

Summary | Area access | Provisioning policy | Members | Review

0 / 1 | 0 / 1 | 0 / 0

This access review is a snapshot of area access, provisioning policies, and members of Information Technology as of September 29, 2023, 2:46 PM – any modifications made after this date and time (area access, members added or removed, or modifications to the provisioning policy) will not be reflected in this access review.

Access review summary

This access review wizard will guide you through the process of reviewing area access, provisioning policies, and role members.

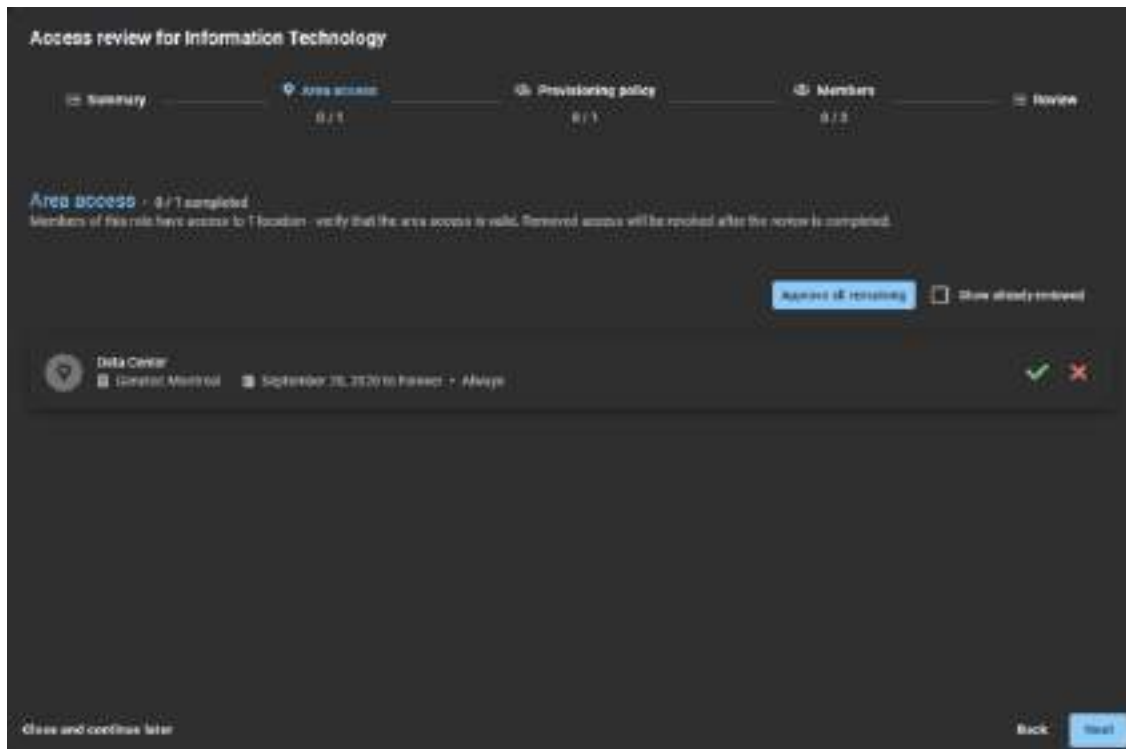
Created by SYSTEM on September 29, 2023, 2:46 PM

1 reviewer

Close and continue later

Next

- Click ⓘ to see the reviewer details.
 - (Optional) Click Close and continue later to pause the review for a later time.
 - Click Next to continue to the next section of the access review wizard.
5. In the Area access section of the role access review, review the access.



- a. Click Keep access (✓) to confirm that access is still valid.
Tip: Use Approve all remaining to speed up approval process when the list is long, then remove any access that is no longer required.
- b. Click Remove access (✗) to remove access that is no longer required.
- c. (Optional) Select Show already reviewed to go back and make modifications.
- d. Click Next to continue to the next section of the access review wizard.

6. In the Provisioning policy section of the role access review, confirm that the policies are still valid.



- a. (Optional) Click view or edit the policy to open the Provisioning policy page to view or make changes to the policy.
- b. Click Approve policy (✓) to confirm that policy is still valid.
- c. Click Next to continue to the next section of the access review wizard.

7. In the Members section of the role access review, confirm that the members are still valid.

Access review for Information Technology

Summary Area access Provisioning policy **Members** Review

Role members • 0/3 completed
The following members have been added to this role manually - verify that this information is up to date. Reported members will be removed from the role after the review is completed.

[Approve all remaining](#) ☐ Show already reviewed

	Supervisor Janssen • janssen.supervising@gmail.com Authorized by Joske Myles on September 20, 2023 (Temporary access added manually)		
	Veronica J. Janssen • janssen.veronica@gmail.com Authorized by Joske Myles on September 20, 2023 (Temporary access added manually)		
	Paul Janssen • janssen.paul@gmail.com Authorized by Joske Myles on September 20, 2023 (Temporary access added manually)		

Close and continue later Back Next

- Click Keep access () to confirm that access is still valid.
Tip: Use Approve all remaining to speed up approval process when the list is long, then remove any access that is no longer required.
- Click Remove access () to remove access that is no longer required.
- (Optional) Select Show already reviewed to go back and make modifications.
- Click Next to continue to the next section of the access review wizard.

8. In the Review section of the role access review, verify that the review details are correct.

Access review for Information Technology

Summary Area access Provisioning policy Members **Review**

No changes can be made to this access review after it is completed - ensure that all information is up to date and valid before completing the review

Additional notes
Enter any additional information or comments relevant to this access review.

Additional notes

When this access review is completed, the following changes will be made:

- Information Technology will have its access revoked for 0 areas.
- No changes to the role provisioning policy.
- 0 members will be removed from Information Technology.
- A report will be created for this access review, which can be found in the Reports section.

Close and continue later Back Complete

- In the Additional notes section, add any notes that you require.
- Before you click Complete, review the changes summary immediately after the Additional notes section.
- (Optional) If any of the information looks incorrect, click Back to return to previous sections and modify your changes.
- If the Review section details are correct, click Complete.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Generate an access reviews report.
Browse

- Reviewing area access in ClearID

Browse

- Access Reviews Feature Note (2 pages)

7.15 | Completing an area access review (area manager or role manager) in ClearID

To ensure security compliance or audit readiness, you can perform access reviews to check who has access to an area or role. These periodic reviews are completed by an area manager or role manager.

Before you begin

Check your mail for an *Access Review Pending* email notification or look on the My tasks page for a pending review.

What you should know

- Area managers or role managers can complete an access review from the My tasks page of the Dashboard or from an email notification.
- No changes can be made to an access review after it has been completed.
- All Completed reviews are retained for audit and tracking purposes.
-

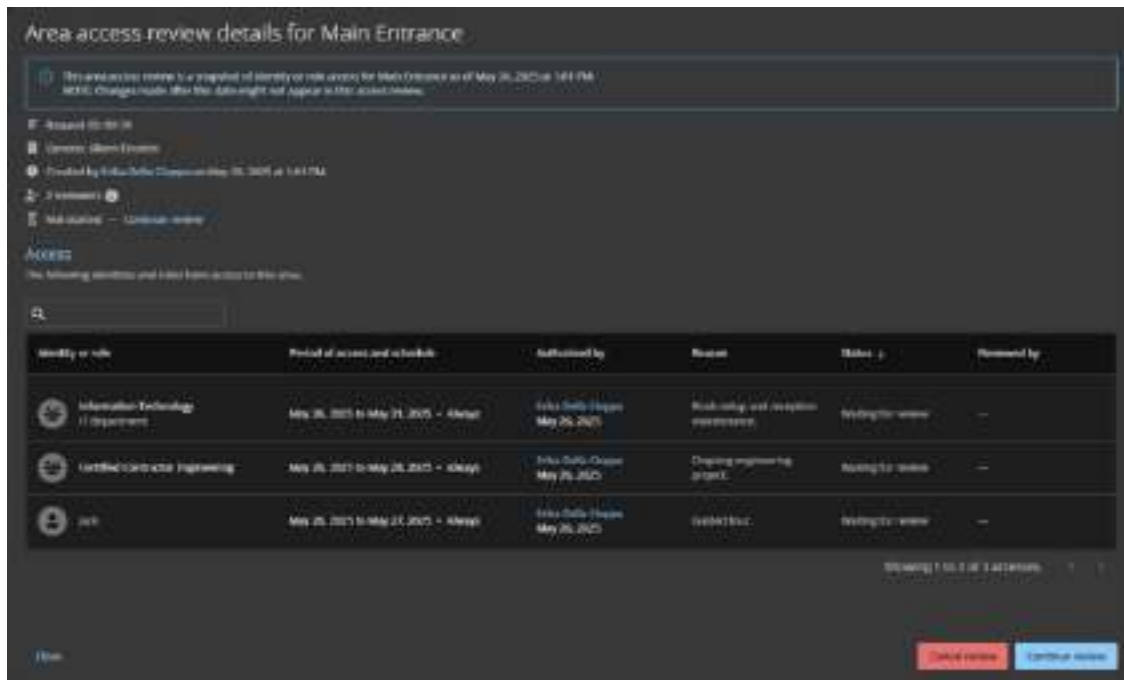
Procedure

To complete an area access review from the Dashboard page:

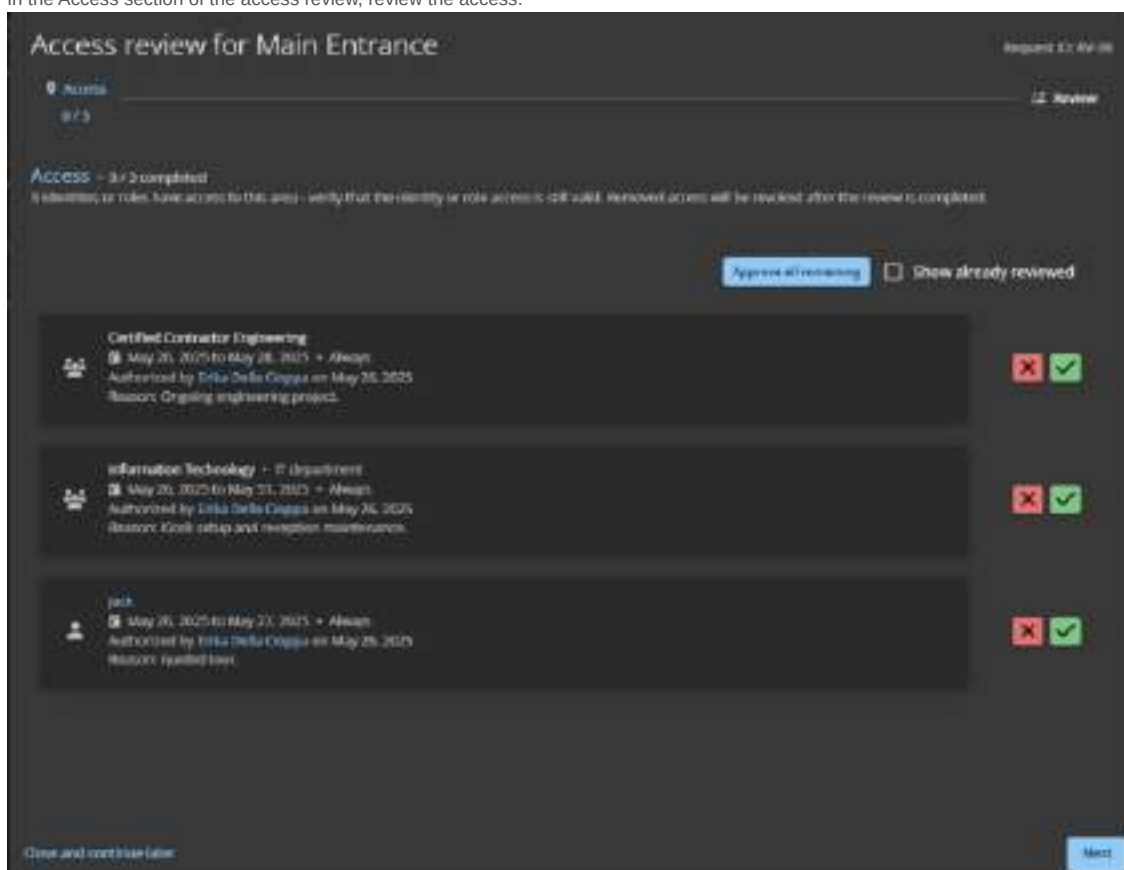
1. Click Dashboard > My tasks.
2. In the My tasks list, click the area that you require.



3. In the Details section of the area access review, check the summary details.



- a. Click  to see the reviewer details.
 - b. (Optional) Click Close and continue later to pause the review for a later time.
 - c. Click Next to continue to the next section of the access review wizard.
4. Click Continue review.
 5. In the Access section of the access review, review the access.



- a. Click Keep access () to confirm that access is still valid.
Tip: Use Approve all remaining to speed up approval process when the list is long, then remove any access that is no longer required.
 - b. Click Remove access () to remove access that is no longer required.
 - c. (Optional) Select Show already reviewed to go back and make modifications.
 - d. Click Next to continue to the next section of the access review wizard.
6. In the Review section of the access review, verify that the review details are correct.

Access review for Main Entrance

Report ID: 04-04

Alerts 3 of 3 Review

No changes can be made to this access review after it is completed. Ensure that all information is up to date and valid before completing the review.

Additional notes

Enter any additional information or comments relevant to this access review. The contents of additional information are not monitored by an administrator and are for audit viewing purposes only.

Add notes

When this access review is completed, the following changes will be made:

- 1 identity or role will have their access revoked from Main Entrance.
- A report will be created for this access review, which can be found in the Reports section.

Click and continue later Back Complete

- In the Additional notes section, add any notes that you require.
- Before you click Complete, review the changes summary immediately after the Additional notes section.
The changes summary displays information about any identity or role changes that will occur when you click Complete.
- (Optional) If any of the information looks incorrect, click Back to return to previous sections and modify your changes.
- If the Review section details are correct, click Complete.

To complete a role access review from the Dashboard page:

- Click Dashboard > My tasks.
- In the My tasks list, click the role that you require.

Genetec Dashboard

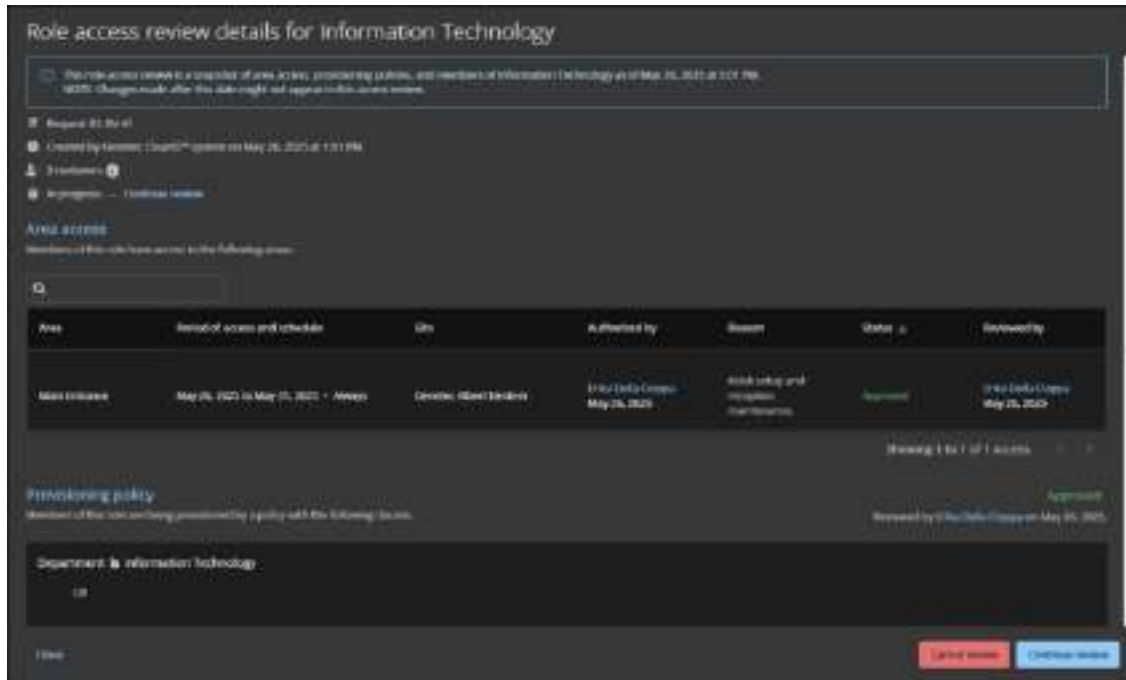
My tasks My tasks My tasks

Filtering

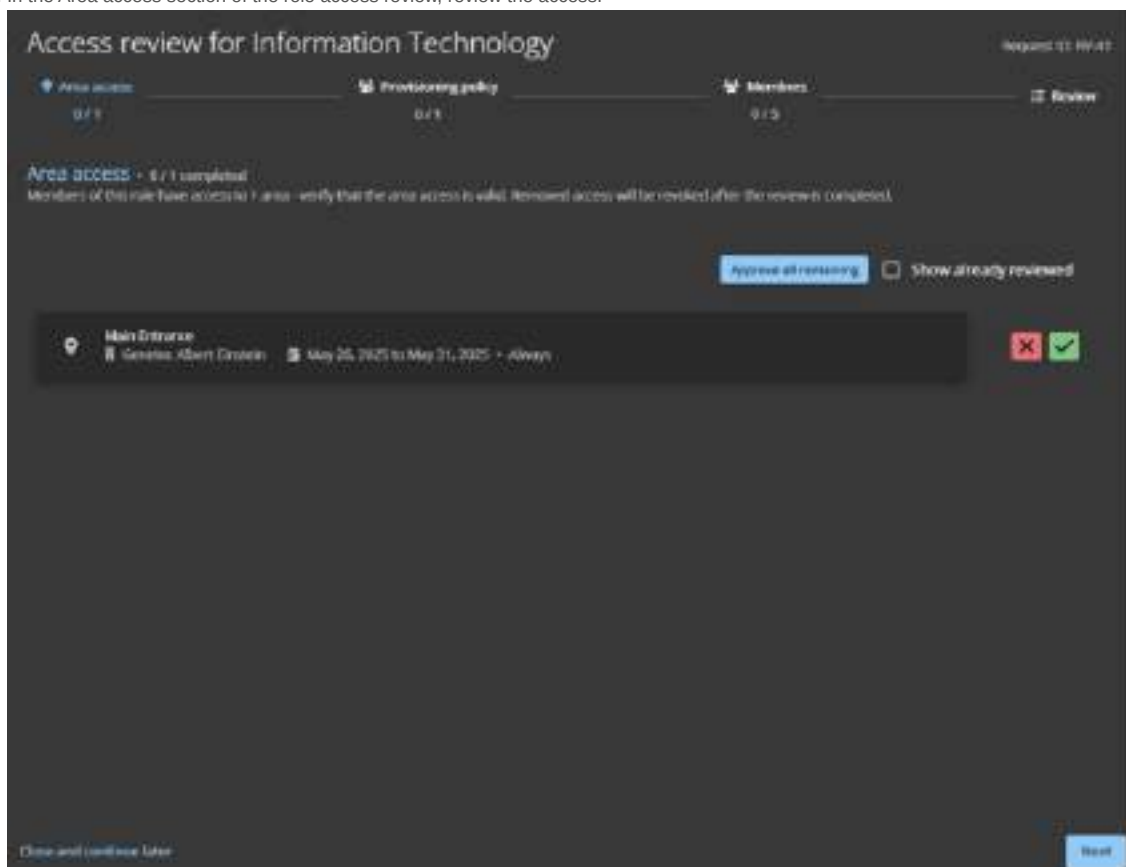
Type	Name	Description	Date updated
Information technology Role access review - 04-04	Role access	Genetec Main Entrance	17 Nov 2020
Controlled access Engineering Role access review - 04-04	Role access	Genetec Main Entrance	17 Nov 2020
Role access Information technology - 04-04	Information	Genetec Main Entrance	17 Nov 2020
Information technology Role access review	Role access	Genetec Main Entrance	16 Nov 2020

Create Role

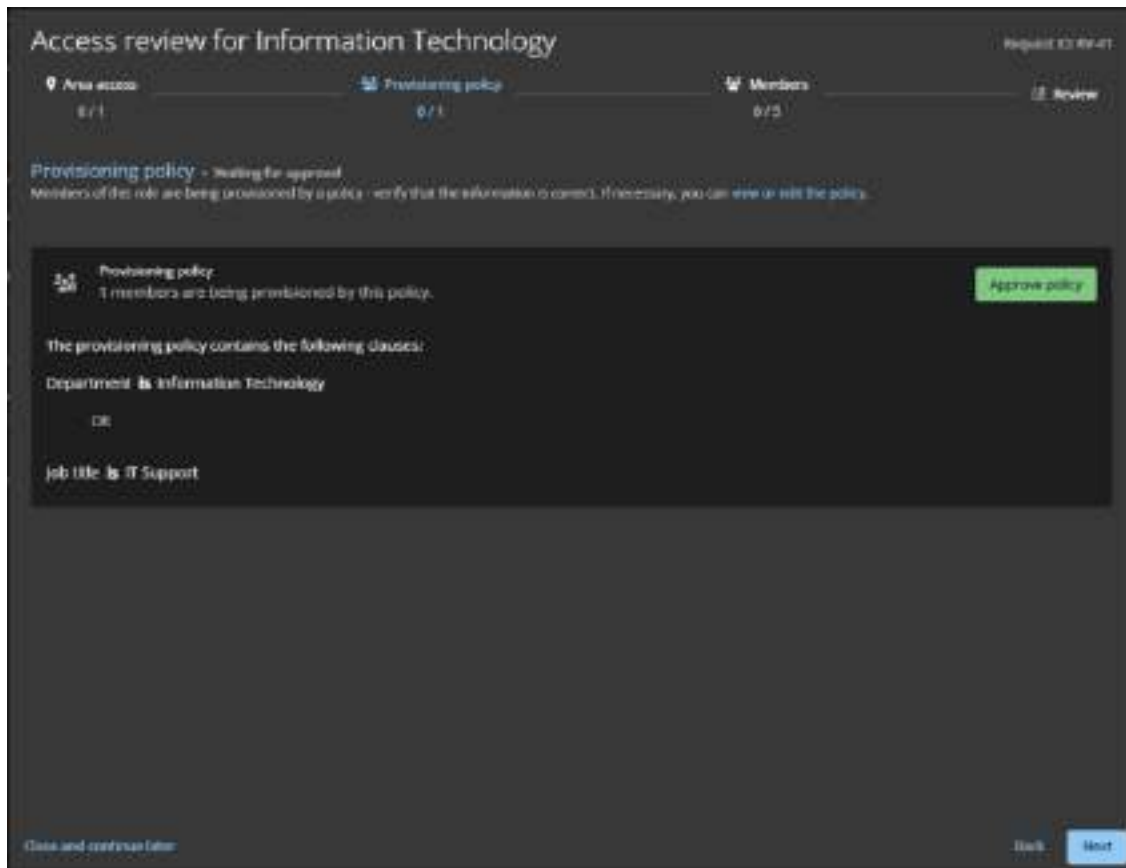
- In the Details section of the role access review, review the summary details.



- a. Click  to see the reviewer details.
 - b. (Optional) Click Close and continue later to pause the review for a later time.
 - c. Click Next to continue to the next section of the access review wizard.
4. Click Continue review.
 5. In the Area access section of the role access review, review the access.

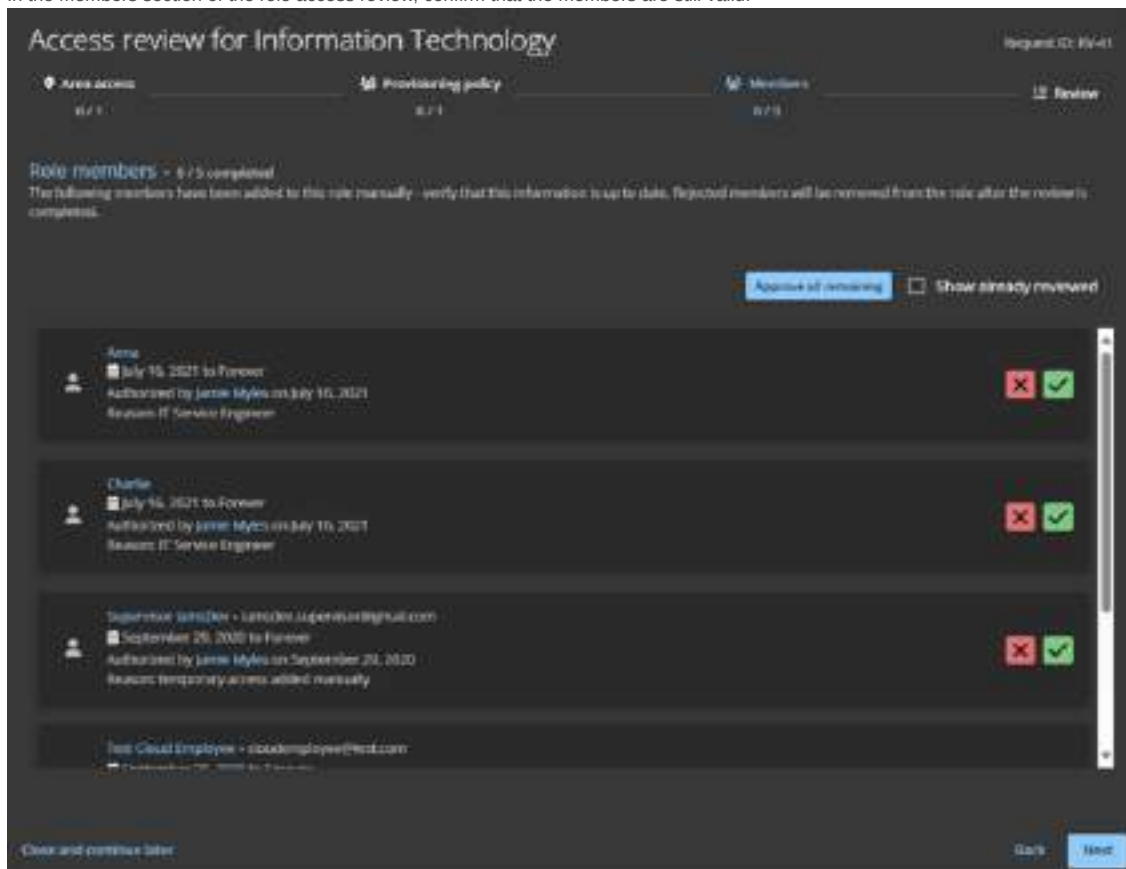


- a. Click Keep access () to confirm that access is still valid.
Tip: Use Approve all remaining to speed up approval process when the list is long, then remove any access that is no longer required.
 - b. Click Remove access () to remove access that is no longer required.
 - c. (Optional) Select Show already reviewed to go back and make modifications.
 - d. Click Next to continue to the next section of the access review wizard.
6. In the Provisioning policy section of the role access review, confirm that the policies are still valid.



- a. (Optional) Click view or edit the policy to open the Provisioning policy page to view or make changes to the policy.
- b. Click Approve policy (✓) to confirm that policy is still valid.
- c. Click Next to continue to the next section of the access review wizard.

7. In the Members section of the role access review, confirm that the members are still valid.



- a. Click Keep access (✓) to confirm that access is still valid.
Tip: Use Approve all remaining to speed up approval process when the list is long, then remove any access that is no longer required.
- b. Click Remove access (X) to remove access that is no longer required.
- c. (Optional) Select Show already reviewed to go back and make modifications.

d. Click Next to continue to the next section of the access review wizard.

8. In the Review section of the role access review, verify that the review details are correct.

Access review for Information Technology Report ID: RW-41

Area access 1 / 1 Provisioning policy 1 / 1 Members 5 / 5 [Review](#)

Warning: No changes can be made to this access review after it is completed. Ensure that all information is up to date and valid before completing the review.

Additional notes
Enter any additional information or comments relevant to this access review. The comments or additional information are not monitored by an administrator and are for audit viewing purposes only.

Additional notes

When this access review is completed, the following changes will be made:

- Information Technology will have access revoked for 0 users.
- No changes to the role provisioning policy.
- 3 members will be removed from Information Technology.
- A report will be created for this access review, which can be found in the Reports section.

[Close and continue later](#) [Back](#) [Complete](#)

a. In the Additional notes section, add any notes that you require.

b. Before you click Complete, review the changes summary immediately after the Additional notes section.

c. (Optional) If any of the information looks incorrect, click Back to return to previous sections and modify your changes.

d. If the Review section details are correct, click Complete.

After you finish

Generating an access review summary in ClearID

Browse

- [Access Reviews Feature Note \(2 pages\)](#)

7.16 | Completing an identity access review (supervisor) in ClearID

To ensure security compliance or audit readiness you can perform identity access reviews to check your direct reports areas and roles access. These periodic reviews are completed by a supervisor.

What you should know

- Supervisors can complete an identity access review from the My tasks page of the Dashboard or from an email notification.
- No changes can be made to an access review after it has been completed.
- All Completed reviews are retained for audit and tracking purposes.

Procedure

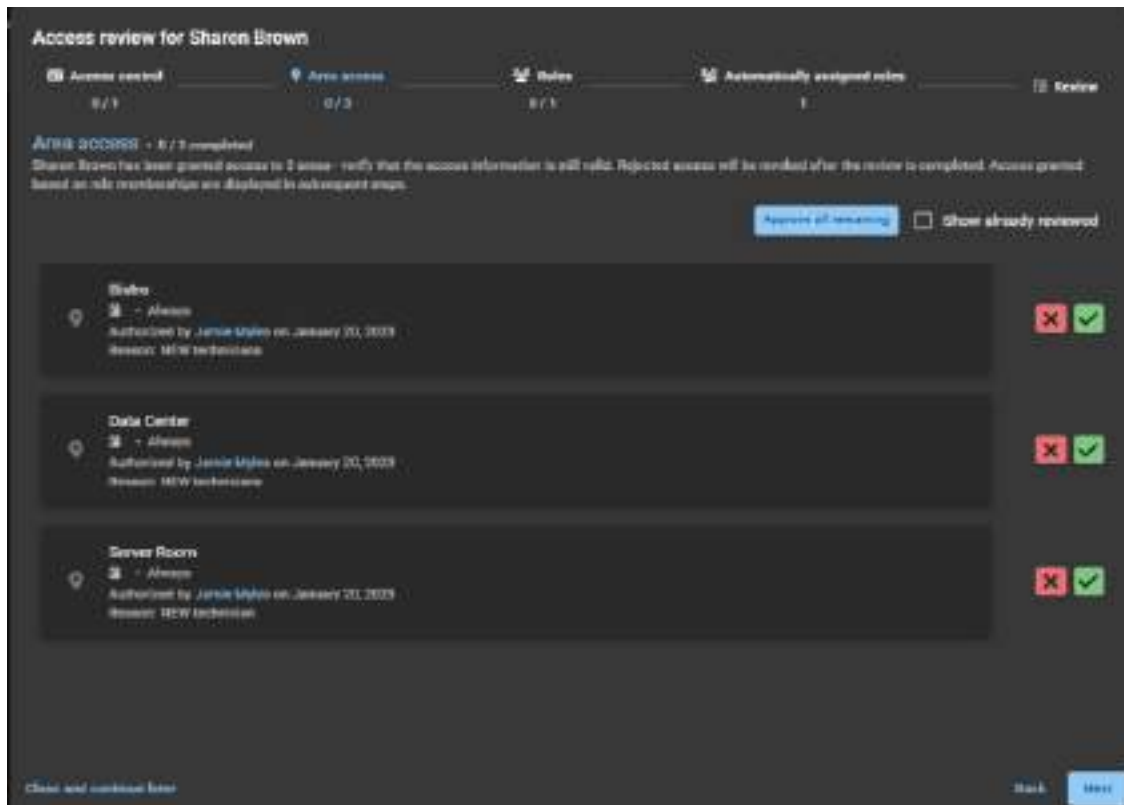
1. Click Dashboard > My tasks.
2. In the My tasks list, click the identity access review that you require.



3. Click Continue review.
4. In the Access control section, review the access control.

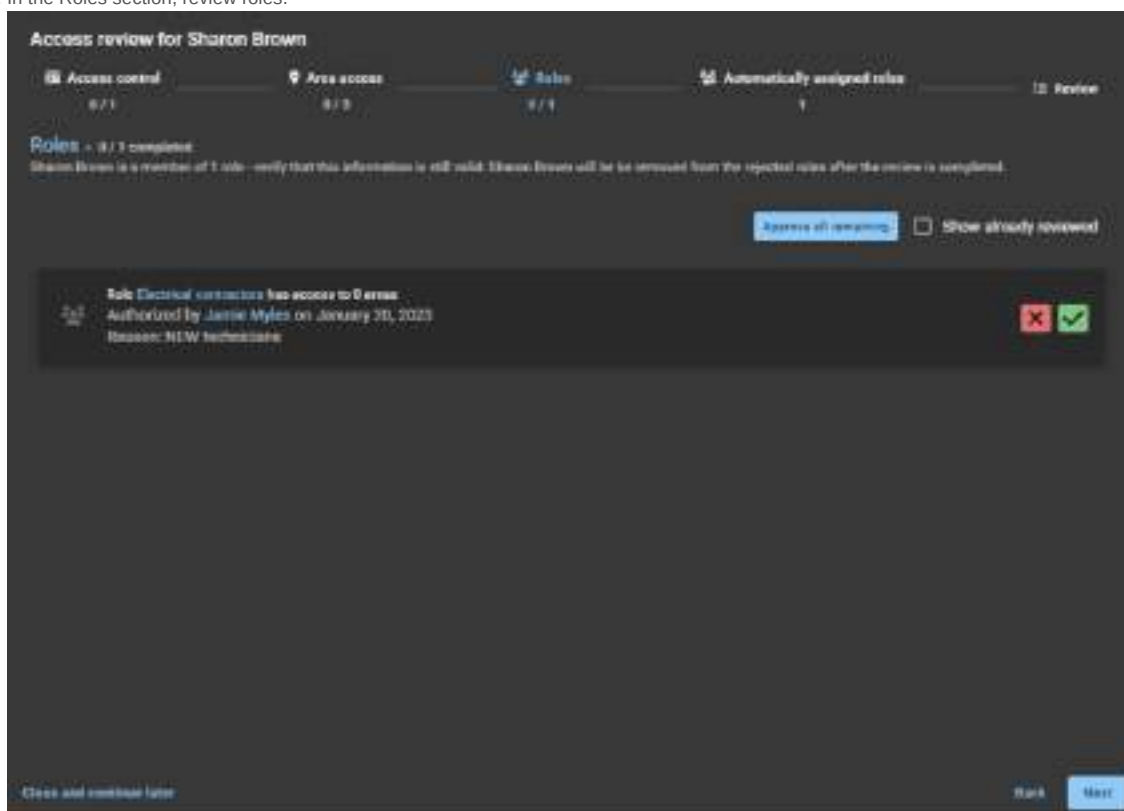


- a. (Optional) If you want to extend the amount of time doors are unlocked (after access is granted) for cardholders with the property "extended grant time" turned on, select the Person requires extended grant time checkbox.
 - b. (Optional) Enter or select an Activation date MM/DD/YYYY and time HH:MM.AM for the cardholder.
If the activation fields are left blank the default current date and time are used.
 - c. (Optional) Enter or select an Expiration date MM/DD/YYYY and time HH:MM.AM for the cardholder.
When the expiration fields are blank, the cardholder never expires.
 - d. Click Approve to approve the access control settings.
NOTE: After an Activation date or Expiration date has been specified, you must include a time. Otherwise, the Approve button is disabled.
 - e. (Optional) If you change your mind about the settings, you can repeat the previous steps to make further modifications and then click Approve again.
 - f. Click Next to continue to the next section of the access review wizard.
5. In the Area access section, review the area access.



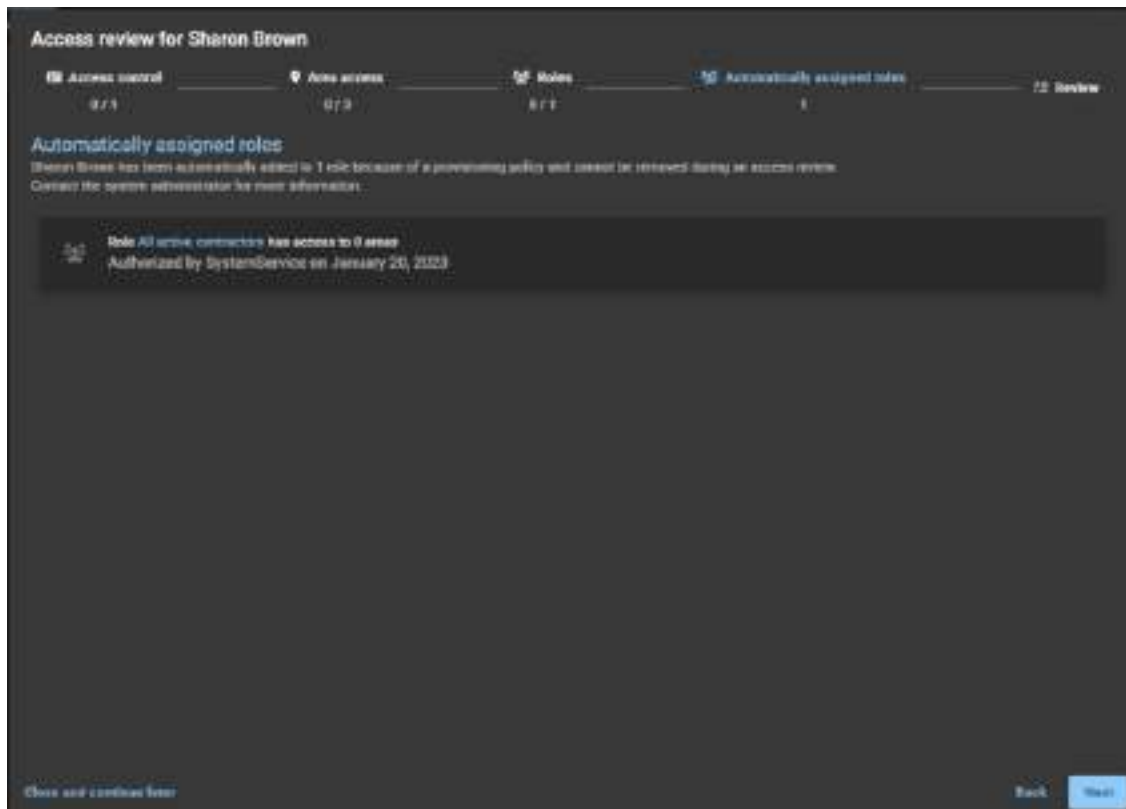
- Click Keep access (🟢) to confirm that access is still valid.
Tip: Use Approve all remaining to speed up approval process when the list is long, then remove any access that is no longer required.
- Click Remove access (🔴) to remove access that is no longer required.
- (Optional) Select Show already reviewed to go back and make modifications.
- Click Next to continue to the next section of the access review wizard.

6. In the Roles section, review roles.



- Verify the role information and either Keep access or Remove access as required.
- Click Next to continue to the next section of the access review wizard.

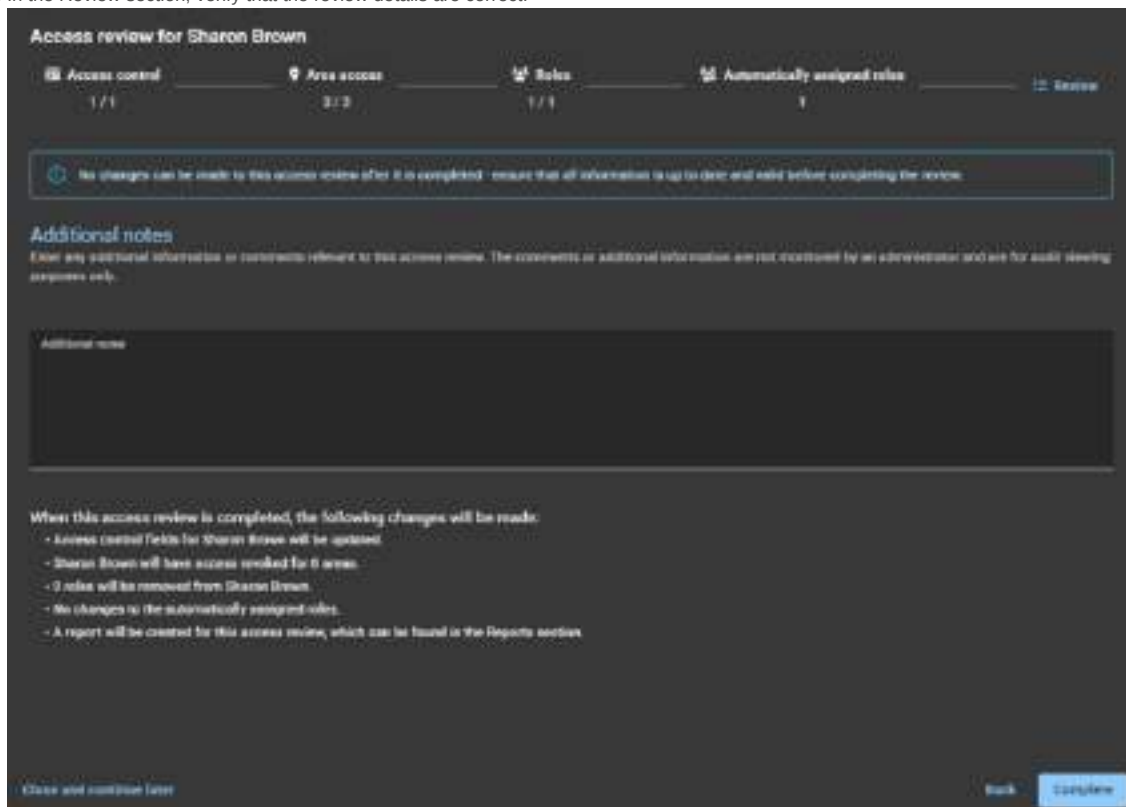
7. In the Automatically assigned roles section, review the automatically assigned roles.



The automatically assigned roles information here is useful context for a supervisor to review for accuracy and understand. It includes other access direct reports might have in addition to their manually assigned area access.

NOTE: Supervisors cannot modify any of this information because the roles were automatically assigned based on setup performed by an account administrator. If any automatically assigned roles information is no longer applicable, the account administrator should be contacted.

8. In the Review section, verify that the review details are correct.



- a. In the Additional notes section, add any notes that you require.
- b. Before you click Complete, review the changes summary immediately after the Additional notes section.
- c. (Optional) If any of the information looks incorrect, click Back to return to previous sections and modify your changes.
- d. If the Review section details are correct, click Complete.

9. Repeat this process as required for each identity listed in your My tasks dashboard inbox.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Generating an access review summary in ClearID

7.17 | Generating an access review summary in ClearID

You can generate an access review summary for any completed access review to share with an auditor or other members of your organization.

Before you begin

Complete your access reviews.

What you should know

You can only generate an access review summary for a single completed access review.

Procedure

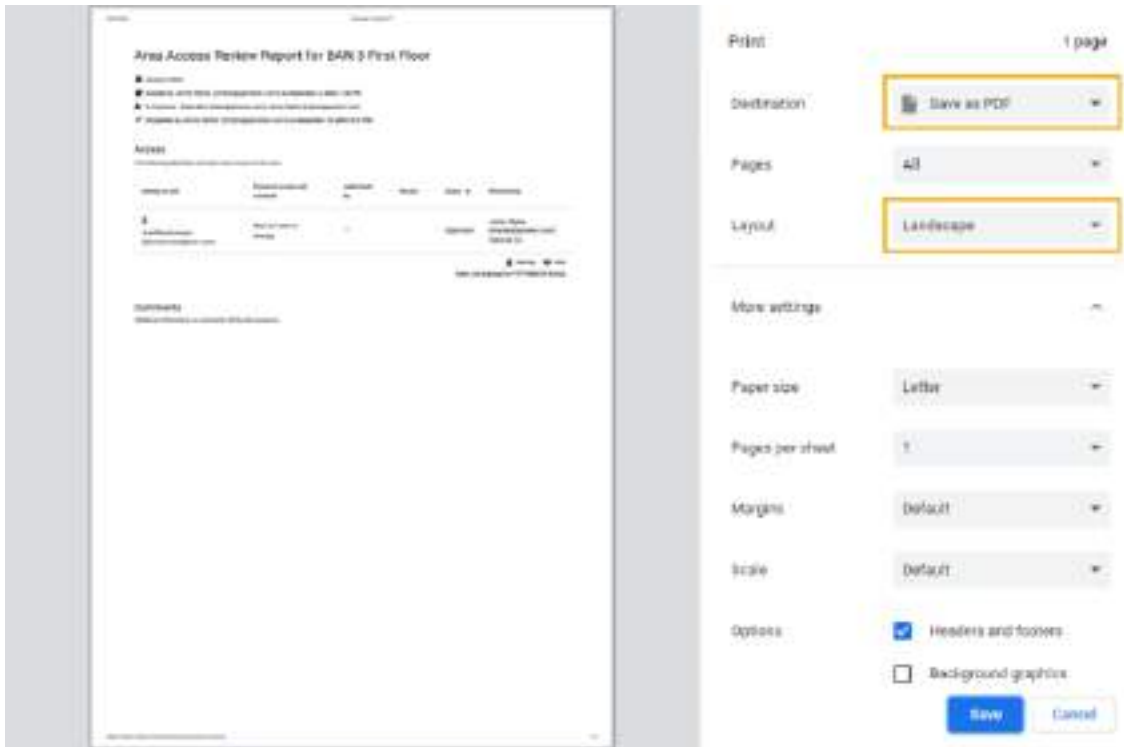
1. From the Home page, click Reports > Access reviews.
2. Configure report column filters to narrow report results as required.
 - a. Click the Status filter and select Completed.
 - b. In the Review item column, click the review item for the *completed* access review that you require.
3. Click Print.

NOTE: The layout Portrait option and the Background graphics checkbox option are not supported.

4. In the Print section, select an option from the Destination list.

Typically the report is either sent to a printer for a hardcopy output, or saved as a PDF so that it can be sent to auditors or shared by email. Other destination options are also available.

Best Practice: In the Layout list, select Landscape for the best viewing experience.



IMPORTANT: The options displayed in the Print dialog vary depending on your browser, your local computer and attached peripherals, and your organizations setup.

- (Optional) In the More settings section, select the Headers and footers option if you want to include the Date and the report Filename in the heading of the report.
- If you selected a printer, click Print and follow the on-screen prompts.
- If you selected Save as PDF, click Save and follow the on-screen prompts.

Tip: Use a file name that makes your access review reports easy to find during an audit or organization review. Include all useful information: area, role or group, and date. For example, Data Center - Access Review July 2020, Server Room - Access Review August 2020, or IT Department - Access Review Sept 2020. The default file name is <Area or Role name> - Access Review YYYY-MM-DD.pdf.

Results

Your report has now been printed or saved as a PDF for reference later.

After you finish

You can now share the access review report with an auditor or other members of your organization.

7.18 | About access requests report in ClearID

In Genetec ClearID™, an access requests report is a list of access requests for a specific site. The report includes information about the access request date, area requested, status, requested by, requested for, and period of access.

Access requests report

Access requests report					
		Download CSV		Display time in local +	Sanctus Head Office -
Request date	Area	Status	Requested by	Requested for	Access dates
July 16, 2021, 3:36 PM	Server Room	Approved	Jessie	Avin	From July 16, 2021, 4:00 AM To August 1, 2021, 3:59 AM
July 16, 2021, 7:06 PM	Server Room	Approved	Jessie	Charlie	From July 16, 2021, 4:00 AM To August 15, 2021, 3:59 AM
July 16, 2021, 7:06 PM	2nd Floor	Waiting for approvals	Jessie	Charlie	From July 16, 2021, 4:00 AM To August 15, 2021, 3:59 AM
December 15, 2020, 9:24 PM	2nd Floor	Cancelled	Jessie	Test Cloud Employee	From December 15, 2020, 9:00 AM To January 1, 2021, 4:59 AM
December 15, 2020, 9:24 PM	Server Room	Approved	Jessie	Test Cloud Employee	From December 15, 2020, 9:00 AM To January 1, 2021, 4:59 AM
December 15, 2020, 8:07 PM	2nd Floor	Approved	Jessie	Charlie	From December 15, 2020, 9:00 AM To January 1, 2021, 4:59 AM
1-17 of 17 total results.					

The access requests report is used by *area owners* and *site owners* to check the status of all access requests for a specific site and all the associated areas. The report can also be used to provide access request information to auditors.

Filters can be used to help refine the report search results by request date, area, status, requested by, requested for, and period of access. Browse

- [Checking the status of access requests in ClearID](#)

7.19 | Checking the status of access requests in ClearID

As *Area owners* and *Site owners* you can check the status of access requests at the site level for areas associated with a specific site. Using the Access request report, you can ensure that the organization is security-compliant, audit ready, and that the requests are processed in a timely fashion.

Before you begin

You must be an *Area owner* or *Site owner* to view the Access requests report and check the status or progress of access requests.

Procedure

1. From the Dashboard, click Reports > Access requests.
Tip: You can filter the results to suit different requirements. For example, to look for overdue requests, you can filter for Waiting for approvals in the Status column.

Request date	Area	Status	Requested by	Requested for	Access dates
July 16, 2021, 3:36 PM	Server Room	Approved	Janice	Anne	From July 16, 2021, 4:00 AM To August 1, 2021, 3:59 AM
July 16, 2021, 7:06 PM	Server Room	Approved	Janice	Charlie	From July 16, 2021, 4:00 AM To August 15, 2021, 3:59 AM
July 16, 2021, 7:06 PM	2nd Floor	Waiting for approvals	Janice	Charlie	From July 16, 2021, 4:00 AM To August 15, 2021, 3:59 AM
December 15, 2020, 9:24 PM	2nd Floor	Canceled	Janice	Test Cloud Employee	From December 15, 2020, 9:00 AM To January 1, 2021, 4:59 AM
December 15, 2020, 9:24 PM	Server Room	Approved	Janice	Test Cloud Employee	From December 15, 2020, 9:00 AM To January 1, 2021, 4:59 AM
December 16, 2020, 8:07 PM	2nd Floor	Approved	Janice	Charlie	From December 15, 2020, 9:00 AM To January 1, 2021, 4:59 AM

- In the Access requests report page, select the required display time format. Choose one of the following:

Display time in local

Show report times using the system time from the computer of the logged-in user.

Display time in UTC

Show report times using Coordinated Universal Time (UTC).

Display time in site time zone

Show report times using the time zone of the site.

- From the sites list, select the site for which you want to review access requests.
- In the Request date column, select one of the options, or click Date range and specify a date and time range to display a list of access reviews.
 - If you selected Date range, use the calendar picker to select the date range that you require.
NOTE: The time period for request date is limited to a maximum of 1 year.
 - (Optional) To sort the report results by Request date in ascending () or descending () order, click .
- In the Area column, click  to filter the results by area name.
 - Search for an area or select one or more check boxes to filter the results by the areas that you require.
 - Click the Area name hyperlink to display and verify the area details.

Tip: To revoke an access request, click the Area name hyperlink in the report, then click Access and click  next to a user.
- In the Status column, click  to filter the results by status.
 - Select one or more check boxes to filter the results by the statuses that you require (Submitted, Waiting for approvals, Denied, Approved, Canceled, or Completed).
 - (Optional) Click the Status hyperlink to display the access request.
NOTE: If you're an approver, you can Approve or Deny the pending access request while viewing the request.
- In the Requested by column, click  to filter the results by access requester.
 - Enter a user name or email address in the search field.
 - (Optional) Click the Requested by hyperlink to display summary details about the requester.
- In the Requested for column, click  to filter the results by access recipient.
 - Select one of the following:

All
Displays all identity and role access requests.

An identity
Select An identity, then enter an identity in the search field when you want to filter access requests for a specific identity.

A role
Select A role, then enter a role in the search field when you want to filter access requests for a specific role.
 - (Optional) Click the Requested for hyperlink to display summary details about the recipient.
- In the Period of access column, click  to filter the results using a date range.
- Click Download CSV, to download a copy of the access requests report in CSV format. The report can then be used for auditing purposes, to keep a physical copy, to attach to an audit request, to review offline, or to manipulate or consolidate data in a spreadsheet for other audiences.
 - Follow your browser prompts to complete downloading the exported file.

Genetec ClearID® User Guide

Displayed in the header

The file is exported as a .CSV file to the default download location for your browser. By default the exported file is created using the name of your site. For example, AccessRequest_yoursitename_fromdate_to_todate.csv (AccessRequest_Genetec_Montreal_2024-09-14.csv).

NOTE: The columns and entries in the CSV file can vary depending on the filters you've selected when you download the report.

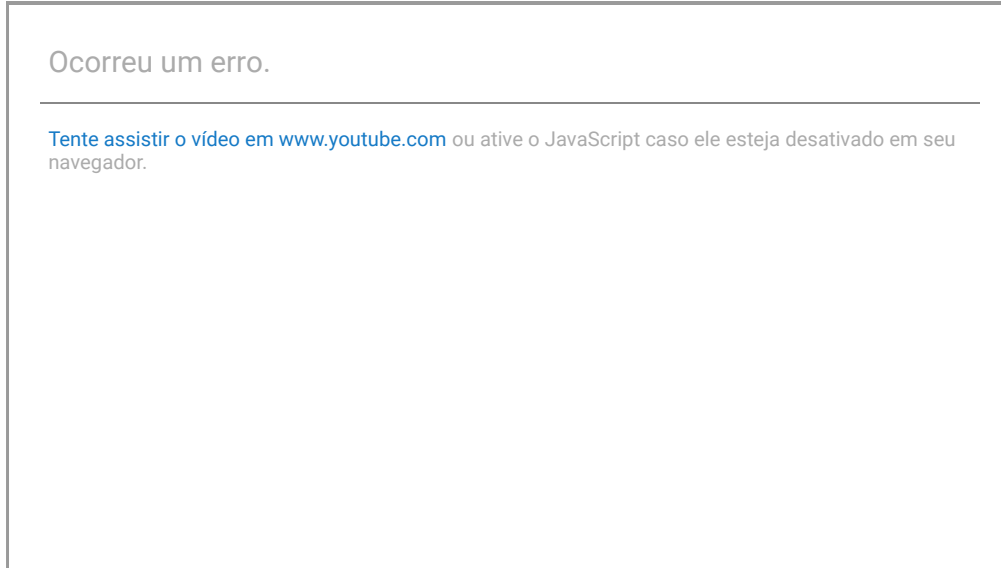
11. (Optional) Click  to reset filter selections.

Results

You have now checked the status of all access requests at a site level for all areas associated with a specified site.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.



After you finish

Approve or reject access requests as required:

- Approving area access requests in ClearID
- Rejecting area access requests in ClearID

Browse

- About access requests report in ClearID
- Requesting access in ClearID

7.20 | About site activity report in ClearID

In Genetec ClearID™, a site activity report is an audit trail of activities or events for a specific site. The report includes timestamp information, activity type, area, who activity was performed by, and a details section including reason information.

Site activity report

Site activity report

Download CSV

Display time in UTC

Genetec Head Office

Timestamp	Activity type	Area	Performed by	Details
August 13, 2021, 4:04 AM	Identity access removed	Server Room	System	Charlie has been removed from Server Room. Reason: Expired
August 1, 2021, 4:04 AM	Identity access removed	Server Room	System	Anna has been removed from Server Room. Reason: Expired
July 16, 2021, 3:38 PM	Identity access granted	Server Room	System	Anna granted access to Server Room. Reason: Contractor (highest access)
July 16, 2021, 2:06 PM	Identity access granted	Server Room	System	Charlie granted access to Server Room. Reason: System engineer requires access to Server room

1-4 of 4 total results

The site activity report is used by *site owners* to check audit trail events at a site level. The report can also be used to provide site activity information to auditors.

Filters can be used to help refine the report search results by timestamp, activity type, area, performed by, and details.

Browse

- Viewing a site activity report in ClearID

7.21 | Viewing a site activity report in ClearID

You can view a site activity report to review an audit trail of activities or events for a specific site.

Before you begin

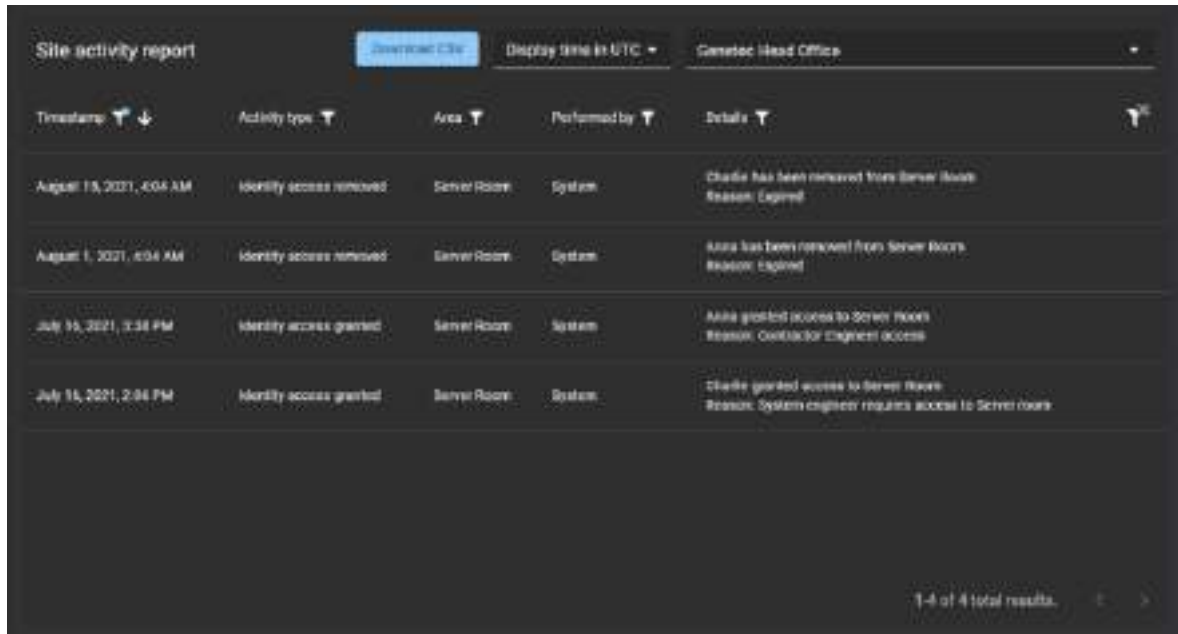
- Add area owners and managers
- Add role members
- Request access

What you should know

Only a site owner can view a Site activity report to review an audit trail of activities or events for a specific site.

Procedure

- From the homepage, click Reports > Site activity.



The screenshot shows the 'Site activity report' interface. At the top, there's a 'Download CSV' button, a 'Display time in UTC' dropdown, and a site selector 'Genetec Head Office'. Below is a table with columns: Timestamp, Activity type, Area, Performed by, and Details. The table contains four rows of activity logs. At the bottom right, it says '1-4 of 4 total results.' with navigation arrows.

Timestamp	Activity type	Area	Performed by	Details
August 18, 2021, 4:04 AM	Identity access removed	Server Room	System	Charlie has been removed from Server Room Reason: Expired
August 1, 2021, 4:04 AM	Identity access removed	Server Room	System	Anna has been removed from Server Room Reason: Expired
July 16, 2021, 1:38 PM	Identity access granted	Server Room	System	Anna granted access to Server Room Reason: Contractor Engineer access
July 16, 2021, 2:04 PM	Identity access granted	Server Room	System	Charlie granted access to Server Room Reason: System engineer requires access to Server room

2. In the Site activity report page, select the display time that you require. Choose one of the following:

Display time in local

Report times are displayed using the system time from the computer of the logged in user.

Display time in UTC

Report times are displayed using Coordinated Universal Time (UTC).

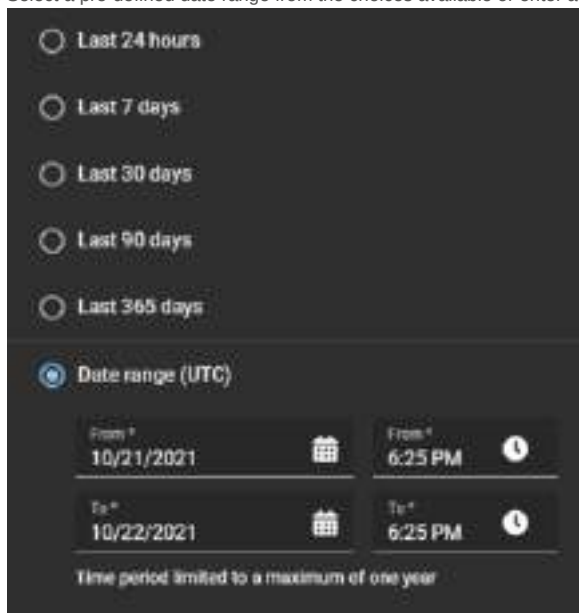
Display time in site time zone

Report times are displayed using the time zone of the site.

3. From the sites list, select the site that you require.

4. In the Timestamp column, click  to filter the results by date.

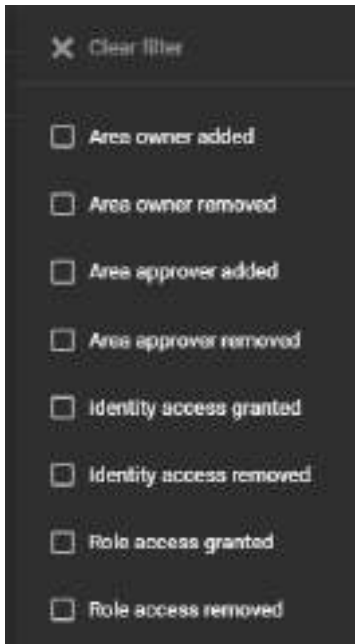
a. Select a pre-defined date range from the choices available or enter a specific date range using the date range picker.



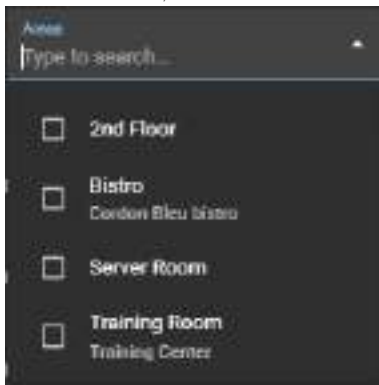
The screenshot shows a date range picker menu. It has radio buttons for 'Last 24 hours', 'Last 7 days', 'Last 30 days', 'Last 90 days', 'Last 365 days', and 'Date range (UTC)'. The 'Date range (UTC)' option is selected. Below it, there are two date pickers: 'From' (10/21/2021) and 'To' (10/22/2021). There are also time pickers for 'From' (6:25 PM) and 'To' (6:25 PM). At the bottom, it says 'Time period limited to a maximum of one year'.

b. (Optional) Use the sort icons ( and ) to display the results in descending or ascending order.

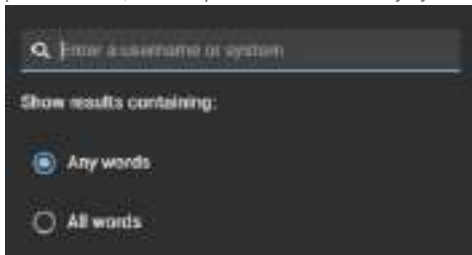
5. In the Activity type column, click  to filter the results by activity type.



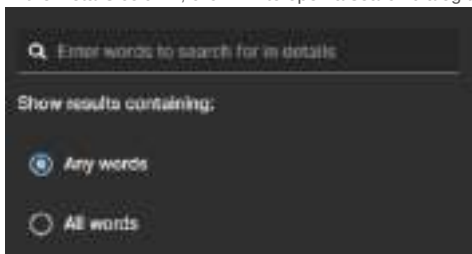
6. In the Area column, click  to filter the results by area.



7. In the Performed by column, click  to open a search dialog and filter the results by who performed an activity. For example, tasks performed by a particular user, or tasks performed automatically by the system.



8. In the Details column, click  to open a search dialog to search the details or reason using a search criteria.



9. Click Download CSV, to download a copy of the site activity report in CSV format. The report can then be used for auditing purposes, to keep a physical copy, to attach to an audit request, to review offline, or to manipulate or consolidate data in a spreadsheet for other audiences.

a. Follow your browser prompts to complete downloading the exported file.

The file is exported as a .CSV file to the default download location for your browser. By default the exported file is created using the name of your site. For example, *yoursitename_fromdate_to_todate_SiteActivityReport.csv* (Genetec Head Office_from_2020-10-22_to_2021-10-22_SiteActivityReport.csv).

NOTE: The columns and entries in the CSV file can vary depending on the filters you have selected when you download the report.

10. (Optional) Click  to reset filter selections.

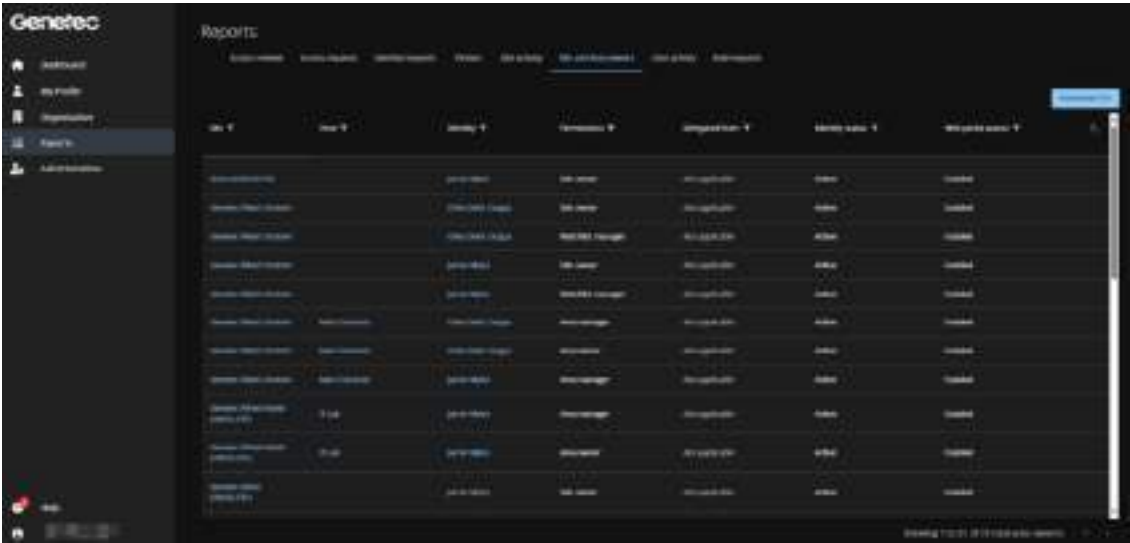
Browse

- About site activity report in ClearID

7.22 | About site and area owners report in ClearID

In Genetec ClearID™, a site and area owners report is a list that provides a global view of the following identities and their permissions: site owner, area manager, area owner, and watchlist manager. The report includes site, area, identity, identity permission, delegated from, identity status, and web portal access information.

Site and area owners report



The site and area owners report is used by account administrators to get a global view of all identities and their permissions. When the report is used by a site owner, only information about their own sites is shown.

Filters can be used to help refine the report search results by site, area, identity, permissions, delegated from, identity status, and web portal access.

Browse

- Viewing a site and area owners report in ClearID

7.23 | Viewing a site and area owners report in ClearID

You can view a site and area owners report to get a global view of all identities and their permissions.

Before you begin

Ensure that you have assigned identities for the following:

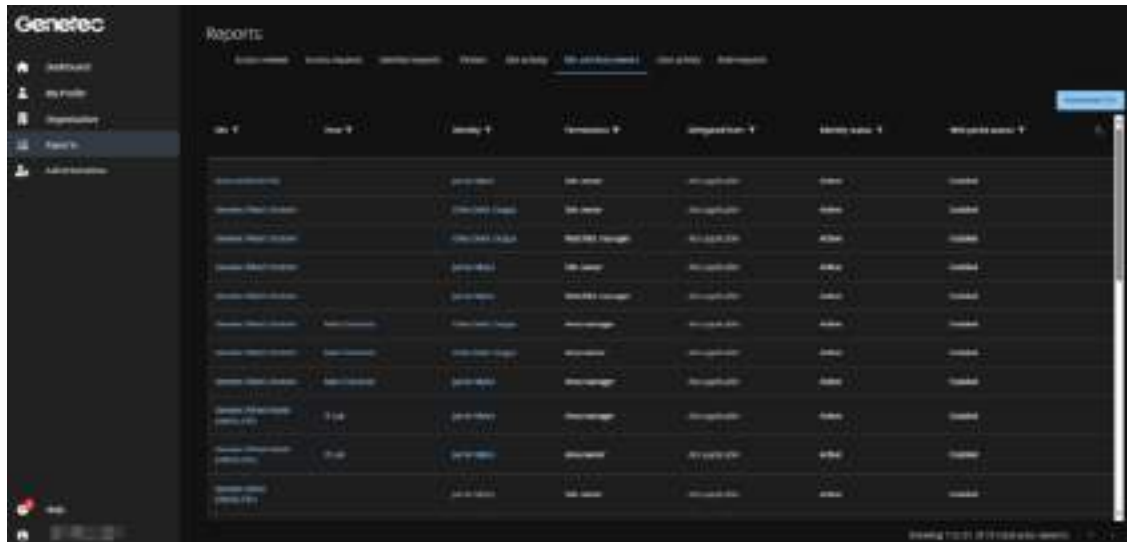
- Site owners
- Area owners and managers
- Watchlist managers

What you should know

Only an account administrator or site owner can view a Site and area owners report to review all identities and their permissions. When the report is used by a site owner, only information about their own sites is shown.

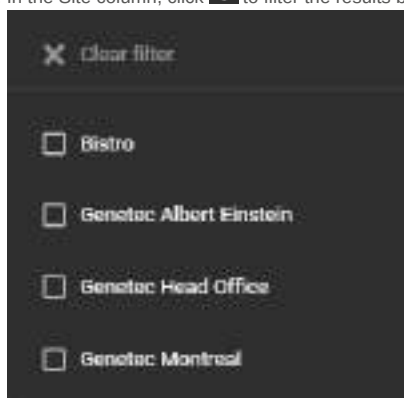
Procedure

1. From the homepage, click Reports > Site and Area owners report.

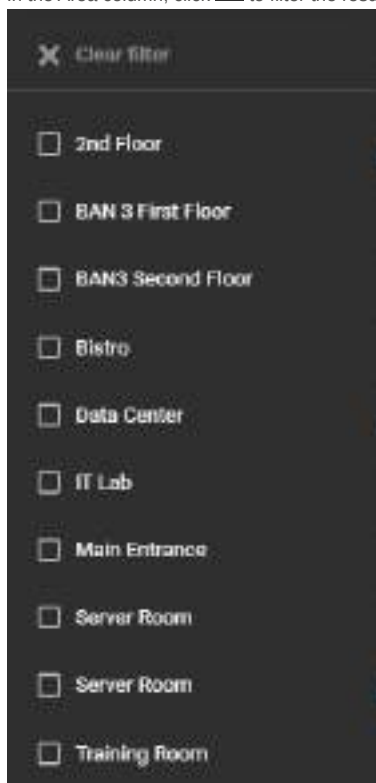


2. In the Site and area owners report page, select the filters that you require.

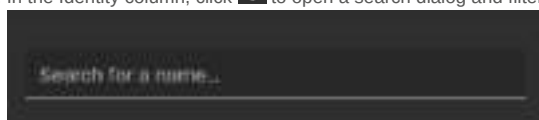
a. In the Site column, click  to filter the results by site.



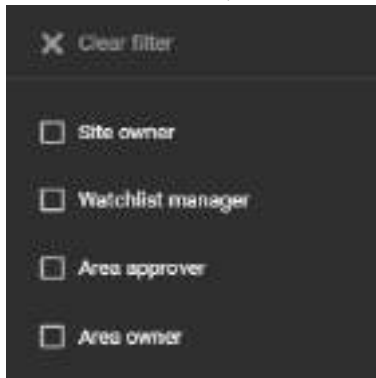
b. In the Area column, click  to filter the results by area.



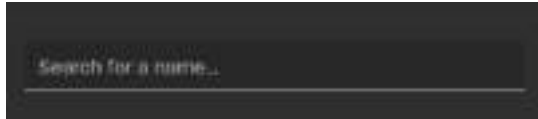
c. In the Identity column, click  to open a search dialog and filter the results by an identity.



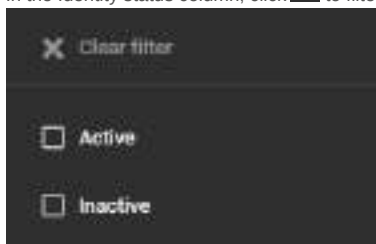
d. In the Permissions column, click  to filter the results by permission type.



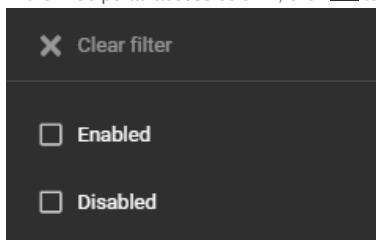
e. In the Delegated from column, click  to open a search dialog and filter the results by a person delegating tasks.



f. In the Identity status column, click  to filter the results by identity status.



g. In the Web portal access column, click  to filter the results by web portal access.



3. Click Download CSV, to download a copy of the site and area owners report in CSV format. This report format can be used for auditing purposes, to keep a physical copy, to attach to an audit request, to review offline, or to manipulate or consolidate data in a spreadsheet for other audiences.

a. Follow your browser prompts to complete downloading the exported file.

The file is exported as a .CSV file to the default download location for your browser. By default the exported file is created using the report name and download date. For example, SiteAreaOwners_2022-02-14.csv.

NOTE: The columns and entries in the CSV file can vary depending on the filters you have selected when you download the report.

4. (Optional) Click  to reset filter selections.

Browse

- [About site and area owners report in ClearID](#)

8 | Managing areas

8.1 | About areas in ClearID

In Genetec ClearID™, an area is a logical entity that defines the relationship between Synergis™ doors and area owners. Areas are managed by the area owner.

Doors are not managed in Genetec ClearID™, doors are managed in Security Center:

- Managing doors from ClearID is impractical due to the distance from the hardware.
- A door must be properly configured in Security Center and linked to the hardware physically managing the door.
- After areas are created in ClearID and synchronized in Security Center, doors can then be added to those areas in Security Center.
NOTE: Doors moved under areas inherit the access rules of the area.
- Door setup is performed in Security Center separately from the areas. After both *doors* and *areas* are present in Security Center, doors must be added to areas.

Browse

- [Adding doors to areas in ClearID](#)

8.2 | Creating areas in ClearID

In Genetec ClearID™, an area is a logical entity that defines the relationship between Synergis™ doors and area owners. Areas are managed by the area owner.

Before you begin

- Create your sites.

What you should know

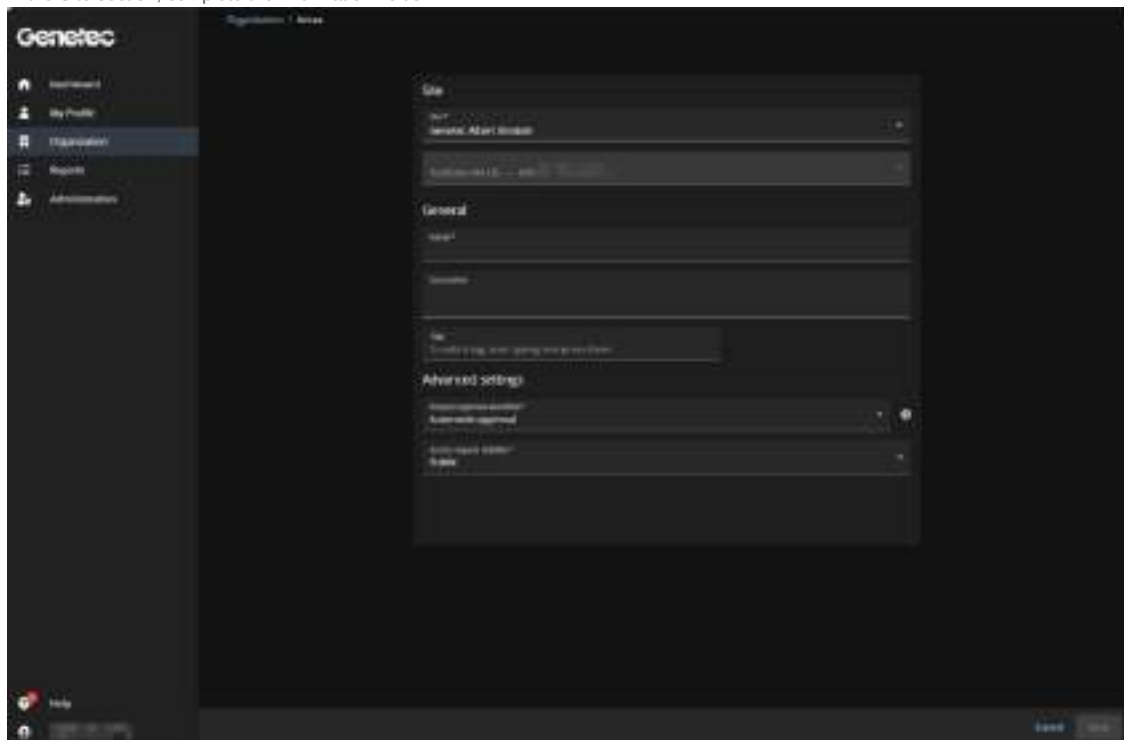
- Only account administrators or *site owners* can create areas in Genetec ClearID™.
- In Genetec ClearID™, an area owner is an identity with authority over an area. The owner can define the policy for an area, assign area managers, give or remove access, and approve or deny access requests for an area.
- An *area* is bound to or associated with a Security Center system.

Procedure

1. Click Organization > Areas.
2. Click Create area.

NOTE: Mandatory fields are highlighted in the user interface with an asterisk (*).

3. In the Site section, complete the information fields:



Site

From the Site list, select the site that you want to associate your area with.

Access control system

This field is prefilled based on the previously selected site. This access control system is used to synchronize changes in ClearID back to Security Center.

NOTE: If a warning message is displayed instead of the associated ACS information, click the link to return to the site configuration and enter the associated ACS information.

- a. In the General settings section, complete the information fields:

Name

Enter an area name.

Description

Enter a description that indicates the geographical location of the building or physical area.

Tags

Enter alternative keywords or search term categorizations that might be used to find the area.

- b. In the Advanced settings section, select the options that you require:

Request approval workflow

Choose the approval workflow option that you require:

Automatic approval

Area requests are automatically approved using a role-based policy.

Area managers

Area requests are manually approved by authorized area managers.

Role managers or supervisor and area managers

Area requests for roles are manually approved by role managers, and requests for identities are manually approved by supervisors. Then, requests are manually approved by authorized area managers.

Role managers or supervisors

Area requests for roles are manually approved by role managers, and requests for identities are manually approved by supervisors.

Visibility

Choose the visibility option that you require:

Public

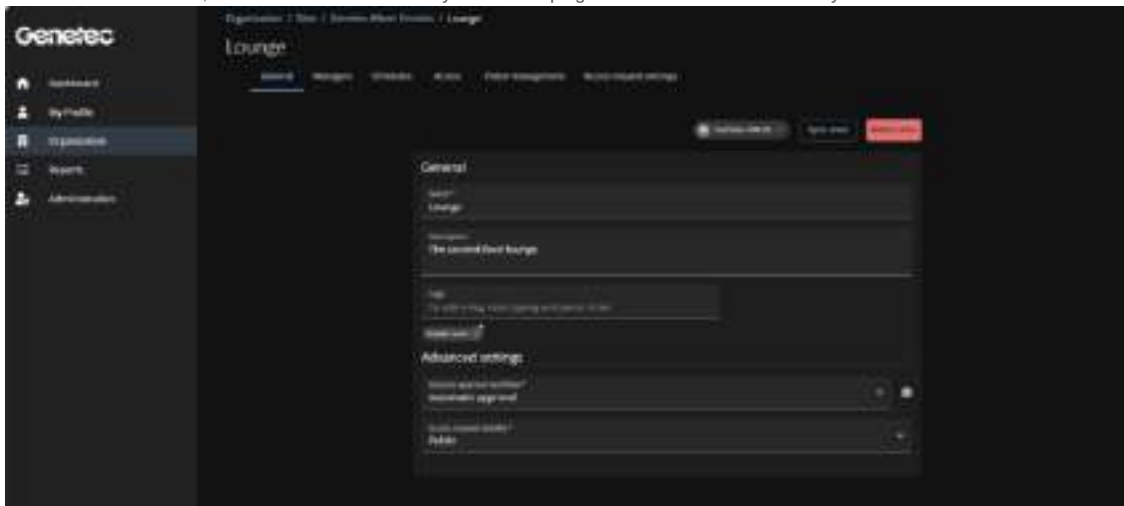
The area is visible to everyone and access requests can be created for the area. This is the default setting.

Private

The area is private and should be hidden, and access requests are not supported for the area.

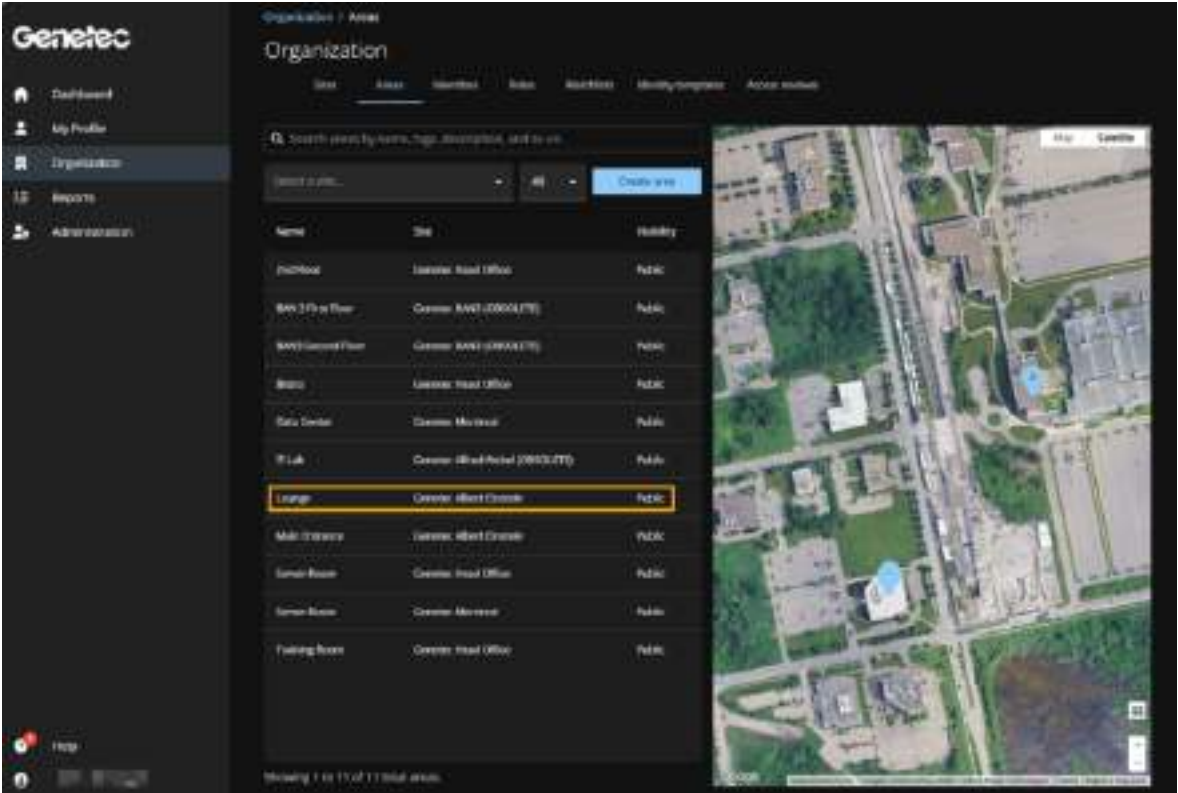
4. Click Save.

When the area is saved, commands are automatically sent to the plugin to create an area in Security Center.



Results

Your area has now been created in ClearID.



Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Add area managers.

8.2.1 | Adding doors to areas in ClearID

Before you can submit access requests or invite visitors, you must add the doors in your areas to the associated areas that were automatically created in Security Center by Genetec ClearID™.

Before you begin

Create your areas.

What you should know

- Only Config Tool users with the *View door properties* privilege can add doors to areas in Security Center that are associated with areas in ClearID.
- When an area is created in ClearID, areas are automatically created in Security Center.
- Doors must then be added to the associated areas that are automatically created in Security Center.

Doors that are members of an area can be configured as *Captive* or *Perimeter* doors:

- Perimeter doors are used to enter and exit an area, and help to control access.
- Captive doors are used within an area.

Set the *door sides* correctly to ensure that *People counting* and *antipassback* are properly tracked. A door's *Entrance* and *Exit* sides are relative to the area being configured.

Procedure

1. From the Config Tool homepage, open the Area view task.
2. Select an area and then click the Properties tab.
3. In the Doors section, click Add an item () and select the doors that you want to link to your area.
4. For all doors in the Doors section, configure the door type:
 - If the door is used to enter or exit the area, set the slider to Perimeter.
 - If the door is located inside the area, set the slider to Captive.

NOTE: If a smaller area is nested inside a larger area, you do not need to add the perimeter doors of the smaller area as captive doors of the larger area. The system automatically organizes nested areas when calculating people counts and applying antipassback rules.

 - To swap the door sides, select the door and click Swap door side.
5. Click Apply.

Results

Your doors are now added to the areas in Security Center that are associated with ClearID areas.

After you finish

In ClearID, you can now [submit access requests](#) or [invite visitors](#).

Parent topic: [Creating areas in ClearID](#)

Browse

- [About areas in ClearID](#)

8.2.2 | Enabling visitor management for areas in ClearID

Before visitors can request an area visit, you must configure the visitor management settings for your area.

Before you begin

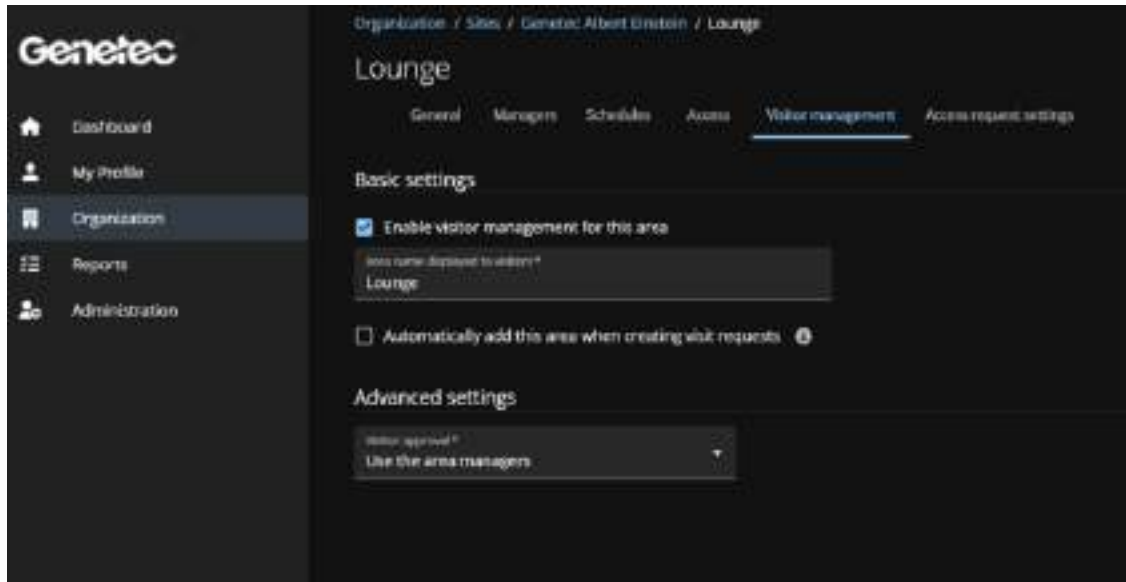
[Create your areas.](#)

What you should know

- Visitor management for areas is off by default.
- Only *area owners* or a *site owners* can enable visitor management for areas in Genetec ClearID™.
- The options displayed when a visit request is created vary depending on the users requesting access and also the settings that you configure here.

Procedure

1. Click Organization > Areas.
2. From the Areas list, select an area.
3. Under the Visitor management tab, configure the following options:



Basic settings

Select the Enable visitor management for this area option to enable visitor management for this area.

Area name displayed to visitors

Enter the area name that you want displayed in email notifications sent to visitors.

Automatically add this area when creating visit requests

If you select this option, all guests in your visit request are automatically granted access to the requested area.

Advanced settings

If you want to define guest access in your visit request, then specify the required approvers:

Visitor approval

Choose the approvers for visitor access from the following options:

Automatically approve visitors

Automatically approve access requests for this area.

Use the area managers

Only area managers can approve or deny access requests for this area.

Define visit approvers

Only people in the Visit approvers list can approve or deny access requests for this area.

4. Click Save.

Results

Visitor management is enabled for the area.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Access requests or visit requests can now be submitted for this area.

Parent topic: Creating areas in ClearID

Browse

- About workflows in ClearID

8.2.3 | About nested areas in Security Center

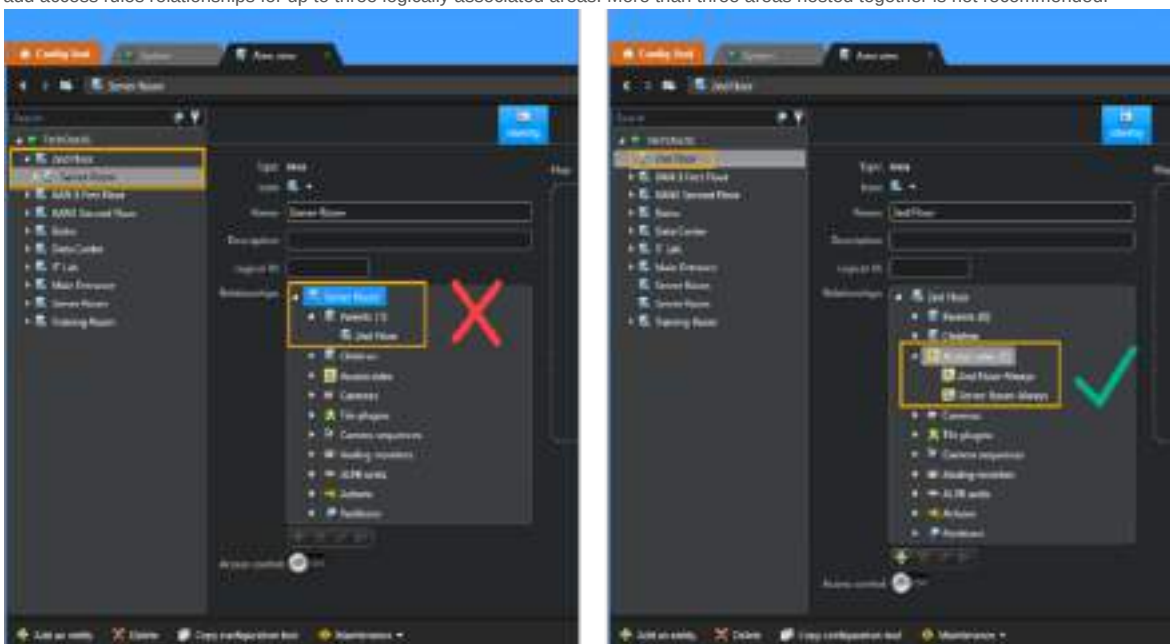
In Security Center, nested areas can be used to logically group areas so that access can be automatically granted to people for associated nested areas when access is requested in Genetec ClearID™ for one of the nested areas.

Nested areas are useful for organizations with lots of restricted areas, lots of logical grouping, or area dependencies. For example, when secure areas require access to other areas to get to the secure area:

- Example 1: Requesting access to a server room might automatically grant access to the floor that the server room is on.
- Example 2: Requesting access to a restricted area might automatically grant access to the floor the restricted area is on, and also grant access to the building that the floor and restricted area are in.

NOTE: In Config Tool, nesting areas using Parents or Children options in the Relationships section of the Area view does not inherit access.

Best Practice: Nest areas using Access rules options in the Relationships section of the Area view to inherit the required access. You can create nested areas to add access rules relationships for up to three logically associated areas. More than three areas nested together is not recommended.



Adding multiple access rules to an area creates the logical group association for nested areas. This relationship association ensures that the areas automatically grant access to the other associated areas when access is requested for one of the nested areas. By default ClearID automatically creates access rules for each schedule that is added to an area.

IMPORTANT: If the schedules for any of the nested areas change, the area relationships (access rules) must be configured again.

Parent topic: [Creating areas in ClearID](#)

Browse

- [Granting access to areas in Security Center automatically](#)

8.2.4 | Granting access to areas in Security Center automatically

To automatically grant access for people to logically grouped areas, you can create nested areas for Genetec ClearID™ in Security Center.

Before you begin

- [Create the areas that you require.](#)
- [Learn about nested areas.](#)
- Plan the logical grouping of your areas before configuring your nested areas to automatically grant or inherit access.

What you should know

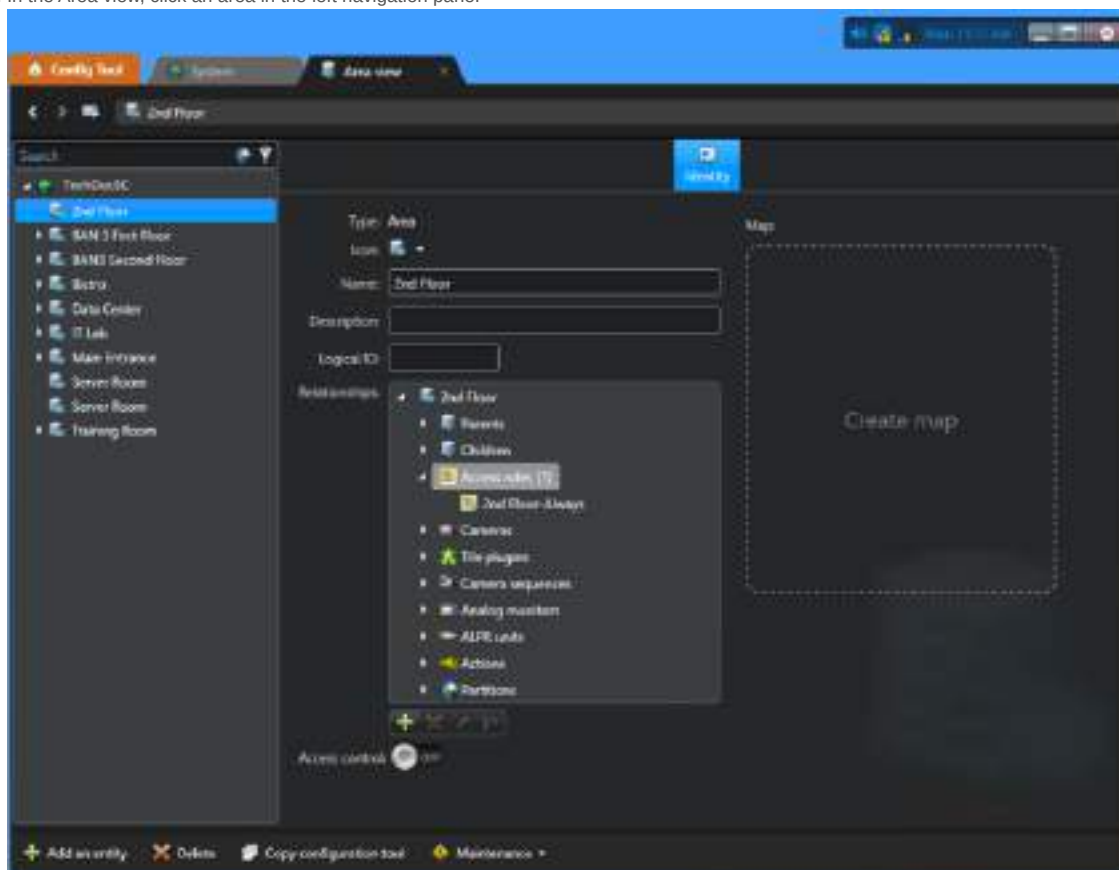
Only a Security Center administrator or system integrator can configure or map the nested areas.

If the schedules for any of the nested areas change, the area relationships (access rules) must be configured again.

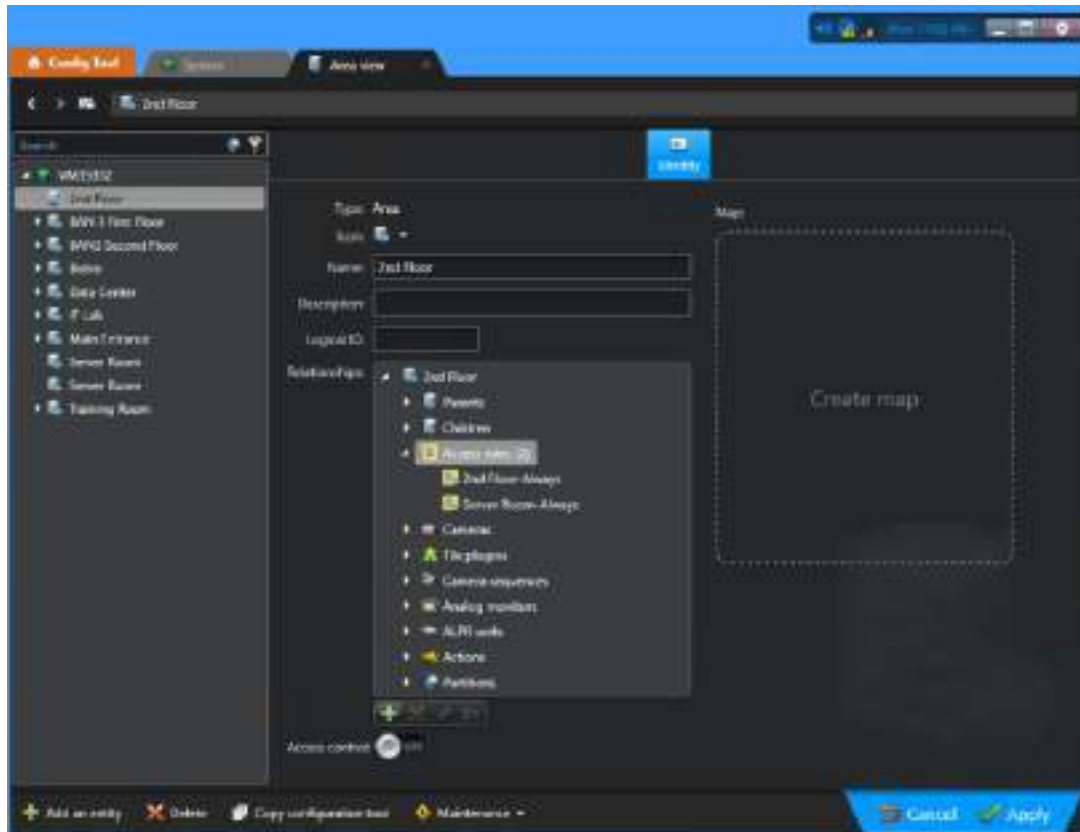
Best Practice: Nest areas using Access rules options in the Relationships section of the Area view to inherit the required access. You can create nested areas to add access rules relationships for up to three logically associated areas. More than three areas nested together is not recommended.

Procedure

1. From the Config Tool homepage, open the Area view task.
2. In the Area view, click an area in the left navigation pane.



3. In the Identity tab Relationships section, double-click Access rules.
 - a. Click Insert an item  then search for and select the *access rules* that contain the required schedules for the *areas* that you want to associate with the area selected earlier in step 2.



Tip: You can also click Entity type and select the Access rule checkbox, then click Search to only display access rules in the entity list.

b. (Optional) Repeat for other areas.

4. Click Apply.

When an access request is received for an area that is part of a group of areas, access is automatically granted based on the relationships defined for the areas. In the previous example, anyone who has access to the Server Room is also automatically granted access to the 2nd floor.

Parent topic: [Creating areas in ClearID](#)

8.3 | Adding area owners and managers in ClearID

Before you can define policies for an area, assign area managers, or approve or deny access requests for an area, you must add your area owners and managers.

Before you begin

Create your areas.

What you should know

- Only *area owners* or *site owners* can add area owners and managers in Genetec ClearID™.
- In Genetec ClearID™, an area owner is an identity with authority over an area. The owner can define the policy for an area, assign area managers, give or remove access, and approve or deny access requests for an area.
- In Genetec ClearID™, an area manager is an identity with approval authority over an area. The manager can give or remove access and approve or deny access requests for an area. They are also responsible for approving area access reviews.

Procedure

1. Click Organization > Areas.
2. From the Areas list, select an area.
3. Click Managers.
4. Use the Search field or click Add managers to add an area owner or manager.
5. Select the required user or users and click Confirm.
6. Select the Role type for the user or users you added:
 - Manager
 - Owner
 - Both



7. Click Save.

Results

The selected people are added to the area as an owner, a manager, or both.

After you finish

Adding schedules to an area in ClearID.

8.4 | Adding schedules to an area in ClearID

Before you can grant people access to an area, you must add schedules to your areas.

Before you begin

Define schedules in Security Center. For more information, see [Creating schedules](#).

What you should know

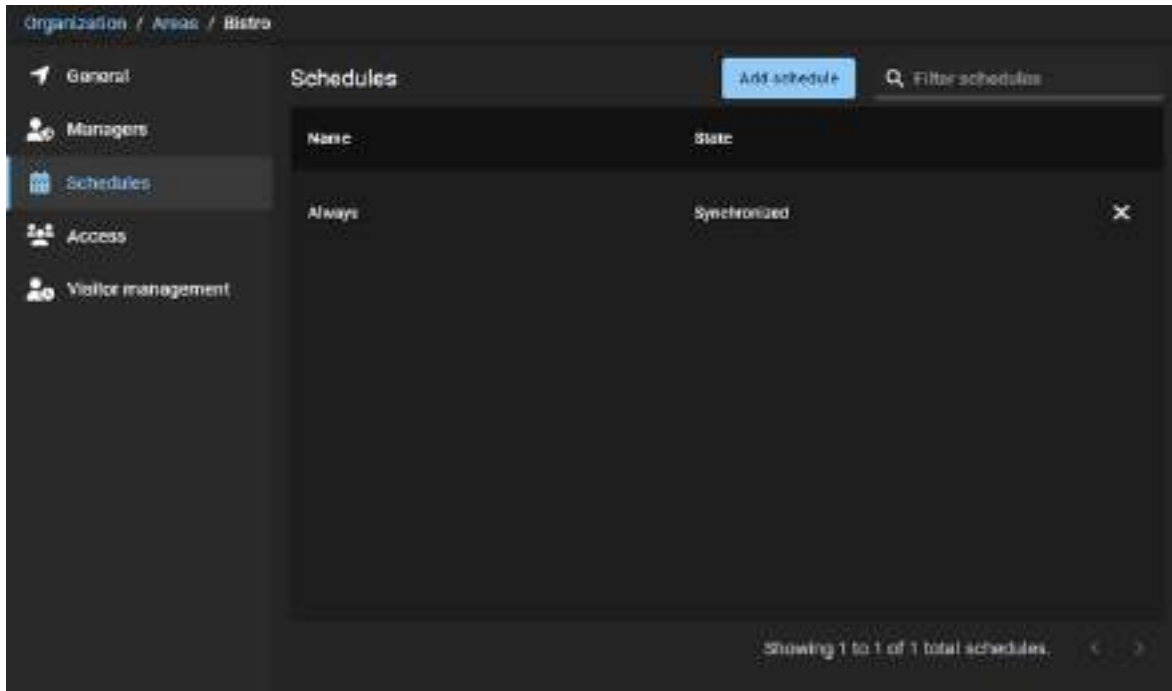
- Only *area owners* can add schedules to an area in Genetec ClearID™.
- A schedule is an entity that defines a set of time constraints that can be applied to a multitude of situations in the system. Each time constraint is defined by a date coverage (daily, weekly, ordinal, or specific) and a time coverage (all day, fixed range, daytime, and nighttime).
- The schedules that are available for selection vary depending on the schedules defined in the Security Center access control system that is selected when you create your area.
- Some schedule examples include: Always, Weekdays, Weekend, 09:00-17:00, and so on.
- When a schedule is added to an area, an *access rule* is automatically created in Security Center. The *area-schedule* access rule defines the schedule that is associated with the area. ClearID automatically adds and removes access for a *cardholder* or *cardholder group* listed in the access rule based on the schedule specified in ClearID.

Procedure

1. Click Organization > Areas.
2. From the Areas list, select an area.
3. Click Schedules.
4. Click Add schedule to configure your area schedule.
 - a. Enter a search term and click Search (🔍).
 - b. Select a schedule from the list and click Confirm.
This list only shows schedules that are not already in your Schedules list.
 - c. (Optional) Repeat previous substeps to add additional schedules.
5. (Optional) Click Remove (✖) to remove any schedules that are no longer required.
6. Click Save.

Results

Your schedules have been added to the area.



After you finish

Grant access to your area.

8.5 | Configuring access request documents for areas in ClearID

For areas with extra security measures or requirements, *Site owners* and *Area owners* can make it mandatory for employees to upload supporting documents like copies of drivers licenses or certifications when requesting access to areas.

Before you begin

Familiarize yourself with [access request workflows](#).

What you should know

- As a *Site owner*, you can manage supporting document requirements for site-level access requests.
- Site or area owners can configure more supporting document requirements at the area level.
- You can configure up to 20 supporting document types per area.

Procedure

1. In the Genetec ClearID™ web portal, click Organization > Site > Area > Access request settings.
2. (*Site owner*) Under Supporting document settings from site, select the radio button to choose whether or not the specific area inherits supporting document requirements configured at the site level:

Include site documents

Access requests use the supporting documents for the area in addition to any existing supporting document settings specified for the site.

Exclude site documents

Access requests only use the supporting documents for the area, excluding the supporting document settings for the site.

NOTE: Include site documents is selected by default for areas. *Site owners* can change these settings.

3. Under Define supporting documents for area, click Add area document.

Access request documents

Supporting document settings from site

Select supporting document settings to inherit from the site for this area.

☒ **Include site documents**
Access requests will only use the supporting documents for this area in addition to any existing supporting document settings specified for the site.

☐ **Exclude site documents**
Access requests will use the supporting documents for this area only, excluding the supporting document settings for the site.

Define supporting documents for area Add area document

Configure the following supporting document fields. These mandatory or optional supporting document fields are displayed to users when submitting access requests.

Certificate of qualification
Required • Enabled

Driver's license
Required • Enabled

Work permit
Required • Enabled

- In the Display name field, enter a name for the document type.
 - Select Show this field in access requests to display the document field in access requests.
Tip: When the checkbox is cleared, the document type remains available in draft mode.
 - Choose whether or not uploading the document is mandatory when submitting an access request by clicking the Required or Optional radio button.
- NOTE: You can configure a combination of mandatory and optional document types to appear in a single access request.

Add document field

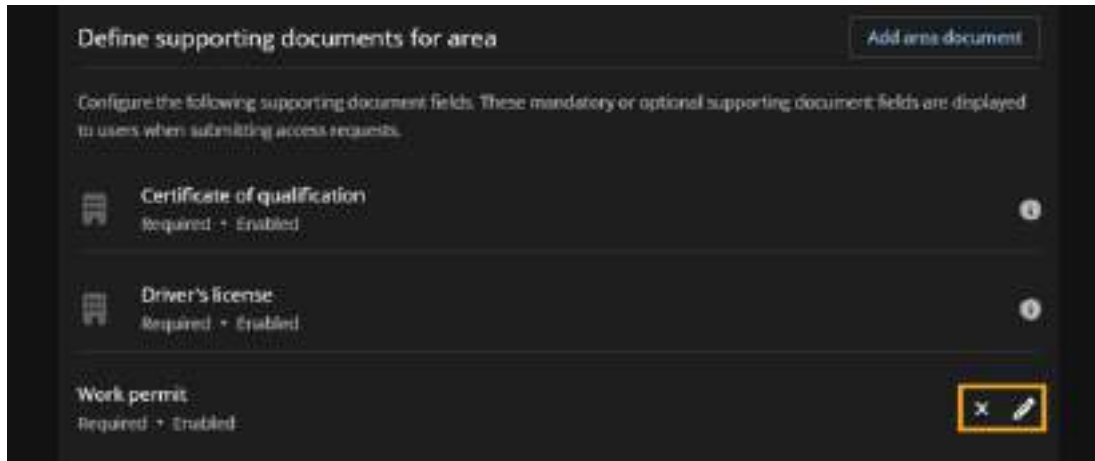
Display name *
Driver's license

☒ **Show this field in access requests**

☒ **Required** ☐ **Optional**

Cancel Add

- Click Add.
- (Optional) You can use the icons to modify or remove each document type:



- Click  to modify the configuration of a supporting document.
- Click  to remove a configured supporting document.

8.6 | Granting access to an area in ClearID

To grant people access to an area, you must add identities or roles to an area and schedule access on a person-by-person or role-by-role basis.

Before you begin

[Add schedules to your areas.](#)

What you should know

- Only *area owners*, *area managers*, and supervisors can grant people or roles access to an area.
- The Access page shows all the identities, roles, and visitors that currently have access to the area.

Procedure

- Click Organization > Areas.
- From the Areas list, select an area.
- Click Access.
- Select a filter from the following:



All

- If all the filter icons for access request type are available () , all access request types are displayed.
- If all the filter icons for access request type are unavailable () , all access request types are hidden.

Identity access ()

Show or hide identity access.

Role access ()

Show or hide role access.

Visit request ()

Show or hide visit requests.

- Click Add access.
 - In the Grant area access dialog, select either Identities or Roles.
- If you selected Identities, complete the fields:
 - Enter an identity name and click Search () .
 - Select the identity name from the Identities list.
 - Search for or select the *schedule* that you require from the Schedule list.

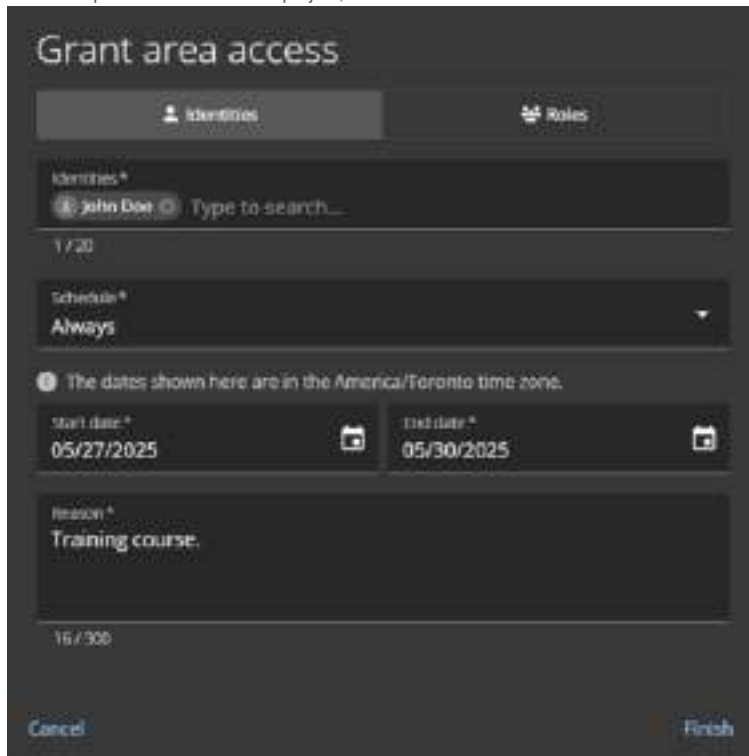
Some schedule examples include: Always, Weekdays, Weekend, 09:00-17:00, and so on.
 - Configure the period that you want the access for.

Start date
Launch a calendar picker to choose the date that the access should start. The default is Now.

End date
Launch a calendar picker to choose the date that the access should expire. The default is Forever.

Reason

(Optional) Enter a reason for the period of access that you require. For example, access required for a business partner conference, employee access required for a multi-week project, and so on.



e. Click Finish.



7. If you selected Roles, complete the fields:

- Enter a role name and click Search (🔍).
- Select the role name from the Roles list.
- Search for or select the *schedule* that you require from the Schedule list.
- Configure the period that you want the access for.

Start date

Launch a calendar picker to choose the date that the access should start. The default is Now.

End date

Launch a calendar picker to choose the date that the access should expire. The default is Forever.

Reason

(Optional) Enter a reason for the period of access that you require. For example, access required for a business partner conference, employee access required for a multi-week project, and so on.

Grant area access

Identities Roles

Roles *

Team C Type to search...

1 / 20

Schedule *

Always

The dates shown here are in the America/Toronto time zone.

Start date: 05/27/2025

End date: 05/30/2025

Reason *

Training course.

16 / 300

Cancel Finish

e. Click Finish.

Genetec

Organization > Sites > Genetec ClearID Office > Training Room

Training Room

General Manager Schedule Access Visitor management Access request history

16 / 300

Role	Schedule	Valid from	Valid to	Authorized by	Reason	Action
Team C	Always	05/27/2025	05/30/2025	Team C	Training course	Remove
Team C	Always	05/27/2025	05/30/2025	Team C	Training course	Remove

8. (Optional) Click Remove (X) to revoke any access that is no longer required.

Results

Your access requests have been granted for this area.

8.7 | Reviewing area access in ClearID

To perform an audit or check who has access to an area, periodic reviews must be performed by an area owner, area manager, or site owner.

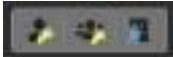
What you should know

Only *area owners*, *area managers*, and *site owners* can review area access.

This procedure describes how to verify who has access to a specified area, one area at a time.

Procedure

- 1. Click Organization > Areas.
- 2. From the Areas list, select an area.
- 3. Click Access.
- 4. Select an access request filter:



All

- If all the filter icons for access request type are available (), all access request types are displayed.
- If all the filter icons for access request type are unavailable (), all access request types are hidden.

Identity access ()

Show or hide identity access.

Role access ()

Show or hide role access.

Visit request ()

Show or hide visit requests.



5. Review the access list to identify any roles, identities, or visitors that can be removed or that require further investigation.

After you finish

Approve access requests or reject access requests.

Browse

- Setting up area access reviews in ClearID
- Completing an area access review (site owner) in ClearID

8.8 | Approving area access requests in ClearID

To approve area access requests, an *Area owner*, *Area manager*, a *Role manager*, or a *Supervisor* must review the pending approvals. They can then decide which requests to approve.

Before you begin

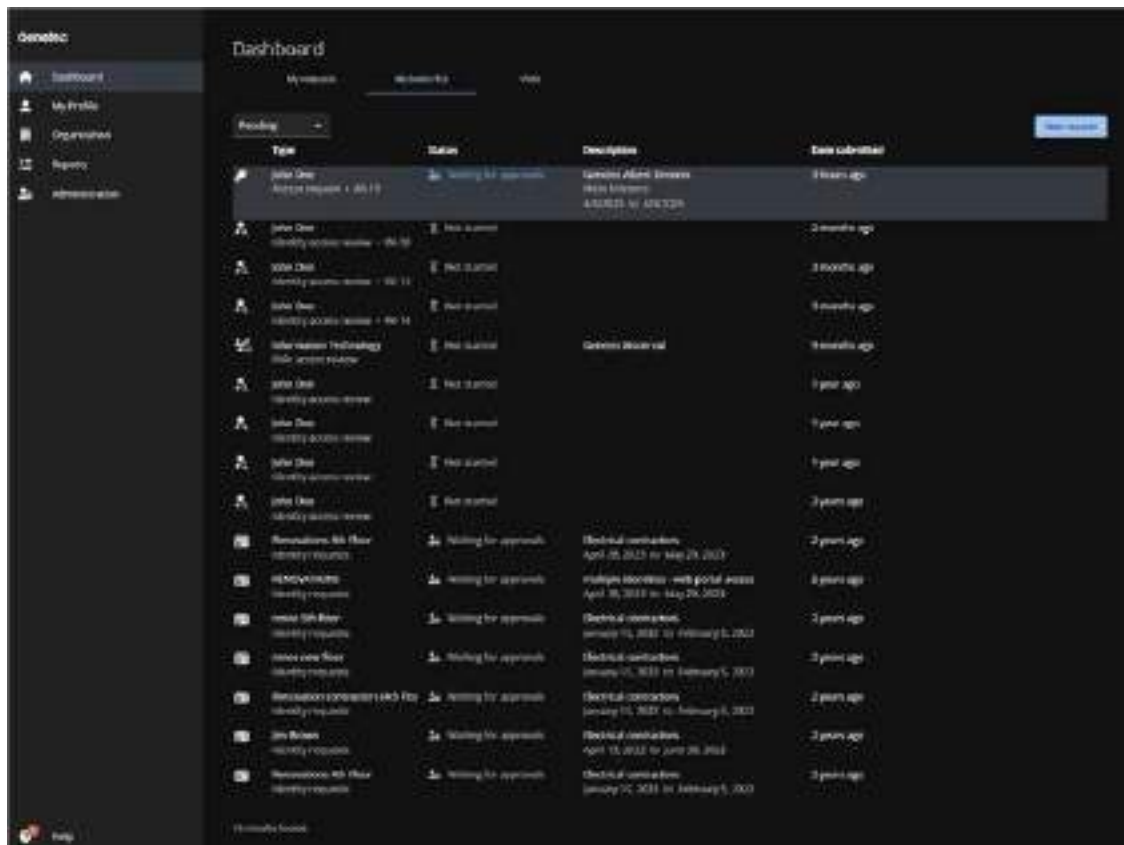
Ensure that some area access requests have already been submitted.

What you should know

Only *Area owners*, *Area managers*, role managers, or supervisors can approve area access requests.

Procedure

1. Click Dashboard > My tasks.



2. From the Status list, filter the tasks that are displayed:

Status

Select a status from the following:

All

Displays all pending or completed tasks.

Pending

Displays tasks waiting for approval.

Completed

Displays completed tasks and their status. For example, approved, completed, denied, or canceled.

3. Click an access request to display additional details about the request.

Access request for John Doe
Request ID: AR-19

Requested by Jack on April 2, 2025

Waiting for approvals

From: 04/03/2025 To: 04/04/2025 Schedule: Always

Genetec Albert Einstein — Main Entrance America/Toronto

Details history

Reason for request
Access required while performing maintenance work.

Mandatory documents
This access request has 3 mandatory document placeholders.

Driver's license * Certificate of qualification * Work permit *

Close Deny Approve

4. Review the request details and make any changes that you require.
Tip: You can modify the request if the request has an error or something that needs to change. For example, you can amend the dates due to an office closure, or amend the schedule to a more appropriate access schedule.
5. (Optional) In the History field, enter a comment about any changes you make to the access request.
6. Click Approve.
7. (Optional) In the Reason for approval field, enter a reason for the access approval.
8. Click Confirm.

Results

The area access requests are now approved. Employees or visitors are able to access the area during the periods specified in their access requests.

8.9 | Rejecting area access requests in ClearID

To reject area access requests, an *Area owner*, *Area manager*, a *Role manager*, or a *Supervisor* must review the pending approvals. They can then decide which requests to deny.

Before you begin

- Ensure that some area access requests have already been submitted.
- Review area access to identify access that is no longer required.

What you should know

Only *area owners*, *area managers*, role managers, or supervisors can reject area access requests.

Procedure

1. Click Dashboard > My tasks.

- Status**
Select a status from the following:
All
Displays all pending or completed tasks.

Displays tasks waiting for approval.

Displays completed tasks and their status. For example, approved, completed, denied, or canceled.

- Displayed in the footer
Page 247 of 473

The screenshot displays the 'Access request for John Doe' interface. At the top, it shows the request ID 'AR-19' and a status 'Waiting for approvals'. Below this, there are fields for 'From' (04/03/2025) and 'To' (04/04/2025), along with a 'Schedule' dropdown set to 'Always'. The location is specified as 'Genetec Albert Einstein — Main Entrance' and the area as 'America/Toronto'. The 'Details' tab is active, showing the 'Reason for request' as 'Access required while performing maintenance work.' and 'Mandatory documents' as 'This access request has 3 mandatory document placeholders.' Below these are three document upload buttons: 'Driver's license *', 'Certificate of qualification *', and 'Work permit *'. At the bottom right, there are 'Deny' and 'Approve' buttons.

4. Review the request details.
5. (Optional) In the History field, enter a comment about any changes you make to the access request.
6. Click Deny.
7. (Optional) In the Reason for denial field, enter the reason why the access request was denied.
NOTE: If the supporting access request documents are incorrect or not valid, you can notify the requester by including this information in the Reason for denial field. The requester will then have to resubmit an access request with valid supporting documents.
8. Click Confirm

Results

The area access requests are now rejected. Employees or visitors are no longer able to access the area.

8.10 | Creating exceptions to the access request approval workflow in ClearID

In Genetec ClearID™, an access request workflow is a series of activities performed by the system or authorized people during the life cycle of an access request. To bypass the access request workflow for certain types of requests or roles, you can modify an area's access request approval workflow settings.

Before you begin

Create an area and define its access request approval workflow.

What you should know

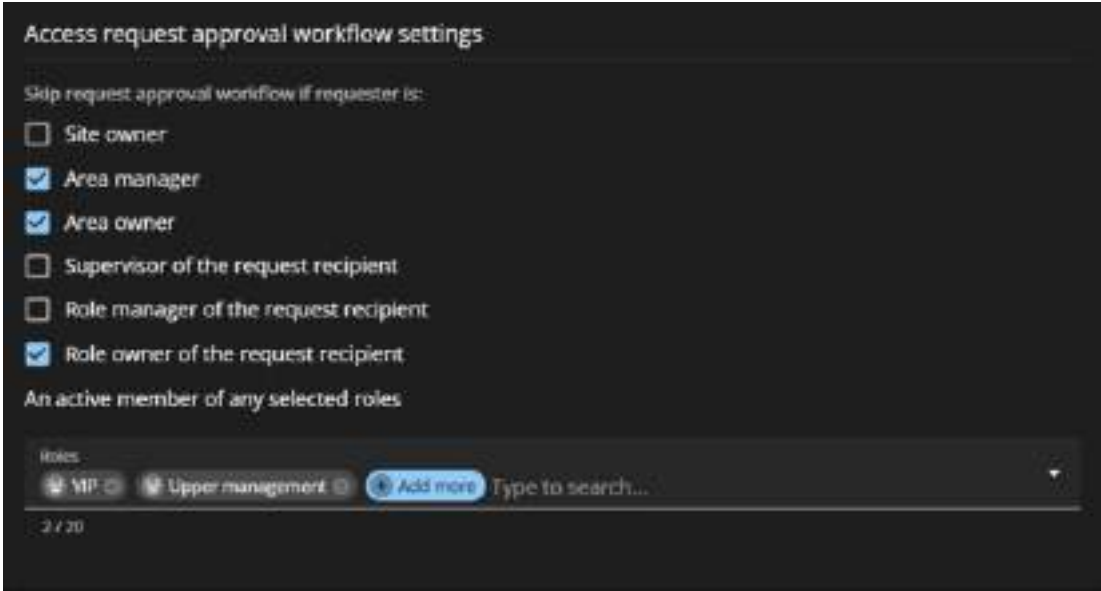
All access requests for an area must follow the steps for approval set by the chosen access request workflow. You can create exceptions to this approval process when certain users or roles make access requests.

For example, you can automatically approve access requests made for users who belong to a VIP or Upper Management role. You can also automatically approve requests if the requester is the Supervisor of the person for whom the request is made.

You must be a *Site owner* or *Area owner* to set exceptions to the access request approval workflow for an area.

Procedure

1. In the Genetec ClearID™ web portal, click Organization > Site > Area > General.
2. Under Access request approval workflow settings, define exceptions to the access request workflow set for the area as needed:
NOTE: If the request approval workflow is set to Automatic approval, the Access request approval workflow settings section is hidden.



Site owner

Automatically approve access requests when the requester is the *Site owner*.

Area manager

Automatically approve access requests when the requester is the *Area manager*.

Area owner

Automatically approve access requests when the requester is the *Area owner*.

Supervisor of the request recipient

Automatically approve access requests when the requester is the *Supervisor* of the identity that is the request recipient.

Role manager of the request recipient

Automatically approve access requests when the requester is the *Role manager* of the role for which the access request was made.

Role owner of the request recipient

Automatically approve access requests when the requester is the *Role owner* of the role for which the access request was made.

An active member of any selected role

Automatically approve access requests when the requester is a member of a listed role.

3. Click Save.

Browse

- [About workflows in ClearID](#)
- [About access request workflow in ClearID](#)

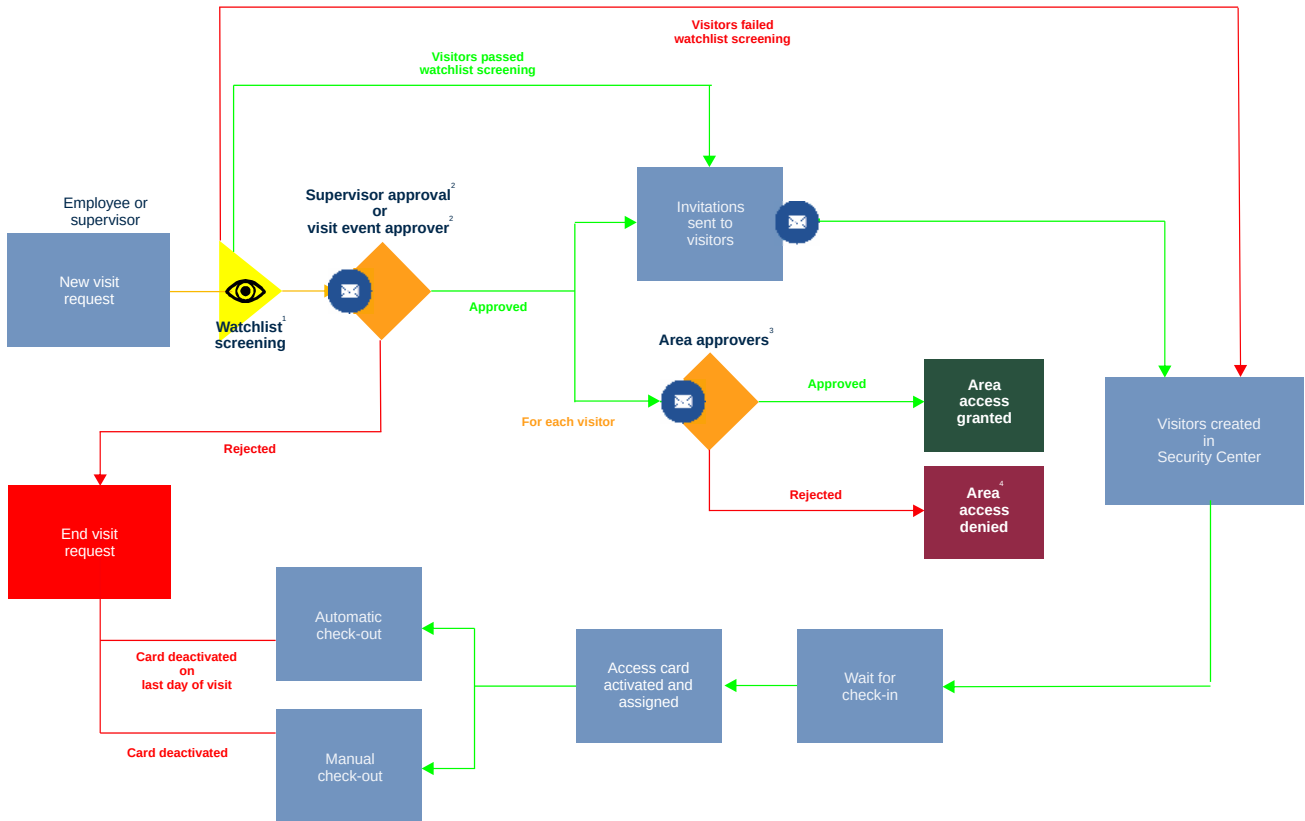
9 | Managing visitors

9.1 | About visit request workflow in ClearID

A visit request workflow is a series of activities performed by the system or authorized people during the life cycle of a visit request. The activities can change the state and properties of visit requests, affect other entities in the system, or wait for conditions to be met.

The workflow helps automate visit request tasks, such as approving or rejecting access requests, so that people involved in the review and approval process can focus on other tasks.

The following diagram illustrates the *visit request workflow* that occurs in Genetec ClearID™ and Synergis™.



¹ (Optional) For more information, see Visit request watchlist workflow.

² (Optional) Approval can be enabled or disabled for each site.

³ (Optional) Approval can be enabled or disabled for each area.

⁴ Visit event has been created and visitor has been created in Security Center but area access has been denied. Visitor might be able to access denied areas if escorted by a host, this access exception is at the discretion of the organization.

Browse

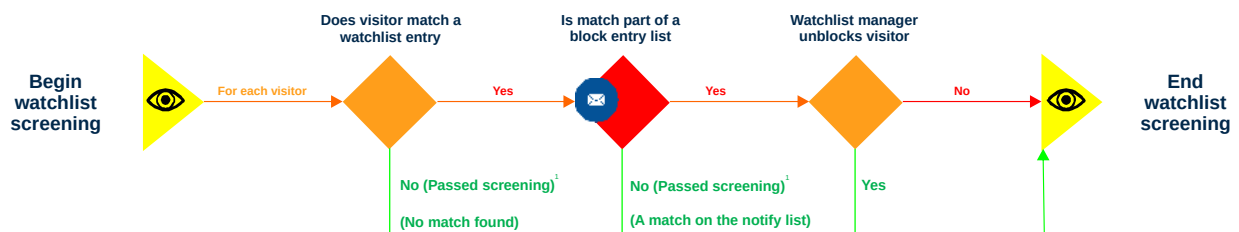
- About workflows in ClearID

9.2 | About visit request watchlist workflow in ClearID

A watchlist workflow is a series of activities performed by the system or authorized people during the life cycle of a visit request if watchlists are enabled. The activities can change the state and properties of watchlists, affect other entities in the system, or wait for conditions to be met.

The workflow helps automate screening visitors for persons or companies of interest during a self-service check-in or a self-registration, so that people involved in the review and approval process can focus on other tasks.

The following diagram illustrates the *watchlist workflow* that occurs (if the watchlist function is enabled for your account) in Genetec ClearID™ and Synergis™ in parallel with the visit request workflow.



¹ Visitor registration is only confirmed after screened visitors are not found in any block entry watchlists. Any visitors that are blocked do not receive a visit notification email.

Browse

- About workflows in ClearID

9.3 | Inviting visitors in ClearID

To invite one or more guests for a site visit or event, use the self-service portal. Using a self-service portal with area managers specified simplifies the approval process, and avoids interrupting a chain of people who might or might not be the correct approvers.

Before you begin

1. Familiarize yourself with workflows.
2. Enable visitor management for your site.
3. Ensure that you have the required permissions to invite visitors to the site.

What you should know

You can add visitors individually or import a large list of visitors using a CSV file.

- If you have fewer than five visitors to invite, add your visitors individually.
- If you have more than five visitors to invite, prepare a CSV file to import your visitor list.
- If your identity home site is configured, you are automatically granted access to invite visitors to that site only if the site visitor management options have been configured to allow people to invite visitors.
- The options displayed when creating a visitor invite can vary depending on the site settings and settings configured for visitor management.

NOTE: Mandatory fields are highlighted in the user interface with an asterisk (*).

Procedure

1. Log on to the self-service portal.
2. Do one of the following:
 - Click Dashboard > My requests > New request > Invite visitors.
 - Click Dashboard > Visits > New visit event.
3. In the New visit event wizard, follow the prompts to complete the wizard for one of the following situations:
 - Invite visitors manually
 - Invite visitors using a CSV import
4. Click Finish.

Results

Your visit request has been submitted and is waiting for the required approvals.

Example



After you finish

Confirm whether the request was approved or rejected:

- Check your email for a *Visit approved* email.
- Check My requests in Genetec ClearID™.

Browse

- [Enabling visitor management for sites in ClearID](#)

Browse

- Visitor Management Feature Note (2 pages)

9.3.1 | Inviting visitors manually in ClearID

If you have fewer than five visitors to invite to your event, you can add your visitors manually.

Before you begin

1. Familiarize yourself with workflows.
2. Enable visitor management for your site.
3. Ensure that you have the required permissions to invite visitors to the site.

What you should know

- If your identity home site is configured, you are automatically granted access to invite visitors to that site. Access is only automatically granted if the options for site visitor management have been configured to allow people to invite visitors.
- The options displayed when inviting visitors can vary depending on the site settings and settings configured for visitor management.

NOTE: Mandatory fields are highlighted in the user interface with an asterisk (*).

Procedure

1. Log on to the self-service portal.
2. Do one of the following:
 - Click Dashboard > My requests > New request > Invite visitors.
 - Click Dashboard > Visits > New visit event.
3. In the New visit event wizard, enter or select details about *where* the event will take place.

Channel Partner event at Genetec Alfred-Nobel

1 Where 2 When 3 Who 4 Details

What is the name of the event?

Name *

Channel Partner event

21 / 100

Where will this event take place?

Site *

Genetec Alfred-Nobel

Host meeting location

Main Entrance

Parking location

Alfred-Nobel

Visitors are automatically assigned default access ⓘ

Area *

IT Lab

Cancel Next

4. Enter or select details about *when* the event takes place and the purpose of the event.

Channel Partner event at Genetec Alfred-Nobel

✓ Where ⌄ When ⌄ Who ⌄ Details

When does the visitor require access?

Remember to include any time before and after the meeting when the visitor might also require access.

📘 The dates and times shown here are in the UTC time zone.

Start date *	01/01/2024	Start time *	10:00 AM
End date *	01/01/2024	End time *	04:00 PM

🕒 Duration: 6 hr

What is the purpose of this event?

Visit reason *

Meeting

Cancel Back Next

Tip: Remember to include time before and after the visitor event or meeting when the visitor might also require access.

5. Enter or select details about *who* to invite to the event.

Channel Partner event at Genetec Alfred-Nobel

✓ Where ✓ When ⌄ Who ⌄ Details

Who are the visitors?

2 visitors added.

Import visitors Add visitors

John Doe	✉ john.doe@test.com	🏢 Genetec ✎
Jane Doe	✉ jdoe@test.com	🏢 N/A ✎

Cancel Back Next

- a. Click Add visitor and complete the fields.
 - b. Click Save.
 - c. Repeat for each additional visitor.
6. Complete *details* about the event.

Channel Partner event at Genetec Alfred-Nobel

Where When Who **4 Details**

Who will escort the visitors?

Name	Email	SMS alerts
John Doe	john.doe@test.com	☒  +1 5141234567
Type to search...		

Notes for security

Cancel Back Finish

Name

The name of the visitor event host.

Email

The email address for the visitor event host.

SMS

Enter a mobile phone number to send SMS alert notifications to visitor hosts when the visitor checks in.

- o NOTE: Use the search field to add more visitor hosts. You can add up to 10 visitor hosts.

(Optional) Notes for security

Add notes about the visitor, the visit invite, or the visit event.

7. Click Finish.

Results

Your visit request has been submitted and is waiting for the required approvals.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Confirm whether the request was approved or rejected:

- Check your email for a *Visit approved* email.
- Check My requests in ClearID.

Parent topic: [Inviting visitors in ClearID](#)

Browse

- [SMS alerts in ClearID](#)
- [About email notifications in ClearID](#)

Browse

- [Visitor Management Feature Note \(2 pages\)](#)

9.3.2 | Inviting visitors using a CSV import in ClearID

If you have more than five visitors to invite to your event, you can use a CSV file import to populate your visitor list.

Before you begin

1. Familiarize yourself with workflows.
2. Enable visitor management for your site.
3. Ensure that you have the required permissions to invite visitors to the site.

What you should know

- If your identity home site is configured, you are automatically granted access to invite visitors to that site. Access is only automatically granted if the options for site visitor management have been configured to allow people to invite visitors.
- The options displayed when inviting visitors can vary depending on the site settings and settings configured for visitor management.

Tip: When you Import visitors, a sample CSV file provided by the system can be used. The columns in the sample CSV file match the settings in the site configuration. You can then complete the visitor details values in the CSV file and import all visitors in one click. For example, importing 500 people to a site visit or customer event.

NOTE: Mandatory fields are highlighted in the user interface with an asterisk (*).

Procedure

1. Log on to the self-service portal.
2. Do one of the following:
 - Click Dashboard > My requests > New request > Invite visitors.
 - Click Dashboard > Visits > New visit event.
3. In the New visit event wizard, enter or select details about *where* the event will take place.

Channel Partner event at Genetec Alfred-Nobel

1 Where 2 When 3 Who 4 Details

What is the name of the event?

Name *
Channel Partner event
21 / 100

Where will this event take place?

Site *
Genetec Alfred-Nobel

Host meeting location
Main Entrance

Parking location
Alfred-Nobel

Visitors are automatically assigned default access 1

Access *
IT Lab

Cancel Next

4. Enter or select details about *when* the event will take place and the purpose of the event.

Channel Partner event at Genetec Alfred-Nobel

1 Where 2 When 3 Who 4 Details

When does the visitor require access?
Remember to include any time before and after the meeting when the visitor might also require access.

1 The dates and times shown here are in the UTC time zone.

Start date * 01/01/2024

Start time * 10:00 AM

End date * 01/01/2024

End time * 04:00 PM

Duration 6 hr

What is the purpose of this event?

Visit reason *
Meeting

Cancel Back Next

Tip: Remember to include time before and after the visitor event or meeting when the visitor might also require access.

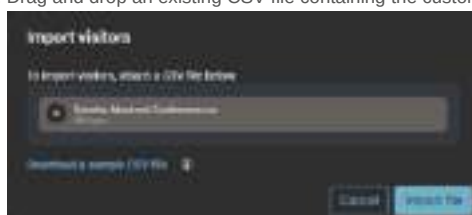
5. Prepare to import *who* you want to invite to the event.



- a. In the Who will attend this event? section, click Import visitors and then choose one of the following:
 - o Use an existing CSV file.
 - o Download a sample CSV file.

6. If you chose to use an existing CSV file, do the following:

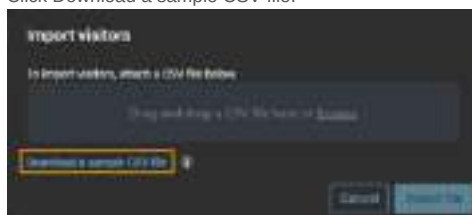
- a. Drag and drop an existing CSV file containing the customers you want to invite or click Browse to select the file you require.



- b. Click Import file to import the visitor list.
- c. Click Confirm to complete the import.
- d. (Optional) Click Edit (✎) to modify any visitor details and click Save to confirm the update.

7. If you chose Download a sample CSV file, do the following:

- a. Click Download a sample CSV file.



- b. Select and open the downloaded CSV file.
- c. For each visitor, complete a row of visitor information in the CSV template file.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	FirstName	LastName	email	companyName	isDisabledByAdmin	isScreeningRequired	screeningCompleted	screeningAgreement	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted
2	FirstName	LastName	email	companyName	isDisabledByAdmin	isScreeningRequired	screeningCompleted	screeningAgreement	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted
3	FirstName	LastName	email	companyName	isDisabledByAdmin	isScreeningRequired	screeningCompleted	screeningAgreement	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted
4	FirstName	LastName	email	companyName	isDisabledByAdmin	isScreeningRequired	screeningCompleted	screeningAgreement	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted	screeningCompleted
5																										
6																										
7																										
8																										
9																										
10																										
11																										
12																										
13																										
14																										
15																										
16																										
17																										
18																										
19																										
20																										

NOTE: The columns in the CSV template can vary depending on the settings in your site configuration.

- d. Save the visitor list as a CSV file.
- e. Return to the Import visitors dialog, to drag and drop or click Browse to select the file you created.
- f. Click Import file to import the visitor list.



g. Click Confirm to complete the import.

8. Complete *details* about the event.

Channel Partner event at Genetec Alfred-Nobel

Where When Who Details

Who will escort the visitors?

Name	Email	SMS alerts
John Doe	john.doe@test.com	☒ +1 5141234567
Type to search...		

Notes for security

Notes

Cancel Back Finish

Name

The name of the visitor event host.

Email

The email address for the visitor event host.

SMS

Enter a mobile phone number to send SMS alert notifications to visitor hosts when the visitor checks in.

- NOTE: Use the search field to add more visitor hosts. You can add up to 10 visitor hosts.

(Optional) Notes for security

Add notes about the visitor, the visit invite, or the visit event.

9. Click Finish.

Results

Your visit request has been submitted and is waiting for the required approvals.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Confirm whether the request was approved or rejected:

- Check your email for a *Visit approved* email.
- Check My requests in ClearID.

Parent topic: [Inviting visitors in ClearID](#)

Browse

- [SMS alerts in ClearID](#)
- [About email notifications in ClearID](#)

Browse

- [Visitor Management Feature Note \(2 pages\)](#)

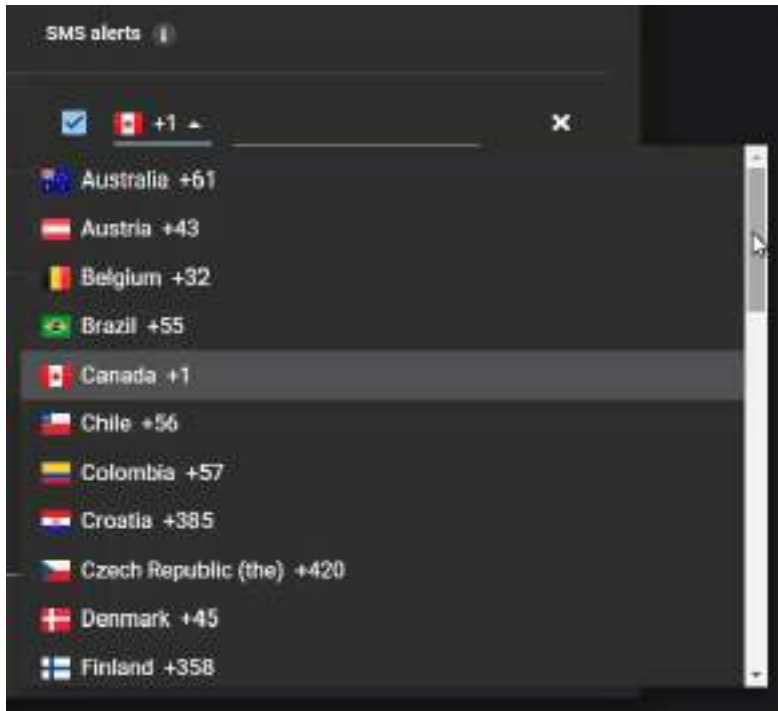
9.3.3 | SMS alerts in ClearID

In Genetec ClearID™, SMS alerts are used in the visit event wizard to automatically send notifications to visitor hosts to inform them when visitors check-in.

SMS alerts for visitor check-in are supported for the following countries:

Country	Country code
 Austria	+43
 Australia	+61
 Belgium	+32
 Brazil	+55
 Canada	+1
 Chile	+56
 Columbia	+57
 Croatia	+385
 Czech republic (the)	+420
 Denmark	+45
 Finland	+358
 France	+33
 Germany	+49

Country	Country code
 Greece	+30
 Iceland	+354
 India	+91
 Ireland	+353
 Italy	+39
 Japan	+81
 Luxembourg	+352
 Malaysia	+60
 Mexico	+52
 Monaco	+377
 Netherlands	+31
 Norway	+47
 Peru	+51
 Philippines (the)	+63
 Portugal	+351
 Romania	+40
 Singapore	+65
 Spain	+34
 Sweden	+46
 Switzerland	+41
 Taiwan (Province of China)	+886
 Thailand	+66
 United Kingdom of Great Britain and Northern Ireland (the)	+44
 United States of America (the)	+1
 Vietnam	+84



Parent topic: Inviting visitors in ClearID

Browse

- Inviting visitors manually in ClearID
- Inviting visitors using a CSV import in ClearID

9.4 | Reviewing visit events in ClearID

Area owners, security, and reception can review current or upcoming visits or events for their areas. Visits can be requested for hosting other site employees, maintenance contractors, appointments, meetings, interviews, customer visits, business partner conferences, and so on.

What you should know

Only *area owners*, security, or reception can review visits.

Procedure

1. Click Dashboard > Visits.
2. Select the options that you require.

Current and upcoming visits

Displays current and upcoming visits. By default, 10 visits are displayed and you can click Load more to display the next 10 visits.

Past visits

Displays past visits. By default, 10 past visits are displayed and you can click Load more to display the next 10 past visits. You can find past visits that occurred in the last year.

All visits

Displays all visits. By default, 10 visits are displayed and you can click Load more to display the next 10 visits.

3. (Optional) Use the column filters to refine the list of visits.

Name

In the Name field, enter your search criteria. Only search results for visits that contain the entered word in the visit name are displayed. For example, if you enter *training*, only visits with names that include the word *training* are displayed in the search results.

Status

Select a filter from the Status list to filter results for the visit request state:

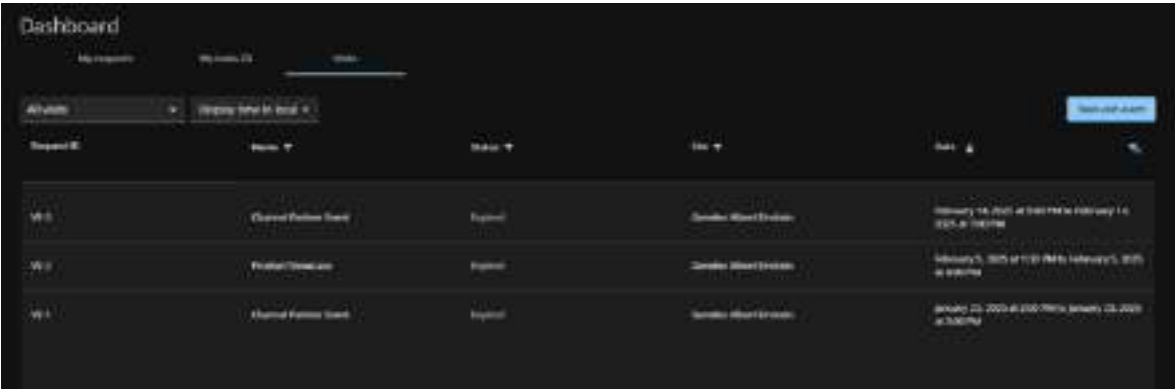
- Submitted
- Waiting for approvals
- Approved
- Canceled
- Denied
- Expired

Site
Select a site from the Site list.

Date
Sort the visits by date in ascending or descending order.

Results

The visits matching your selections are displayed.



The screenshot shows the Genetec ClearID Dashboard. At the top, there are tabs for 'My requests', 'My visits', and 'Visits'. Below the tabs, there are filters for 'All visits' and 'Display total in table'. A table of visit events is displayed with columns for 'Request ID', 'Event', 'Status', 'Site', and 'Date'. The table contains three rows of data.

Request ID	Event	Status	Site	Date
W-1	Checked-Passive (Event)	Expired	Genetec World Event	January 14, 2025 at 10:00 AM to February 14, 2025 at 10:00 PM
W-2	Proctor/Time-lapse	Expired	Genetec World Event	January 15, 2025 at 11:00 AM to January 15, 2025 at 10:00 PM
W-3	Checked-Passive (Event)	Expired	Genetec World Event	January 15, 2025 at 10:00 PM to January 15, 2025 at 10:00 PM

After you finish

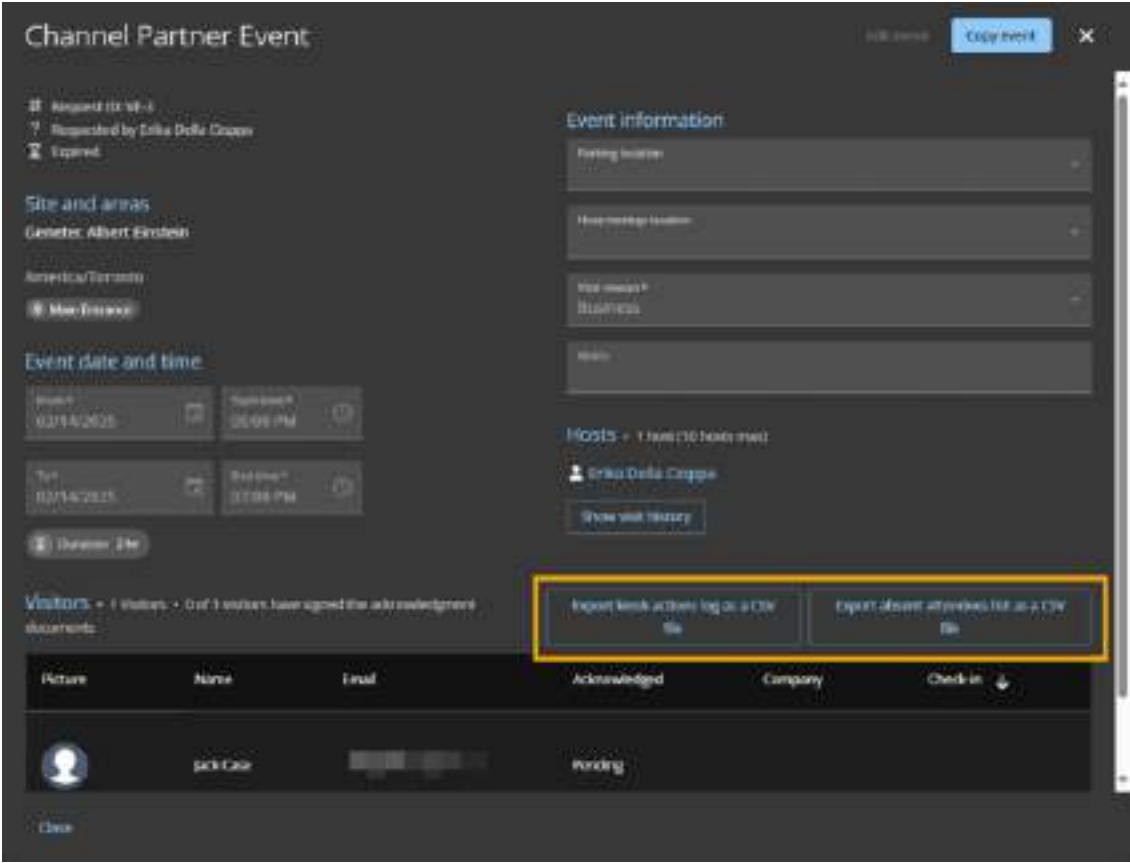
- Copy a visit event.
Browse
- About visit event logs in CearID

9.5 | About visit event logs in CearID

In Genetec ClearID™, *Account administrators*, *Site owners*, requesters, and hosts can use visit event logs to audit events and identify absentees. These logs show detailed records of operator and visitor actions on check-in devices, as well as invited guests who didn't check in.

ClearID organizes visit data into two logs:

- Kiosk actions log
- Absent attendees list



Kiosk actions log

The kiosk actions log contains information about actions performed at activated Self-Service Kiosk iPads and Mobile Operator Check-In iPhones during a visit event. Each time a device scans a visitor's QR code or a visitor checks into the visit event, an entry is entered in the log.

The exported .CSV file contains columns with identifying data for each kiosk action:

Timestamp

The time and date when the kiosk action was performed.

Action type

The type of kiosk action performed at a Self-Service Kiosk or with a Mobile Operator Check-In device. This column contains Scan when a device scans a QR code, and CheckIn when the visitor check-in process is complete.

Visit event ID

The identification number assigned to the visit event in the ClearID portal.

Visitor ID

The identification number assigned to the visitor associated with the visit event in the ClearID portal.

Visitor email

The email of the visitor associated with the visit event.

Registration code

The visitor QR code value associated with the visit event.

Device object ID

The identification number assigned to the device that performed the scan or check-in during the visit event.

Absent attendees list

The absent attendees list contains information about visitors who were invited to the event but didn't check in. The list can be used to identify absent attendees, allowing hosts to follow up as needed.

The exported .CSV file contains columns with identifying data for each absent attendee:

Visitor email

The email of the visitor flagged as an absent attendee.

Visit event name
The name assigned to the visit event.

Visitor ID
The identification number assigned to the visitor in the ClearID portal.

Visit event ID
The identification number assigned to the visit event in the ClearID portal.
Browse

- Viewing visit event logs in ClearID.
- Reviewing visit events in ClearID

9.6 | Viewing visit event logs in ClearID.

To audit operator and visitor actions on check-in devices during visit events, and review lists of absent attendees, you can export the logs of each event from the Genetec ClearID™ portal.

Before you begin

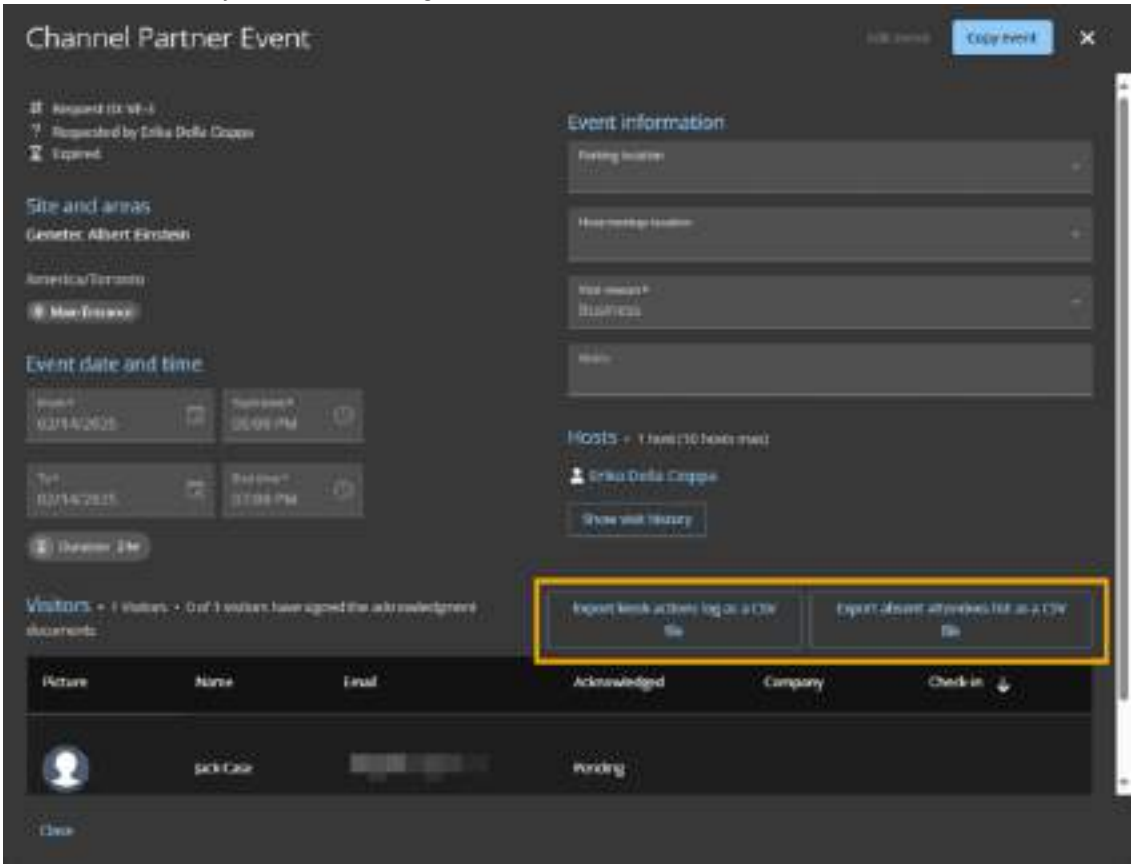
Invite visitors and review your visit events.

What you should know

You must be an *Account administrator*, *Area owner*, requester, or host to view visit event logs.

Procedure

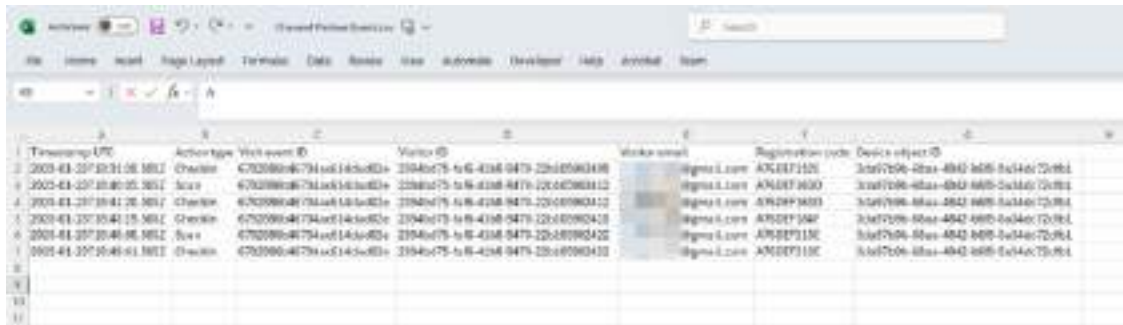
1. From the dashboard, go to Visits.
2. From the visit type filter, select All visits.
NOTE: By default, 10 visits are displayed. You can click Load more to display the next 10 visits.
3. Select the event for which you want to audit visit logs.



- a. Click Export kiosk actions log as CSV file to download a log of actions performed on visitor management devices during the event.
- b. Click Export absent attendees list as CSV file to download a list of visitors who didn't check in to the visit event.

Example

The visit event log is downloaded as a .CSV file. By default, the exported file is created using the visit event name. For example, Channel Partner Event.csv or Channel Partner Event-absentees.csv.



Timestamp UTC	Action type	Visit event ID	Visitor ID	Visitor email	Registration code	Device object ID
2023-01-20T10:00:00.000Z	Checkin	670208046734a6143a083e	2304a675-5d-42a8-9479-22a00903110	sigma.l.com	A90E7110	3a6700e-88aa-4942-8605-5a34ac7208d
2023-01-20T10:00:00.000Z	Scan	670208046734a6143a083e	2304a675-5d-42a8-9479-22a00903110	sigma.l.com	A90E7110	3a6700e-88aa-4942-8605-5a34ac7208d
2023-01-20T10:01:00.000Z	Checkin	670208046734a6143a083e	2304a675-5d-42a8-9479-22a00903110	sigma.l.com	A90E7110	3a6700e-88aa-4942-8605-5a34ac7208d
2023-01-20T10:01:00.000Z	Checkin	670208046734a6143a083e	2304a675-5d-42a8-9479-22a00903110	sigma.l.com	A90E7110	3a6700e-88aa-4942-8605-5a34ac7208d
2023-01-20T10:01:00.000Z	Scan	670208046734a6143a083e	2304a675-5d-42a8-9479-22a00903110	sigma.l.com	A90E7110	3a6700e-88aa-4942-8605-5a34ac7208d
2023-01-20T10:01:00.000Z	Checkin	670208046734a6143a083e	2304a675-5d-42a8-9479-22a00903110	sigma.l.com	A90E7110	3a6700e-88aa-4942-8605-5a34ac7208d

Browse

- [About visit event logs in ClearID](#)

9.7 | Copying a visit event in ClearID

You can copy a visit event to take advantage of reusable information in a recurring visit or visit events that include a large number of participants.

Before you begin

[Review visit events.](#)

What you should know

- Any user can copy their visits to create a similar visit.
- Use the Copy event function when you have recurring visits or a visit that includes a large number of participants. For example, one of the following situations:
 - Repeat visitors
 - A meeting that has the same or similar attendees as a previous meeting
 - Monthly customer visits
 - A yearly business partner conference

Procedure

1. Click Dashboard > Visits.
2. Click the visit event that you want to copy.
3. Click Copy event.
A copy of the visit event is created.
4. Modify the visit event as required and click Save.
For example: changing the event details, changing dates, adding or removing visitors, adding or removing hosts, or amending notifications.

Results

The new visit event is created and a *Visit created* email notification is sent to all visitors and hosts.

9.8 | Modifying visit events in ClearID

From time to time, you might want to modify a visit event to change the event details, or to add or remove visitors or hosts. Updating the visit event details ensures that your visitors are always kept up to date following any changes to an upcoming event.

Before you begin

Create your visit events in Genetec ClearID™ by doing one or more of the following:

- [Inviting visitors manually in ClearID](#)
- [Inviting visitors using a CSV import in ClearID](#)

What you should know

- Visit events can only be modified before the start of the visit event.
- Any modifications to a visit event are highlighted in the updated email notifications sent to relevant recipients.
- If visit event approval is enabled, any modifications to a visit event that are not Reason field modifications generate approval notifications for the relevant approvers to re-approve any changes or additions.
- Changing an existing visitor or host email to a different email triggers a cancellation notification for the original email and a visit event notification for the newly updated email.
- If visit event approval is enabled, changing a visitor name or host name details does not trigger email notifications for visitors, but does trigger the approval workflow again.

Procedure

1. Click Dashboard > Visits.
2. (Optional) If the list is long, use the drop-down menus and column filters to refine the results.

Name

Enter a search criteria to search for the visit event by name.

Status

Select one or more status filters to search for the visit event using the event status.

Site

Start typing to find a site or select a site from the Site list.

Date

In the Date column, use the ascending (▲) or descending (▼) controls to adjust the order of the results.

3. Click a visit event and review the event details to verify it is the event that you want to modify.
4. Click Edit event.

5. Modify one or more of the following as required:
 - a. In the Name field, modify the name.¹
 - b. In the Event date and time section, modify the start or end date and time.¹
 - c. In the Event information section, modify the parking location, host meetup location, or notes.¹

Visit event Visit reason modifications do not trigger any approval notifications because the reason has no impact on visitors attending the event.
 - d. In the Visitors section, add, modify, or remove visitors.

Any changes to visitors are assessed again to verify any watchlist screening criteria.
 - e. In the Hosts section, add, modify, or remove hosts.
- NOTE: ¹Modifying the Name, Event date and time, or Event information does not trigger re-approval (if approvals are applicable).
6. Click Save to confirm your changes.

After you finish

Review your visit event details to verify that the changes are correct.

9.9 | Approving visit event requests in ClearID

To modify or approve visit requests, *Visit event approvers* must review the pending approvals and then decide which requests to approve.

Before you begin

Enable visitor management for sites.

What you should know

When a visit request is submitted, the specified *Visit event approvers* receive an email notification.

Procedure

1. To view the details of a request for approval or denial, click Approve in the visit request email.
You're redirected to the Genetec ClearID™ portal where you're prompted to sign in.
2. Review the request details and make any required changes.
Tip: You can modify the request if the request has an error or something that needs to change. For example, you can amend the dates due to an office closure, or amend the parking location to a more appropriate location.

The screenshot displays the Genetec ClearID portal interface for a visit request titled "Global meeting with vendors". The request is in a "Waiting for approval" state, requested by "Sharon". The interface is divided into several sections: "Site and areas" (SJ Corp, New York), "Event date and time" (From: 10/13/2024, To: 10/17/2024), and "Event information" (Parking location, Host meeting location, Visit reason: Business). A "History" section on the right shows system actions like "Genetec ClearID™ system edited the request" and "Genetec ClearID™ system has verified all people against watchlists". At the bottom right, there are "Deny" and "Approve" buttons, with the "Approve" button highlighted by a yellow box.

- a. (Optional) Click Show more... to view the history of changes made to the visit request.
 - b. (Optional) Click Add comment to add notes to the history of the visit request. For example, you can add notes explaining why you changed the date and time of the visit.
3. Click Approve.
 - a. (Optional) In the Reason for approval field, enter a reason for the visit approval.
 - b. Click Confirm.

Tip: To view a list of all pending approvals, go to Dashboard > My tasks and select Pending from the list.

Results

A confirmation email is sent to both the visitor and the host outlining the details of the visit.

After you finish

Add the visit event to your calendar.

9.10 | Adding ClearID visit events to your calendar

Hosts and visitors can keep track of events and simplify the check-in process by adding visits to their calendars. To add a Genetec ClearID™ visit event to your calendar, open the visit confirmation email and download the attached ICS file.

Before you begin

Create a visit event.

What you should know

When a visit event is created, both the host and the visitors receive a confirmation email with the details of the event. The confirmation email also includes an ICS file that you can use to add the event to your digital calendar.

Procedure

1. Open the visit confirmation email.
2. Download the attached CSV file.

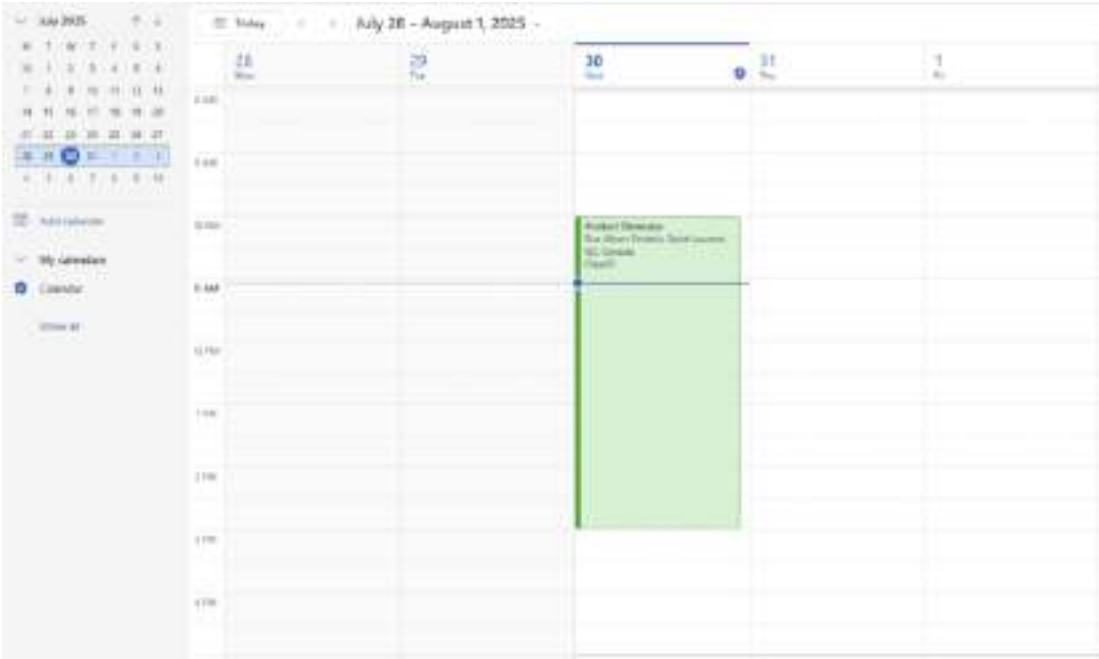


NOTE: Both ICS files contain the details of the visit. The visitor's copy also includes a QR code, allowing them to check in to the event directly from their calendar.

3. Follow the instructions in your chosen digital calendar to add the visit event.

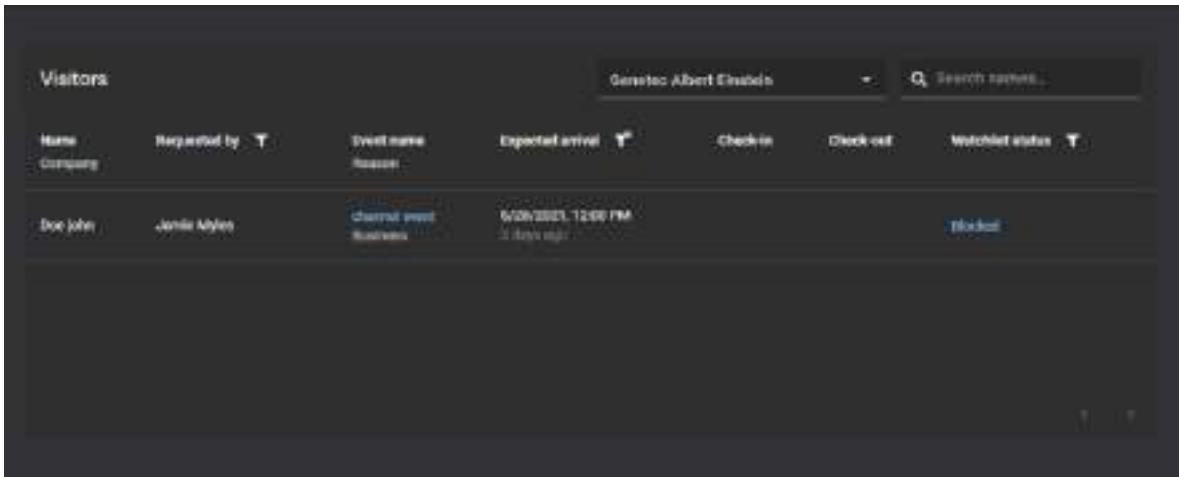
Results

You can now view the visit event and its details in your calendar.



9.11 | About visitors report in ClearID

In Genetec ClearID™, a visitors report is a list of current or upcoming visits, or visits that occurred in the past for a specific site. The report includes information about visitor name, event requester, event name, expected arrival, check-in, check-out, and watchlist status.



Visitors report

The visitors report is used by *site owners* and *watchlist managers* to check current or upcoming visits, or visits that occurred in the past and also to provide information to auditors.

Filters can be used to help refine the report search results by event requester, expected arrival, and watchlist status.

Browse

- [Viewing a visitors report in ClearID](#)

9.12 | Viewing a visitors report in ClearID

You can view a visitors report for any current or upcoming visits, or visits that occurred in the past. The report results are specific to a site, and can be filtered using event requester, expected arrival, and watchlist status.

Before you begin

[Invite your visitors.](#)

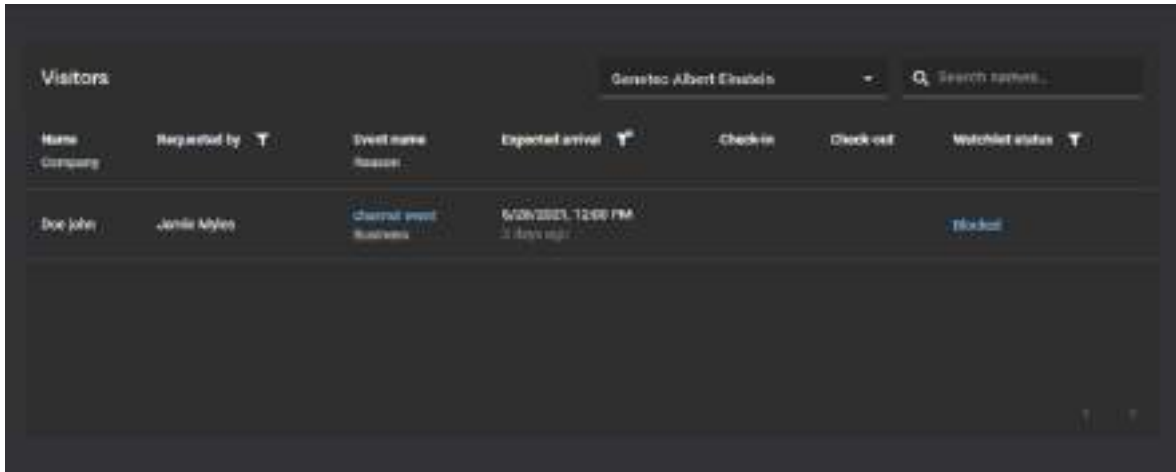
What you should know

- *Site owners* and *watchlist managers* can view the visitors report.
- Only watchlist managers can unblock or allow blocked visitors.

NOTE: For customers who have not purchased a watchlist license, the Watchlist status column is present in the report but displays N/A because no watchlist data is available.

Procedure

1. From the homepage, click Reports > Visitors.
2. Select a site from the Site list.



3. (Optional) Enter a name in the search box.
4. (Optional) Click the Requested by filter icon  and enter a visit requesters name.
5. (Optional) Click the Expected arrival filter icon  and select an expected arrival option:
 - [Current and upcoming visits](#)
 - A day ago
 - 7 days ago
 - 30 days ago
 - 90 days ago
 - All past events

Tip: If no visitors are displayed, select a longer Expected arrival filter to increase the filtered results that are displayed.

6. (Optional) Click the Watchlist status filter icon  and select one or more checkbox options:

Allowed

The visitor did not match any block list entries during the watchlist screening process and was allowed access to visit the site.

Blocked

The visitor matched one or more block list entries during the watchlist screening process and was blocked from visiting the site.

Unblocked

The visitor matched one or more block list entries during the watchlist screening process but was allowed access to visit the site by the watchlist manager.

In progress

Visitor watchlist screening is in progress.

Notified

The visitor matched one or more notify list entries during the watchlist screening process. The watchlist manager was notified and the visitor was allowed access to the site.

- a. (Optional) Click the Blocked hyperlink to open the Visitor watchlist alert dialog. From this dialog, a watchlist manager can allow entry if required.
- b. (Optional) Click the information icon next to an unblocked watchlist status for more information about who unblocked the visitor.

7. (Optional) Click  to reset filter selections and return to the visitors list.

Browse

- [Unblocking visitors blocked by a watchlist in ClearID](#)
- [About visitors report in ClearID](#)

9.13 | QR codes as a credential for visitors in ClearID

Genetec ClearID™ can use QR codes as a credential for visitors to simplify access to parking entrance barriers, turnstiles, or gated facilities.



The following third-party vendor QR code solutions are currently supported:

- Qscan barcode readers
- STid QR code readers

Visitors can use a QR code as a credential to open parking entrance barriers, turnstiles, or gated facilities:

- The QR code contained in a visitor confirmation email can be presented using a smartphone.
- The visitor confirmation email can also be printed and used for check-in.
- SMS messages notify hosts when their visitors arrive (if the check-in notification function is enabled).

Browse

- [Supported devices for ClearID](#)

9.13.1 | Importing a custom card format (QR code credential) in Synergis

Before you can use QR codes as a credential in Genetec ClearID™, you must configure Synergis™ to support the ClearID QR code custom card format. A QR code can then be used as a credential to access parking entrances, turnstiles, or gated facilities.

Before you begin

- [Install the ClearID plugin](#)
- Make sure that the Visitor Management module is activated in your Security Center Synergis License.

What you should know

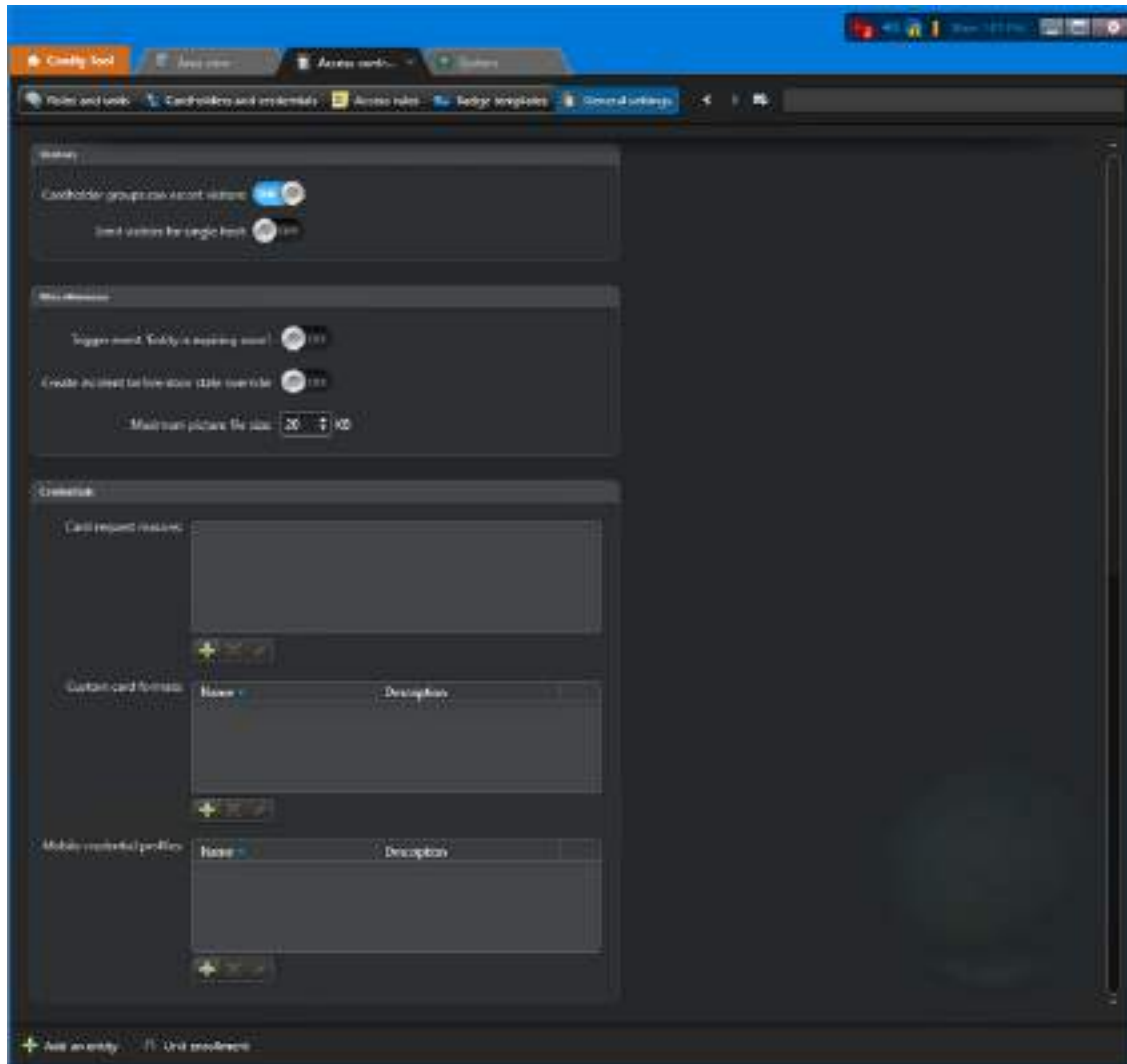
Only Security Center administrators or users with the *modify credential properties* privilege can import the custom card format.

The SDK and ClearID Plugin do not automatically create the custom card format for QR codes.

IMPORTANT: The custom card format is found on the Security Center machine where the ClearID plugin is installed.

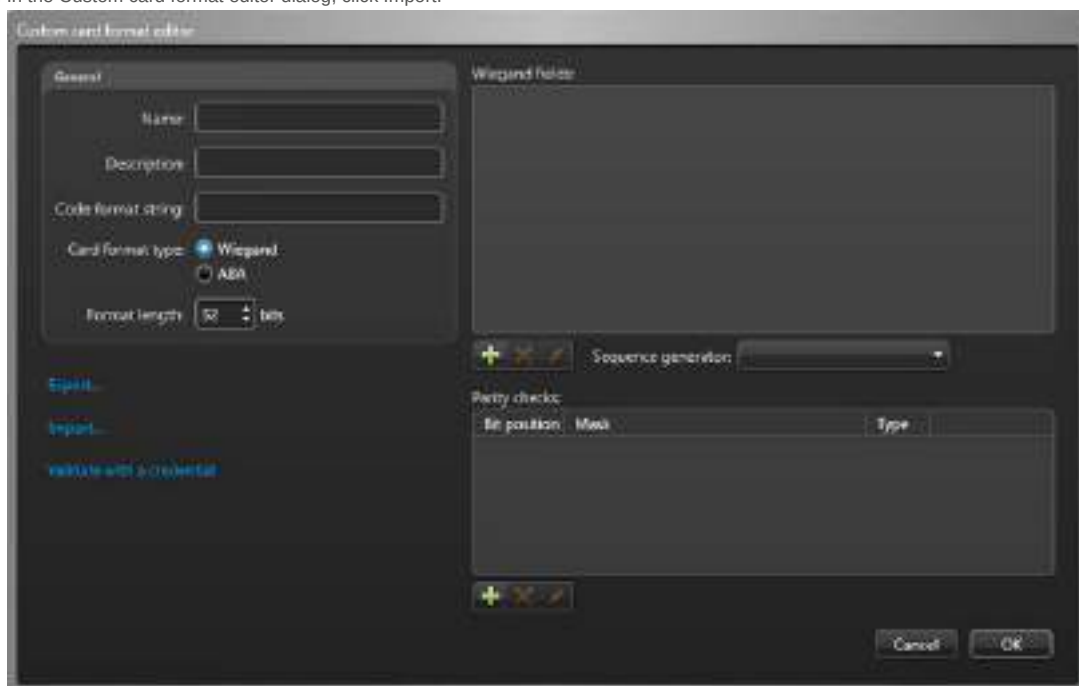
Procedure

1. In Config Tool, open the Access control task and select the General settings view.



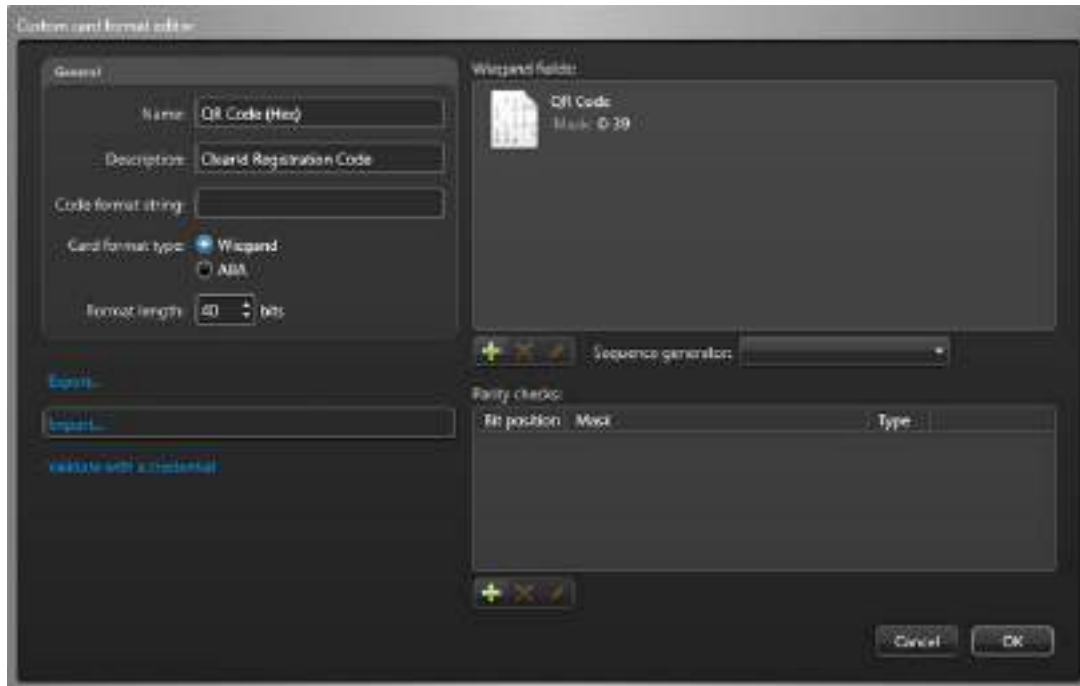
2. In the Custom card formats section of Credentials, click Add an item (+).

 - a. Download this [QRcode.xml](#) file.
 - b. In the Custom card format editor dialog, click Import.

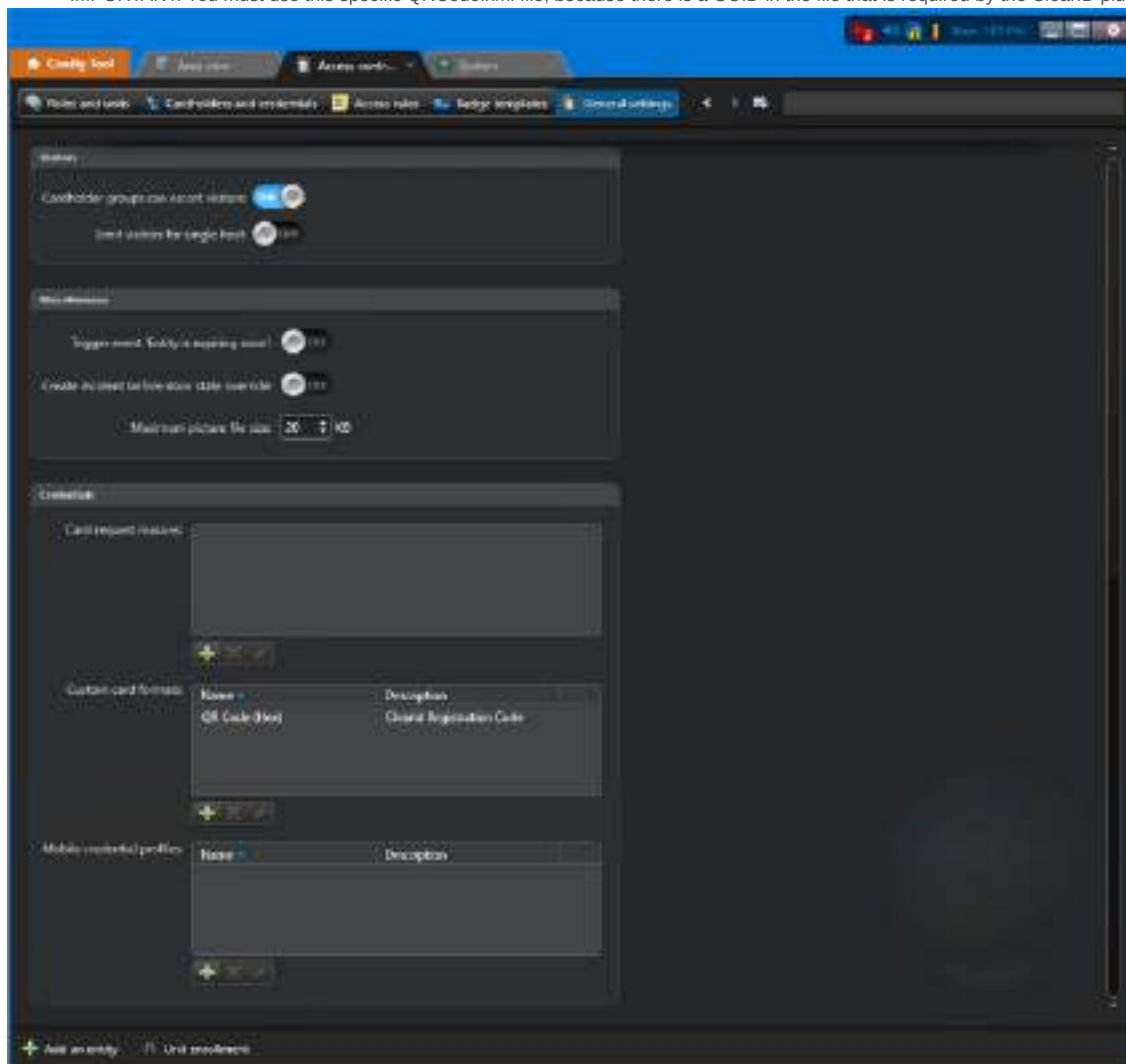


IMPORTANT: You must import the custom card format on the machine where the ClearID plugin is installed. The card format type that is used during import is Wiegand format.

- c. Navigate to and select the QRcode.xml file you downloaded.
- d. Click Open and click OK.



IMPORTANT: You must use this specific QRCode.xml file, because there is a GUID in the file that is required by the ClearID plugin.



Results

In the Access control task General settings view, the QR code (Hex) custom card format is now selected and available.

After you finish

Enable QR code credentials for visitors.

Parent topic: QR codes as a credential for visitors in ClearID

Browse

- License options for ClearID system integration

9.13.2 | Enabling QR code credentials for visitors in ClearID

To automatically create a QR code credential for visitors when a visit request is created, you must enable QR code credentials for visitors.

Before you begin

- Enable visitor management for sites in Genetec ClearID™
- Import a custom card format (QR code credential) in Synergis™

IMPORTANT: Make sure that the custom card format (QR code) is imported and available in the Security Center that your site is connected to.

What you should know

Only site owners or account administrators can enable the QR code credentials for visitors.

- When a QR code is automatically created for a visitor, the visitor is created in an inactive state, and the visitor credential contains an automatically generated QR code. The QR code in the credential matches exactly the QR code in the visitor confirmation email.
- The visitor credential is active at this point, but the QR code is not usable, because the visitor is not checked in yet. When the visitor check-in occurs, the QR code is valid until the visitor checks-out, or the end of the day for the scheduled visit.

For example, QR code credentials for visitors could be used to automatically grant access to a turnstile after check-in.

Procedure

1. Click Organization > Sites.
2. Search for and select a site.
3. Click Visitor management to configure the visitor management options for a site.
4. In the Advanced section, select Automatically create QR code credentials for visitors.



5. Click Save.

Results

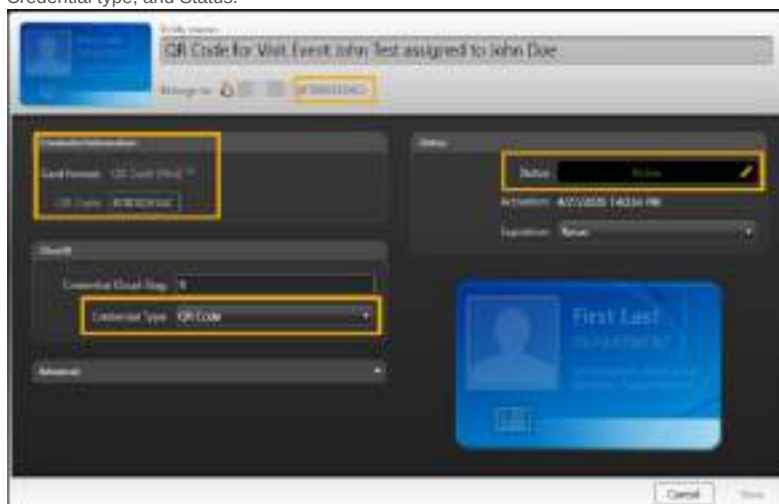
The next time a visitor is invited to the site, ClearID automatically creates a QR code credential for the visitor. The QR code is included in the visitor confirmation email.



After you finish

Perform a visitor invite and check-in test, to validate that QR code credentials are automatically created for visitors.

Tip: You can perform a visitor search in the Visitor management task in Security Desk, then edit the credential to check the visitors' Credential information, Credential type, and Status.



Parent topic: QR codes as a credential for visitors in ClearID
Browse

- Enabling visitor management for sites in ClearID

9.13.3 | Configuring Qscan devices for ClearID

Before you can use QR codes as a credential in Genetec ClearID™, you must configure your Qscan devices to support the custom card format (QR code credential) used in ClearID. A QR code can then be used as a credential to access parking entrances, turnstiles, or gated facilities.

Before you begin

Familiarize yourself with the Qscan documentation:

- [Qscan User Guide \(PDF\)](#)
- [Qscan \(for parking lots\) brochure \(PDF\)](#)
- [QscanT \(for turnstiles\) brochure \(PDF\)](#)
- [QscanI \(indoor version\) brochure \(PDF\)](#)

WARNING: Qscan barcode readers contain a Class 2 laser. Do not look directly into the laser.

What you should know

This procedure is for system integrators or account administrators who install and configure barcode scanners.

The following Qscan devices can be used with ClearID to scan QR codes as a credential for visitors:

- Qscan (for parking lots)
- QscanT (for turnstiles)
- QscanI (indoor version)

Procedure

1. Connect a Qscan barcode reader to a Mercury Controller.
2. Configure Qscan barcode reader to support 40-bit hexadecimal QR codes.

Parent topic: [QR codes as a credential for visitors in ClearID](#)

Browse

- [Supported devices for ClearID](#)

9.13.3.1 | [Connecting a Qscan barcode reader to a Mercury Controller for ClearID](#)

[QR codes as a credential for visitors in ClearID](#) >

In situations where you need to use a Qscan barcode reader to access parking entrances, turnstiles, or gated facilities, you must connect a Qscan barcode reader to a Mercury controller. This ensures that the barcode reader can communicate with Security Center Synergis™ to manage access.

Before you begin

WARNING: Qscan barcode readers contain a Class 2 laser. Do not look directly into the laser.

What you should know

This procedure is for system integrators or account administrators who install and configure barcode scanners.

In this scenario, we describe how to connect a Qscan barcode reader to a Mercury EP 1502 controller.

Procedure

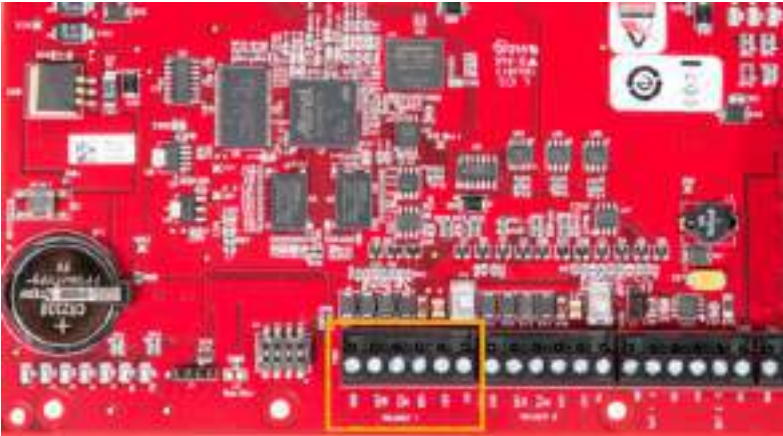
Connect your Qscan barcode reader device to the Reader 1 connection block in the Mercury EP 1502 controller.



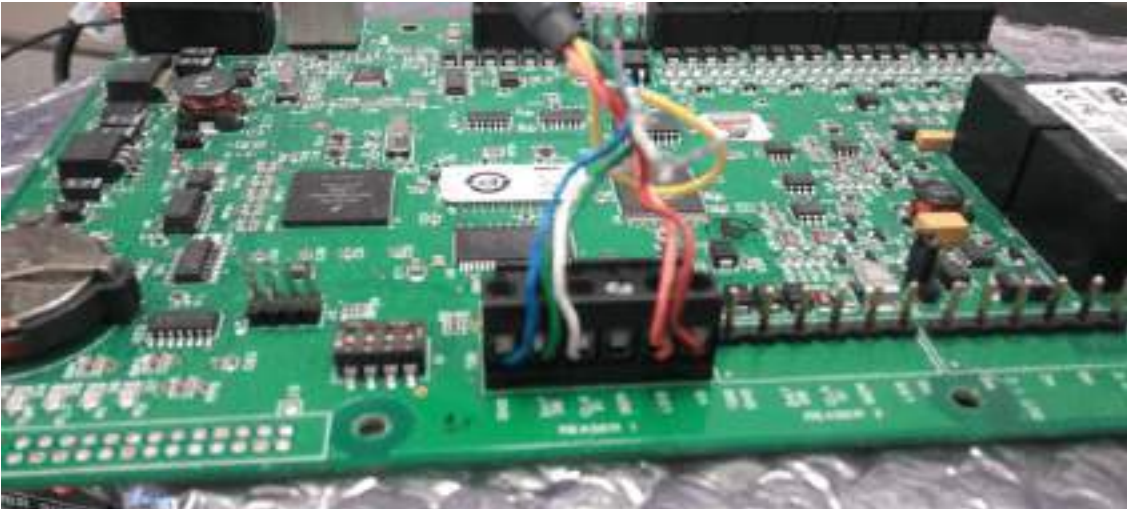
Figure 1: Qscan barcode reader



Figure 2: Mercury EP1502 controller boards



NOTE: The Mercury controller boards can vary in color depending on when they were manufactured and purchased.
Figure 3: Mercury EP1502 controller board wiring loom connections



Use the following table to understand how to connect the Qscan barcode reader wires to the terminals on the Mercury controller *Reader 1* connector block.

Mercury controller and Qscan reader wiring connections	
Mercury EP1502: Reader 1 connections	Qscan barcode reader: wire colors
GND (Ground)	BLUE
DAT D0 (Data/Data 0/TR-)	GREEN
CLK D1 (Clock/Data 1/TR+)	WHITE
BZR (Reader Buzzer)	Not applicable
LED (Reader LED)	ORANGE
V0 (Reader Power)	RED

After you finish

Configure Qscan barcode reader to support 40-bit hexadecimal QR codes
Parent topic: [Configuring Qscan devices for ClearID](#)

9.13.3.2 | Configuring Qscan barcode reader to support 40-bit hexadecimal QR codes for ClearID

QR codes as a credential for visitors in ClearID >

Before the QR codes automatically generated by Genetec ClearID™ for visitor confirmation email notifications can be understood and processed by Synergis™ Cloud Link during check-in, you must configure your Qscan barcode reader to support 40-bit hexadecimal QR codes.

Before you begin

Connect Qscan barcode reader to Mercury controller

WARNING: Qscan barcode readers contain a Class 2 laser. Do not look directly into the laser.

What you should know

This procedure is for system integrators or account administrators who install and configure barcode scanners.

In this scenario, we describe how to program Qscan devices to support 40-bit hexadecimal QR codes used in ClearID and output to Synergis Cloud Link.

For example, a QR code when scanned by Qscan is typically read as alphanumeric ABC1234567.

Synergis Cloud Link requires the QR code in HEX format 0xAB 0xC1 0x23 0x45 0x67 to manage access requests.

CAUTION:

The steps described in the following process remove alphanumeric QR code support from the Qscan barcode reader. The Qscan barcode reader cannot be used in alphanumeric mode while the 40-bit hexadecimal mode is active.

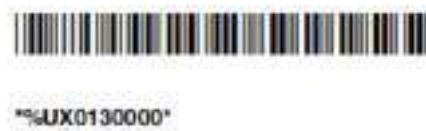
Procedure

1. To reset to factory default settings, scan the qscan resetbarcode1.pdf barcode.



NOTE: The Qscan reader beeps twice if the factory reset is successful.

2. To ignore alphanumeric characters, scan the qscan no alpha delete.pdf barcode.



3. To turn HEX conversion on, scan the qscan hex conversion.pdf barcode.



4. To output 40-bits, scan the qscan 40-bit.pdf barcodes.

NOTE: This file has three barcodes so scan one at a time.



Parent topic: Configuring Qscan devices for ClearID

9.13.4 | Configuring STid devices for ClearID

Before you can use QR codes as a credential in Genetec ClearID™, you must configure your STid devices to support the QR code custom card format used in ClearID. A QR code can then be used as a credential to access parking entrances, turnstiles, or gated facilities.

Before you begin

Familiarize yourself with the STid documentation:

- Architect® Blue QR code readers.
 - ARCS-AQ/BT - 13.56 MHz + Bluetooth® + QR Code multi-technology reader
- SECard - High security programming kits
- SECard User Manual

What you should know

This procedure is for system integrators or account administrators who install and configure QR code readers.

In this scenario, we describe how to program STid devices to support 40-bit hexadecimal QR codes used in ClearID and output to Synergis™ Cloud Link.

Procedure

1. Learn about STid QR code readers.
2. Import custom card format.
3. Set up and connect your QR code reader to your access control panel.

NOTE: The steps you must perform will vary depending on your access control panel.

 - To connect your OSDP reader to Synergis Cloud Link, see OSDP readers connected to the Synergis Cloud Link RS-485 ports.
 - To connect your OSDP reader to Mercury, see Adding OSDP (Secure Channel) readers to a Mercury controller.
4. Creating an STid QR code reader configuration for ClearID.
5. Transferring your reader configuration to your STid QR code reader for ClearID.

After you finish

Add doors to areas.

Parent topic: [QR codes as a credential for visitors in ClearID](#)

9.13.4.1 | [About STid QR code readers in ClearID](#)

[QR codes as a credential for visitors in ClearID](#) >

In Genetec ClearID™, STid QR code readers can be used to read QR code credentials.



NOTE: The image shown here illustrates STid readers that you might have in your organization. For a list of the Open Supervised Device Protocol (OSDP) readers that ClearID supports, see [Supported devices](#).

Why choose the OSDP protocol over Wiegand protocol?

WIEGAND Protocol

In Wiegand the reader always sends a fixed-length wiegand format, regardless of the credential length. The *custom card format* called by Security Desk is always the same. The manufacturer has confirmed this Wiegand readers (SY-ARCS-R31-AQBT1-XX1) limitation.

Consequence: The credential does not match the length required by the protocol and an Unknown credential message is displayed in Security Desk even if this QR code credential is already enrolled in the Security Center Synergis™ database.

Workaround: To make sure that all types of credentials work simultaneously with Wiegand protocol readers and Synergis, all other credentials (RFID or QR code from another source such as Axis) should match the ClearID QR code credential length (40 bits). This approach ensures that Synergis always receives the same *custom card format* (the card format from ClearID) and correctly interprets all types of payloads that the reader sends.

OSDP Protocol

In Open Supervised Device Protocol (OSDP) the reader dynamically adapts the format length regarding the credential length.

Best Practice: Use OSDP with STid QR code readers to ensure that the QR code credential is accepted and understood.

The following table shows example reads from the same reader.

Credential code	Card format	
4AE6CD6464E	QR code (HEX)	ClearID QR code
E01EC72022429729	64 bits	DESFire 64 bits private ID credentials

The examples show that the *custom card format* called by Security Desk is different for each read.

Consequence: The OSDP reader is more flexible and correctly interprets the credential.

Planning your QR code reader deployment

Depending on your needs, you can use the latest STid Architect® Blue QR code readers. Alternatively, you can add interchangeable QR code modules if you want to reuse existing STid readers.



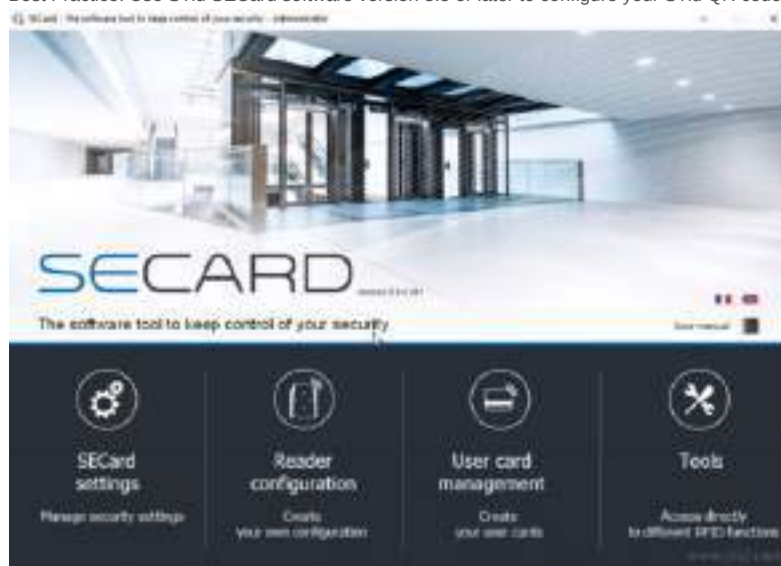
Consider the following when planning your STid QR code reader implementation:

- Best Practice: If you are planning a new STid QR code reader implementation, consider using the latest QR code readers with the latest firmware. For example, model: ARCS-AQ/BT. Only use STid readers that support the OSDP protocol and have upgraded to firmware version 10.
- If you already have numerous STid readers deployed in your organization, consider adding the interchangeable QR code reader module and updating your firmware.
Tip: Using the interchangeable module upgrades can result in significant savings on a large project.
- If you are re-using existing readers, refer to *STid documentation* about how to upgrade your reader to firmware version 10 or later.

Programming your STid QR code readers

The STid QR code readers can be programmed using the *STid SECard - High security programming kit*.

Best Practice: Use STid SECard software version 3.5 or later to configure your STid QR code readers.



The KIT-SECARD-BT-V3.X includes the following:

- STid Architect® ARC-G desktop reader, enroller, encoder



- USB key containing the STid SECard software



IMPORTANT: Genetec Inc. does not provide support for the STid SECard solution. Customers must use the stand-alone STid SECard software to configure the OSDP readers to work with the ClearID ACS panel solution.

Parent topic: [Configuring STid devices for ClearID](#)

[Browse](#)

- [Supported devices for ClearID](#)

9.13.4.2 | Creating an STid QR code reader configuration for ClearID

[QR codes as a credential for visitors in ClearID >](#)

Before you can use QR codes as a credential in Genetec ClearID™, you must create your STid QR code reader configuration. A QR code can only be used as a credential for an STid QR code reader after the QR code reader configuration has been uploaded to an STid OCB smart card and then transferred to the STid QR code reader.

Before you begin

Familiarize yourself with the STid documentation:

- [SECard - High security programming kits](#)
- [SECard User Manual](#)
- [Install the STid SECard - High security programming kit software.](#)

What you should know

This procedure is for system integrators or account administrators who install and configure QR code readers.

NOTE: The STid SECard software requires a license, the number is typically found on the USB reader that is used to encode a smart card.

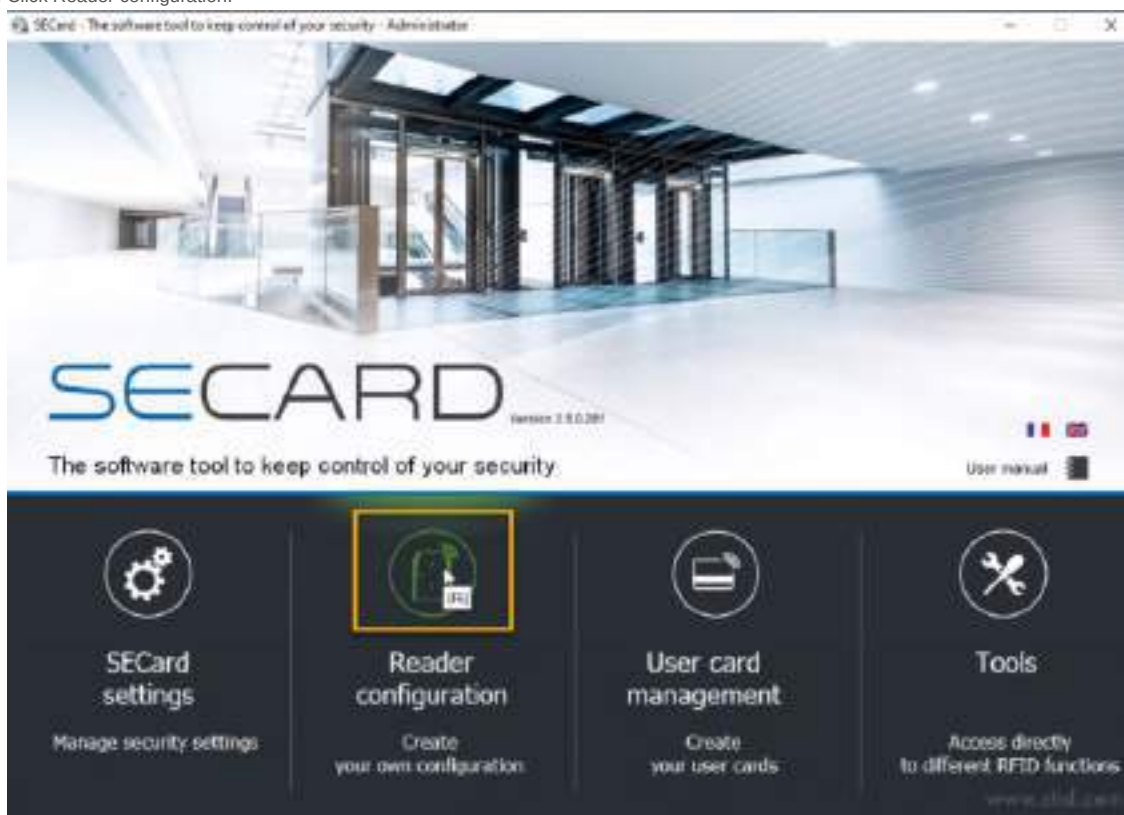


Procedure

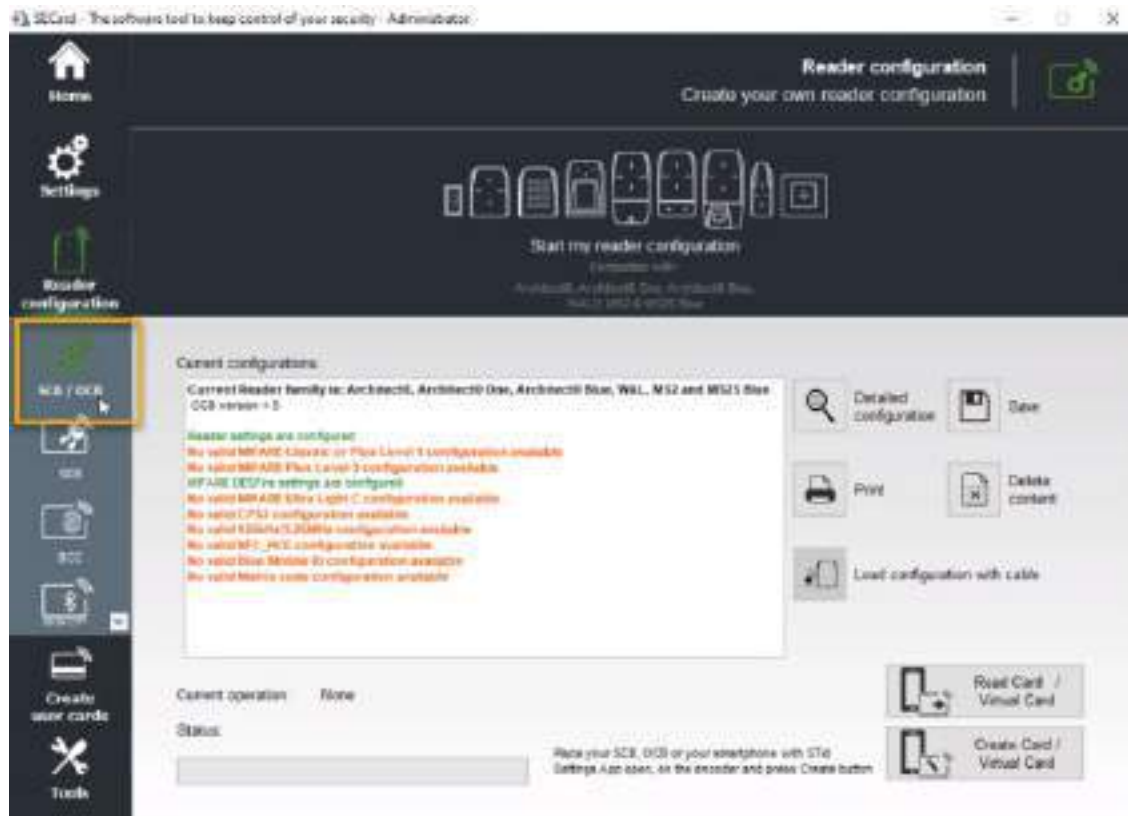
1. Launch the STid SECard - High security programming kit software to configure your STid QR code reader.



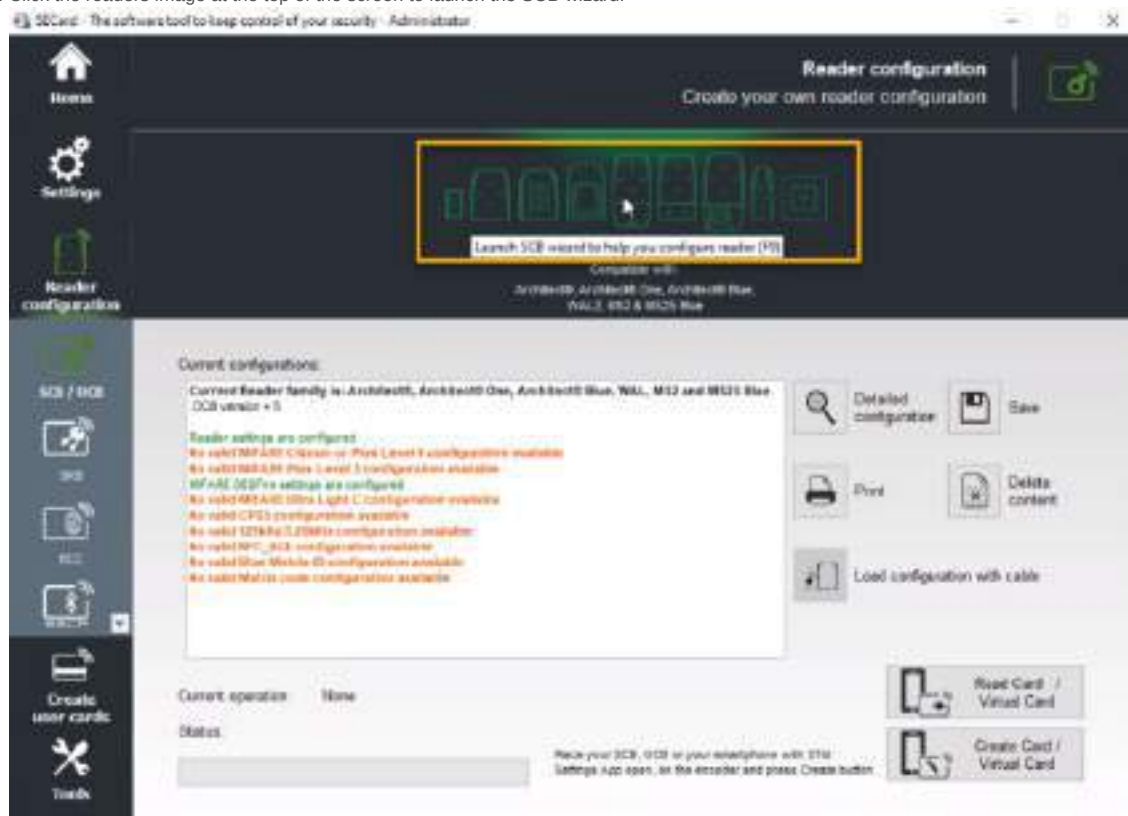
2. Click Reader configuration.



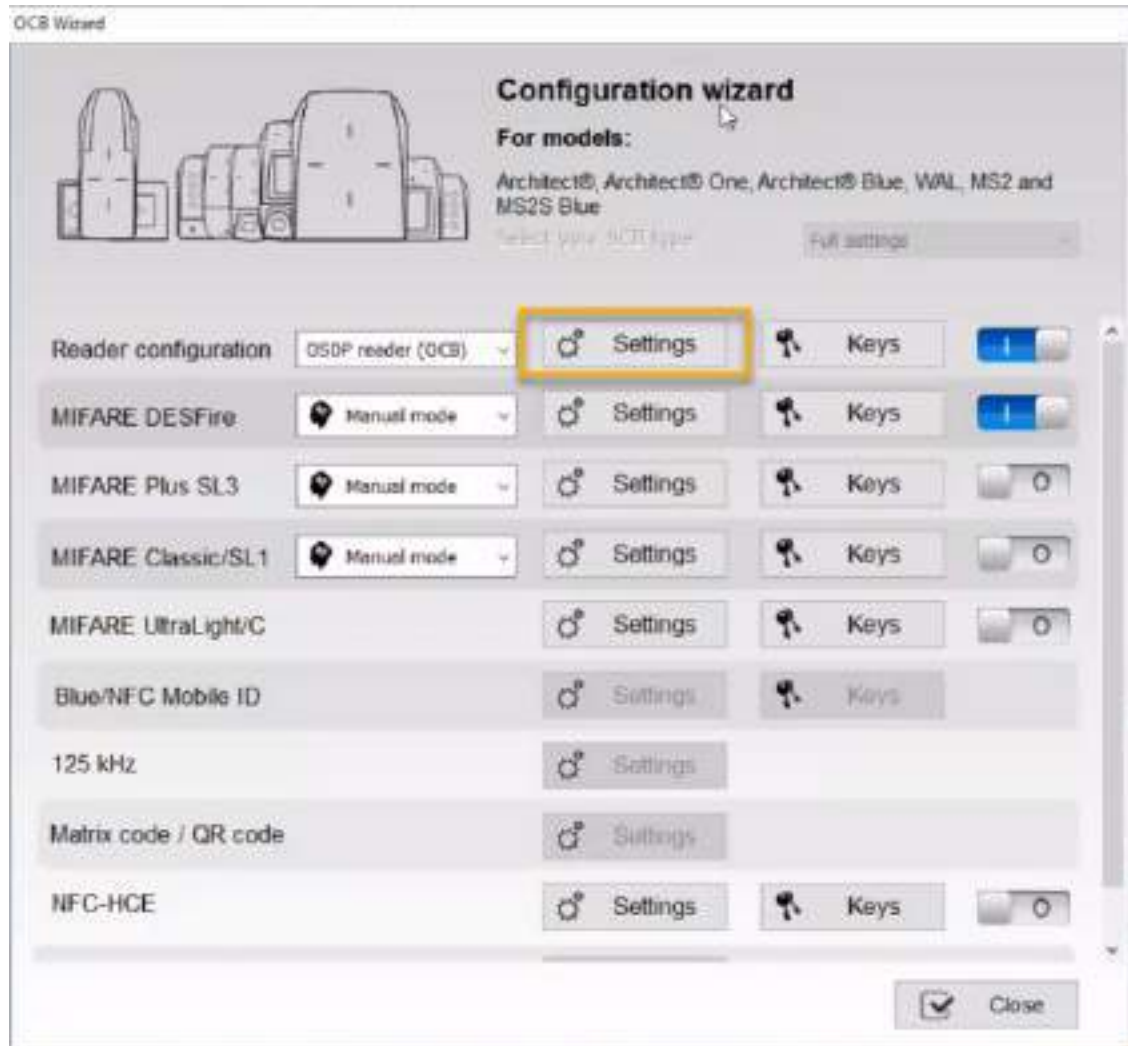
a. In the navigation sidebar, click SCB / OCB.



b. Click the readers image at the top of the screen to launch the SCB wizard.



c. In the Reader configuration row, next to OSDP reader (OCB), click Settings to open the Configuration wizard.



3. In the Configuration wizard dialog, select SECard V3.5 x OCBv5 and click Next.



a. In the Reader reference selection dialog, select the Matrix / QR Code check box and click Next.

OCB Wizard

Reader reference selection

Choose reader type and options to configure

1 2 3 4 5 6 7 8

Features activation


☐ Keypad


☐ Touchscreen


☐ Blue/NFC
Mobile ID


☐ Biometric


☐ Prox 125 kHz


☒ Matrix code /
QR code

Reader protection options

☒ Save user keys in non volatile memory

☒ Tamper switch signal

☒ Erase keys on tamper switch activation

Accelerometer sensitivity

☐ On tamper activation keeps LED red as default

Low

◀ Back Next ▶ ✕ Cancel

b. In the Reader parameters dialog Protocols section select the Type RAW and click Next.

OCB Wizard

Reader parameters
Protocol and options

1 2 3 4 5 6 7 8

Private ID security

☐ Data authenticated encryption

Protocols

Type: ☒ RAW ☐ Wiegand

☐ Use protocol size: 4 Byte(s)

☒ Backward compatibility

☒ Justify data to left ☐ Justify data to right

Protocol options

☐ Forced site code on UID

☐ 2 bytes Value: AB

☐ Enable Plain mode after secure channel authentication

☒ Use ACK instead of Busy command

Offset: 0 bit(s)

☐ Change RS485 address: 0

Baudrate: No change

☒ No wrap text

ISO14443-3B PUPi / iClass

☐ Enable

Card ID range filter (LSB)

UID/ID range: 00000000 to 80000000

Back Next Cancel

NOTE: The Byte(s) setting is not used when the Use protocol size check box is not selected. This ensures that the reader will adapt the length according to the length of the credential.

4. The following steps (4.a - 4.d) are not essential for QR code use, but might still be relevant to your installation.
- a. Click Next to skip the LED and Buzzer dialog.

OCB Wizard

LED and Buzzer
Options and parameters

1 2 3 4 5 6 7 8

LED default state

Mode: ☒ Off ☐ Fixed ☐ Blinking

Color: [LED icon]

Blink duration ON: 4 at 80ms

Blink duration OFF: 4 at 80ms

Buzzer sound level

[Speaker icon] Low

Card detection action

LED cycle number: 3

LED duration ON: 4 at 80ms

LED duration OFF: 4 at 80ms

Buzzer cycle number: 3

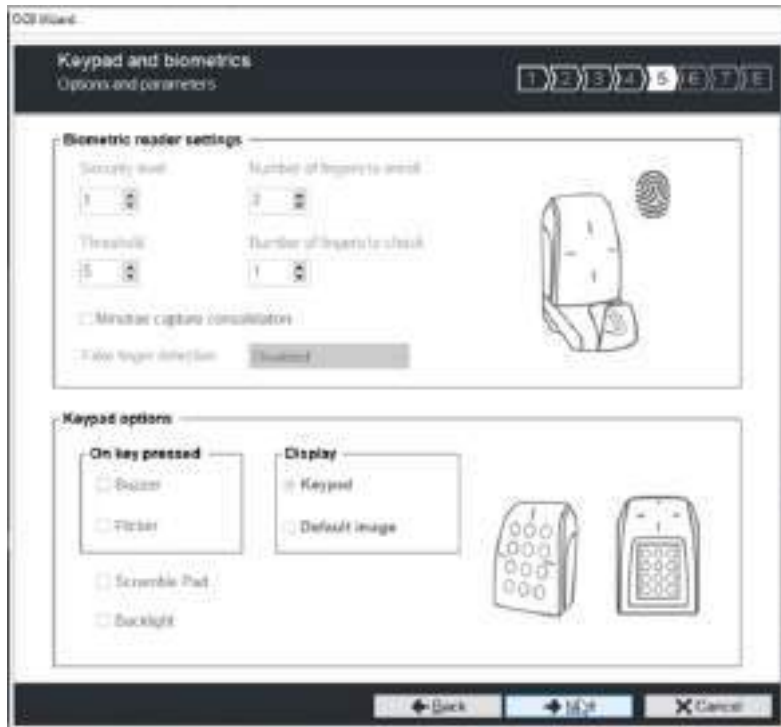
Buzzer duration ON: 4 at 80ms

Buzzer duration OFF: 4 at 80ms

☐ Lights at Bluetooth (BT) connector

Back Next Cancel

- b. Click Next to skip the Keypad and biometrics dialog.



c. Click Next to skip the Touchscreen options dialog.

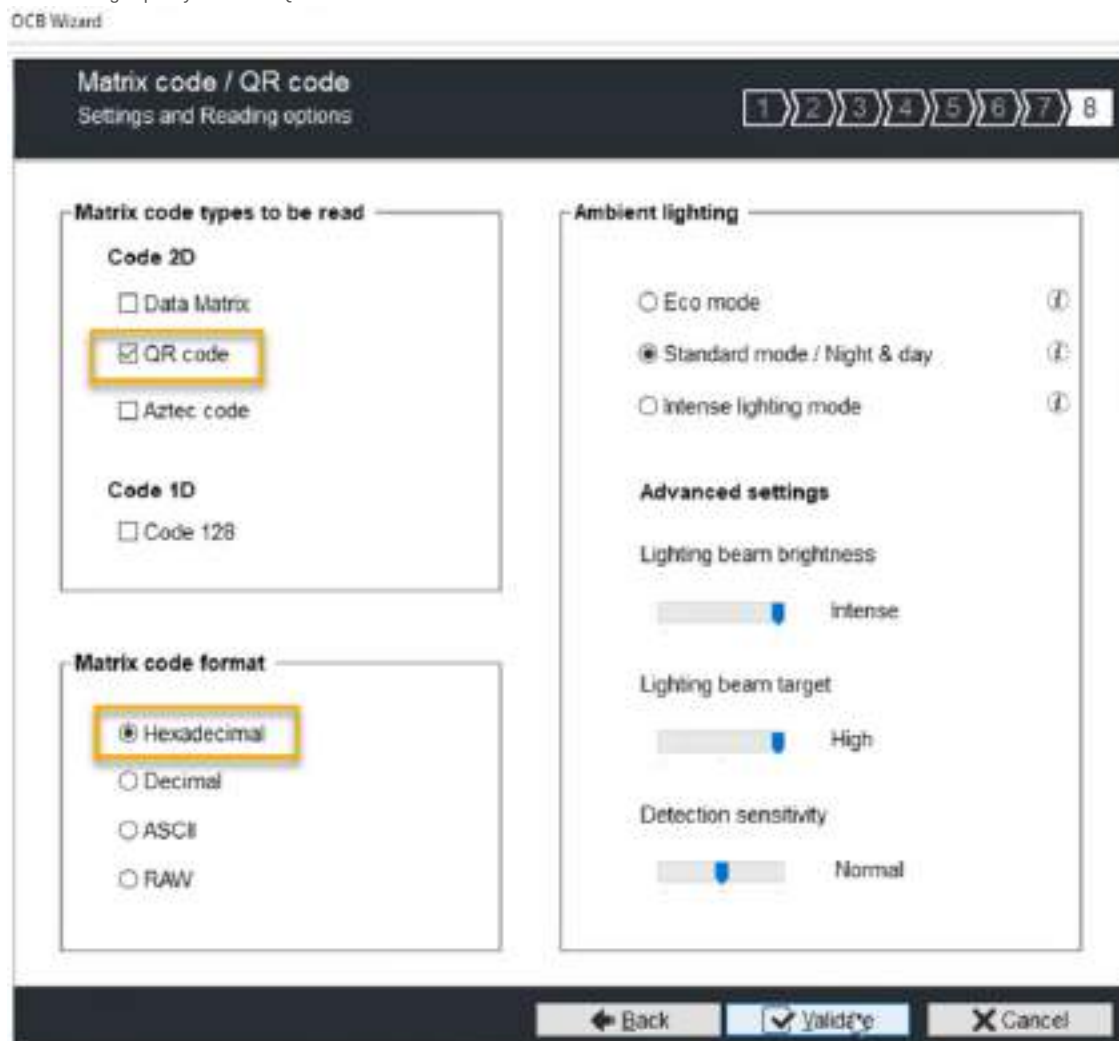


d. Click Next to skip the Blue/NFC Mobile ID options dialog.



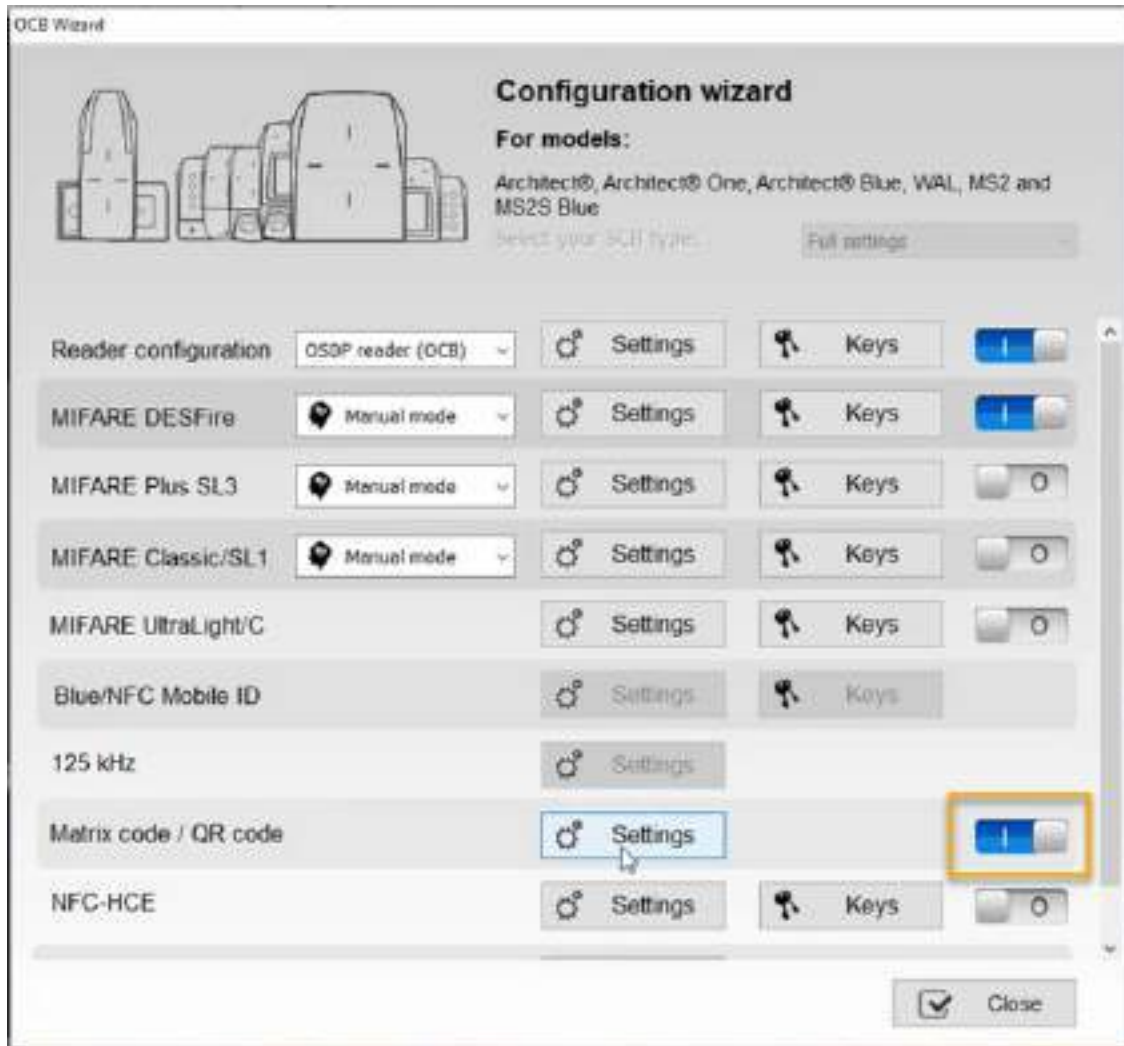
5. In the Matrix code types to be read section of the Matrix code / QR code dialog, select the QR code check box only. Then in the Matrix code format section, select the Hexadecimal check box.

These settings specify that a 2D QR code can be read and sent in hexadecimal format.



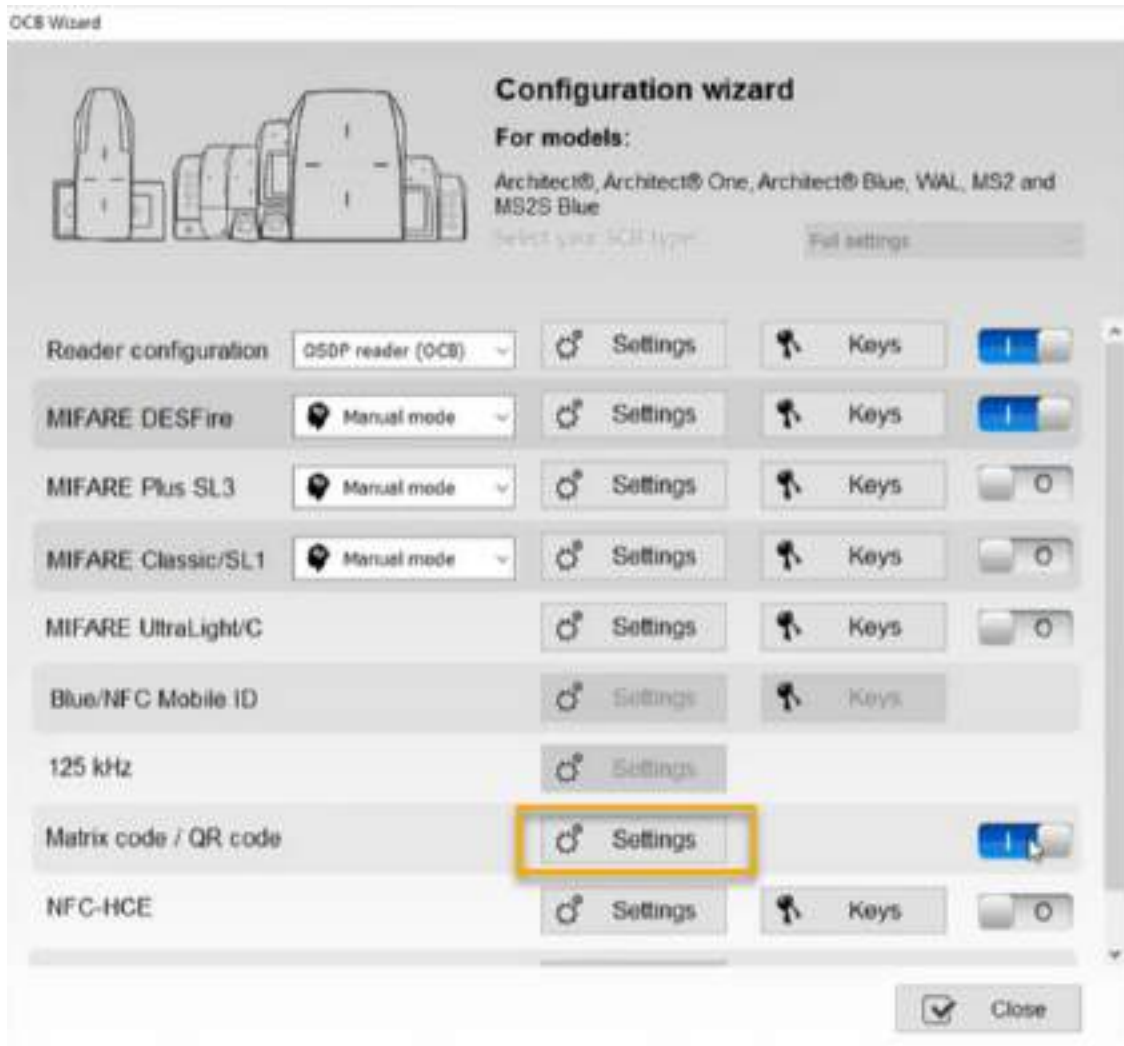
- a. (Optional) In the Ambient lighting section, modify the settings if required.
- b. Click Validate.

6. In the Matrix code / QR code row, drag the slider to the enabled position.



Tip: If the Matrix code / QR code section is not available for selection in the Configuration wizard, make sure that you have validated your Reader configuration as detailed earlier.

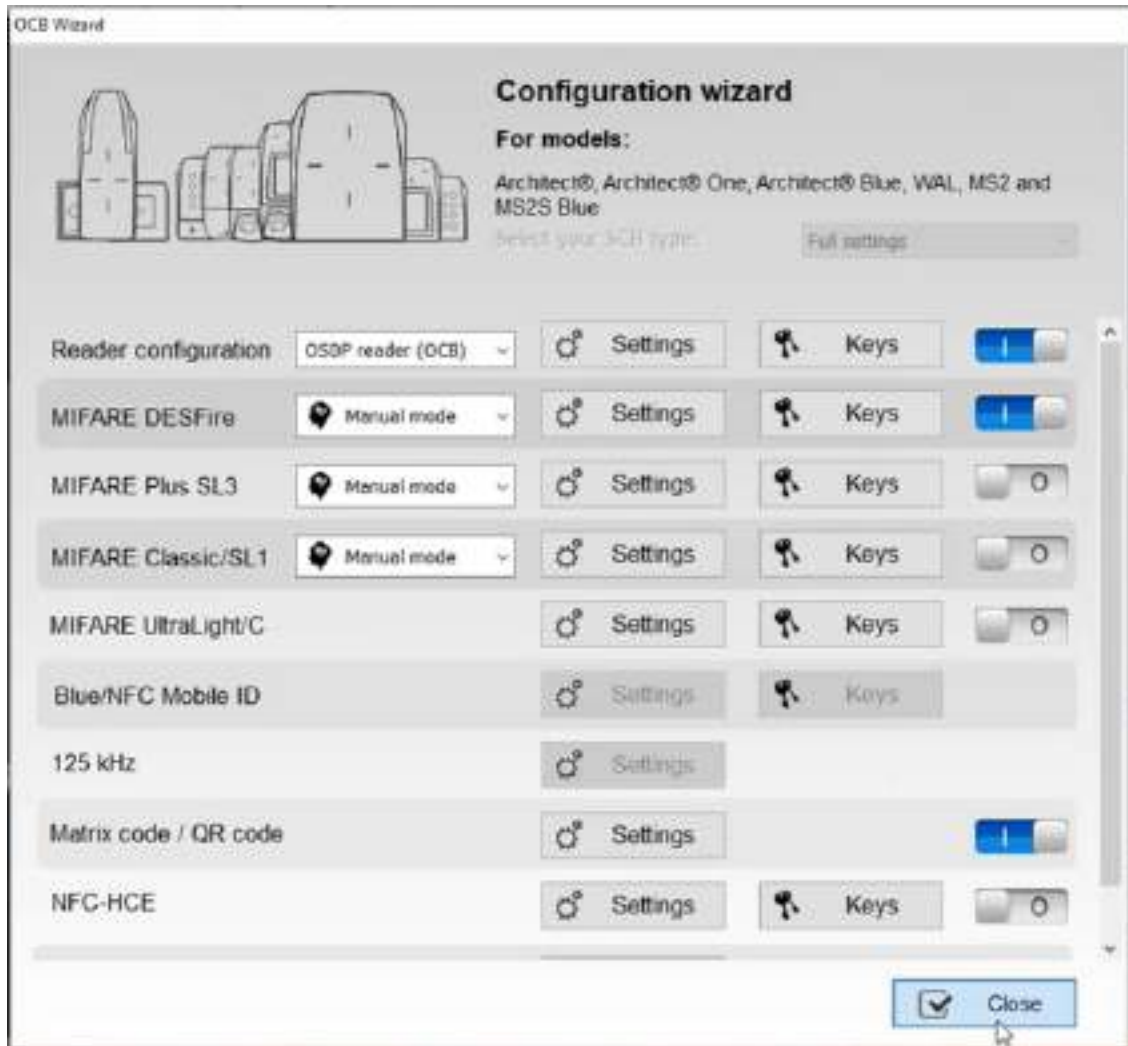
7. In the Matrix code / QR code row, click Settings.



a. In the Matrix code / QR code settings dialog, use the default settings and click Validate.



b. Click Close.



Results

Your STid QR code reader configuration has now been created.

After you finish

Transfer your reader configuration to your STid QR code reader.

Parent topic: Configuring STid devices for ClearID

9.13.4.3 | Transferring your reader configuration to your STid QR code reader for ClearID

QR codes as a credential for visitors in ClearID >

Before you can use QR codes as a credential in Genetec ClearID™, you must complete your STid QR code reader configuration by configuring an STid OCB smart card so that you can transfer the reader configuration to the STid QR code reader.

Before you begin

Familiarize yourself with the STid SECard documentation:

- SECard - High security programming kits
- SECard User Manual
- Install the STid SECard - High security programming kit software
- Create your STid QR code reader configuration

What you should know

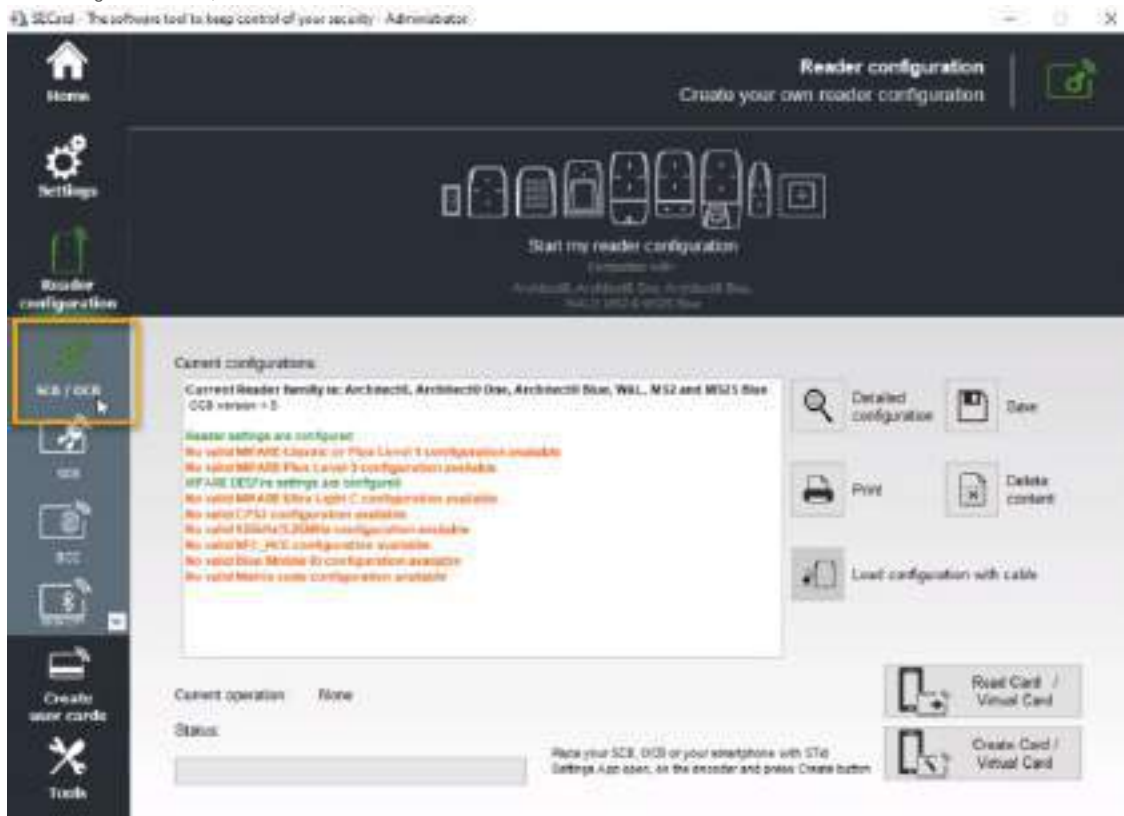
This procedure is for system integrators or account administrators who install and configure QR code readers.

NOTE: Ensure that you have a USB encoder installed and ready to configure your OCB card. For example, the STid Architect® ARC-G desktop reader, enroller, encoder.



Procedure

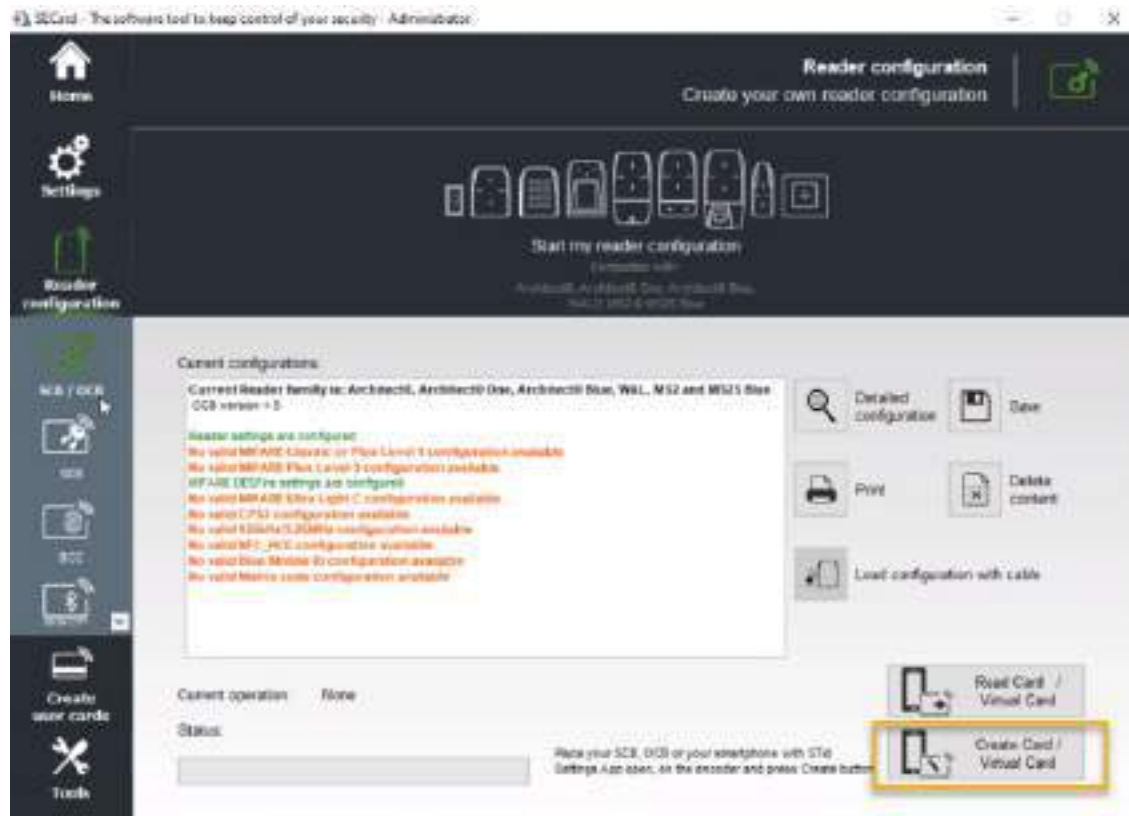
1. Launch the STid SECard software to configure your card.
2. In the navigation sidebar, click SCB / OCB.



3. Create your STid OCB card.
 - a. Place the OCB card on your USB encoder (reader).



- b. Click Create Card / Virtual Card to create your configuration card.

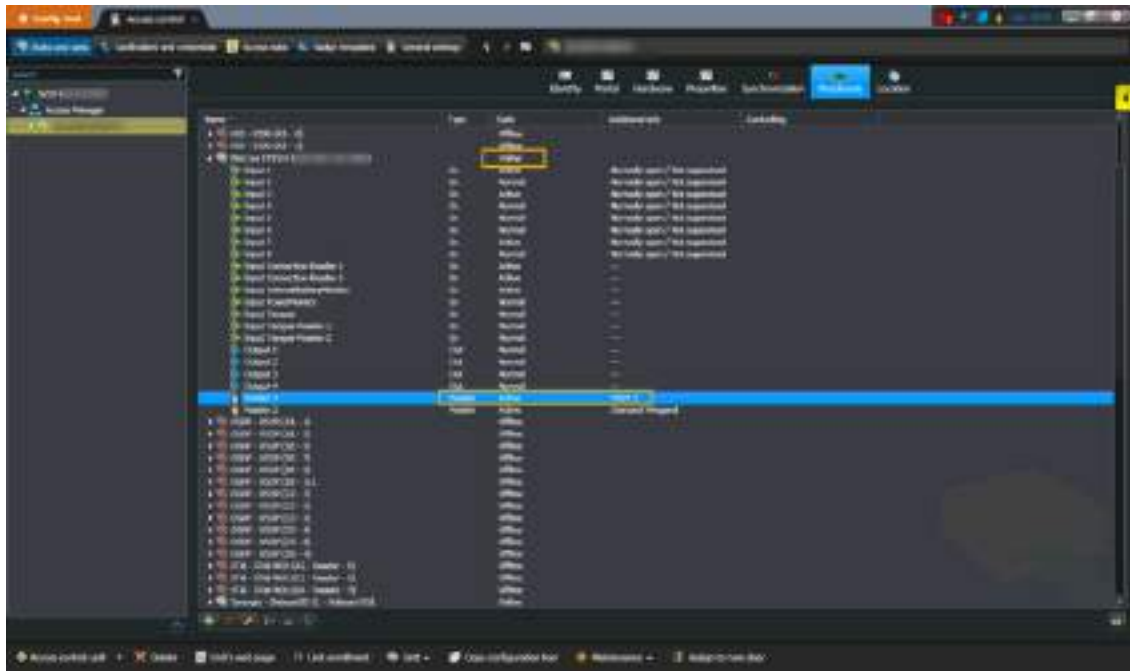


4. Take the OCB smart card containing your reader configuration to the location of your new QR code reader and pass the card in front of the reader.



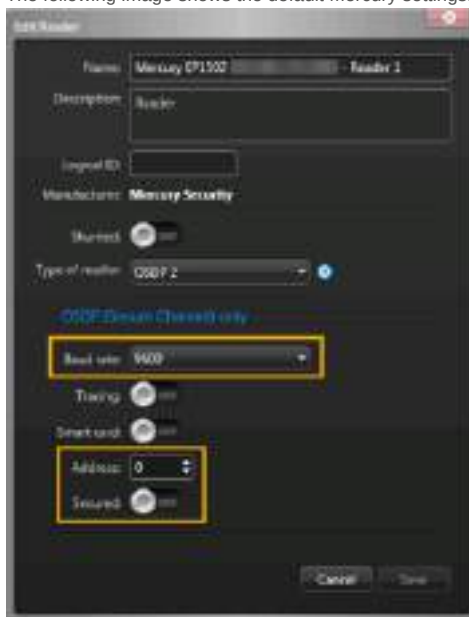
NOTE: Your new QR code reader must be online and available for the QR code reader to transfer the QR code reader configuration settings from the smart card to your QR code reader.

5. Verify your QR code reader is still active after the OCB has been swiped on the wall reader.
- In Config Tool, open the Access control task.
 - In the Roles and units view, navigate to and select your access control unit.
 - In the Peripherals tab Name field, Select your OSDP reader.



- d. In the Peripheral tab Name field, verify that the ODSP reader State is Online.
- e. In the Peripheral tab Name field, verify that the Reader State is Active.
- f. Double-click your reader (Reader 1) in the Edit Reader dialog, make sure your settings match the reader settings.

The following image shows the default Mercury settings:



After you finish

Add doors to areas.

Parent topic: [Configuring STId devices for ClearID](#)

9.13.5 | Automating visitor access and check-in using a macro in Security Center

You can configure a Security Center macro to automatically check in and grant access to visitors at specified parking entrances or gated facilities. The macro can be used for visitors who need access to a parking entrance or gated facility before they can check in or at locations without self-service kiosks.

Before you begin

- Import a custom card format (QR code credential) in Synergis™
- Enable QR code credentials for visitors

What you should know

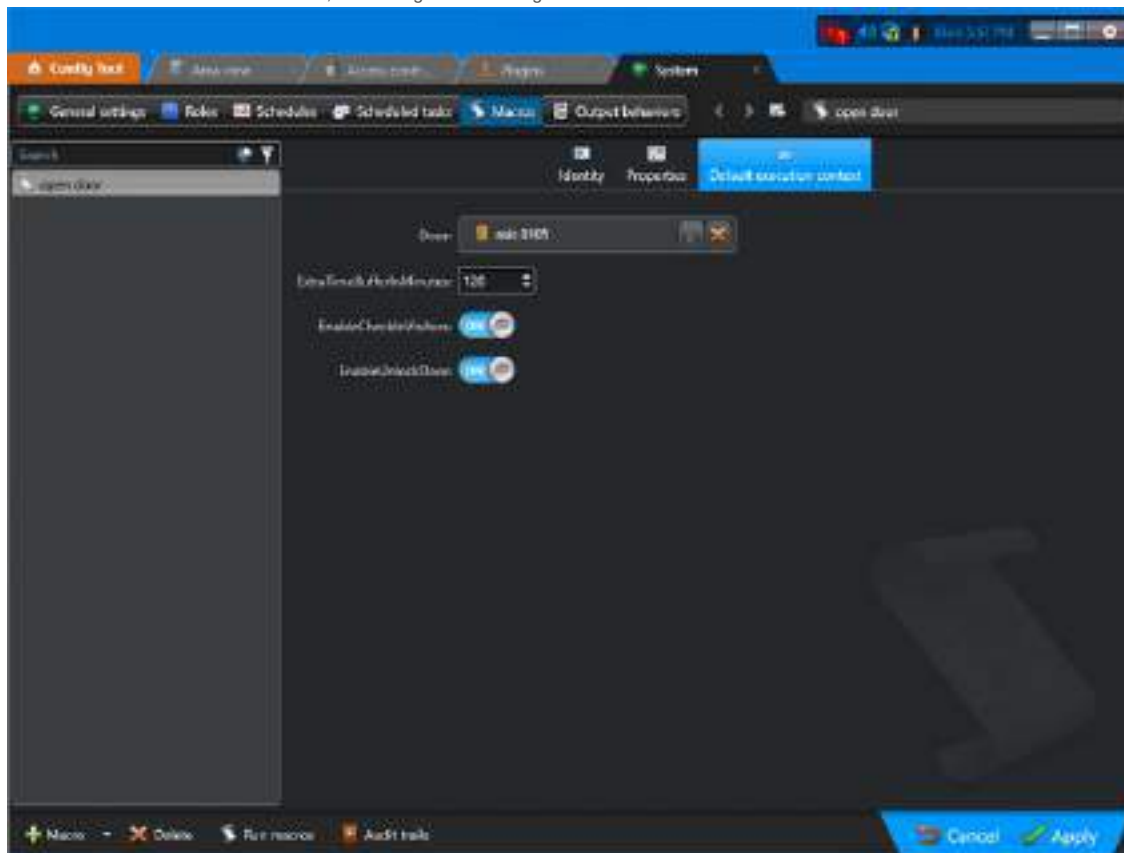
This macro is only for use when sites want to use a QR code as a credential to automate visitor check-in. The macro can grant access for a specified parking entrance or gated facility automatically before visitor check-in.



IMPORTANT: This procedure is only compatible with Security Center 5.11 and later.

Procedure

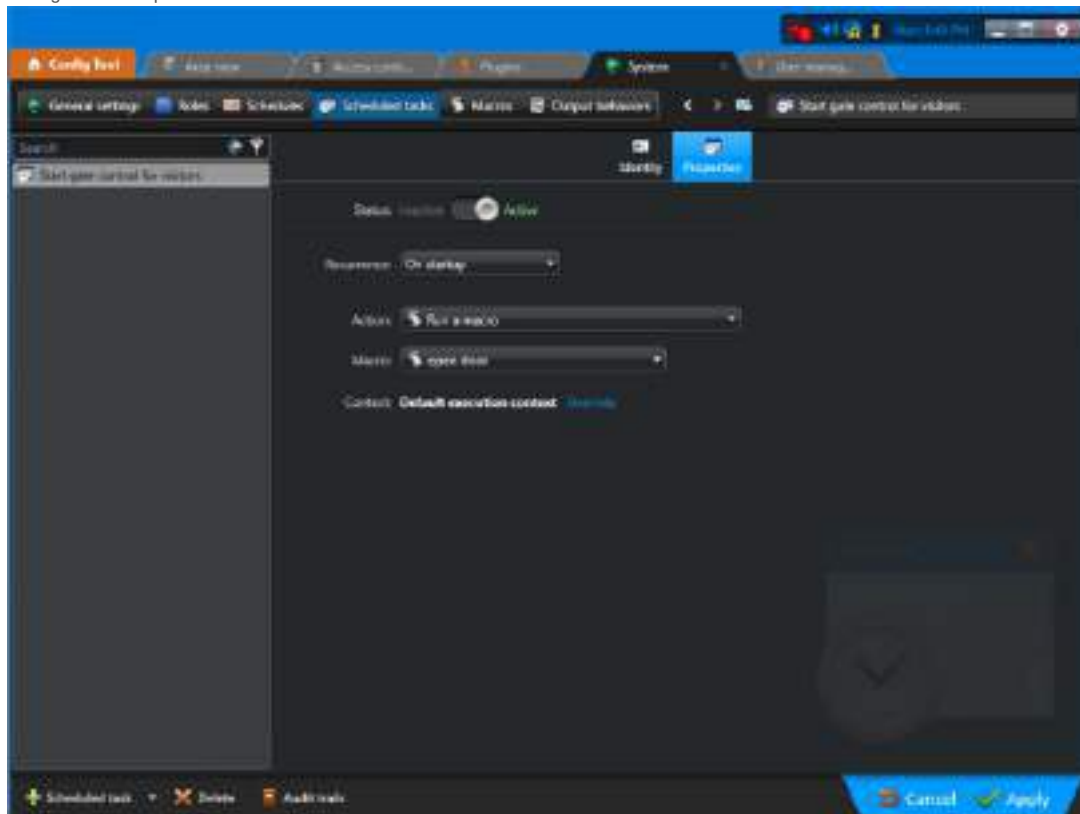
1. From the Config Tool homepage, open the System task and click the Macros view.
2. Click Macro (+), and enter the macro name.
3. Click the Properties tab, and do one of the following:
 - Cut and paste the Macro file code into the Macro definition (C#) section in the Properties tab.
 - Macro 1 (C# example) : Compatible with Security Center 5.7 SR4 - 5.11.2.
 - Macro 2 (C# example) : Compatible with Security Center 5.11.3 or later.
 - Import the source code from a file by clicking Import from file, select the file containing the C# code, and then click Open.
4. Click the Default execution context tab, and configure the settings as follows:



NOTE: The door selected in the Default execution context relates to a specific parking entrance or gated facility entrance. When a visitor presents their QR code, the macro is triggered to automatically provide access for this door only.

5. Click Apply.
6. Click Run macros.
7. From the Config Tool homepage, open the System task and click the Scheduled tasks view.

- a. Click Scheduled task (📅), and enter the scheduled task's name.
- b. Configure the Properties tab as follows:



- c. (Optional) In the Context section, click Override hyperlink to change the macro's execution context:



Results

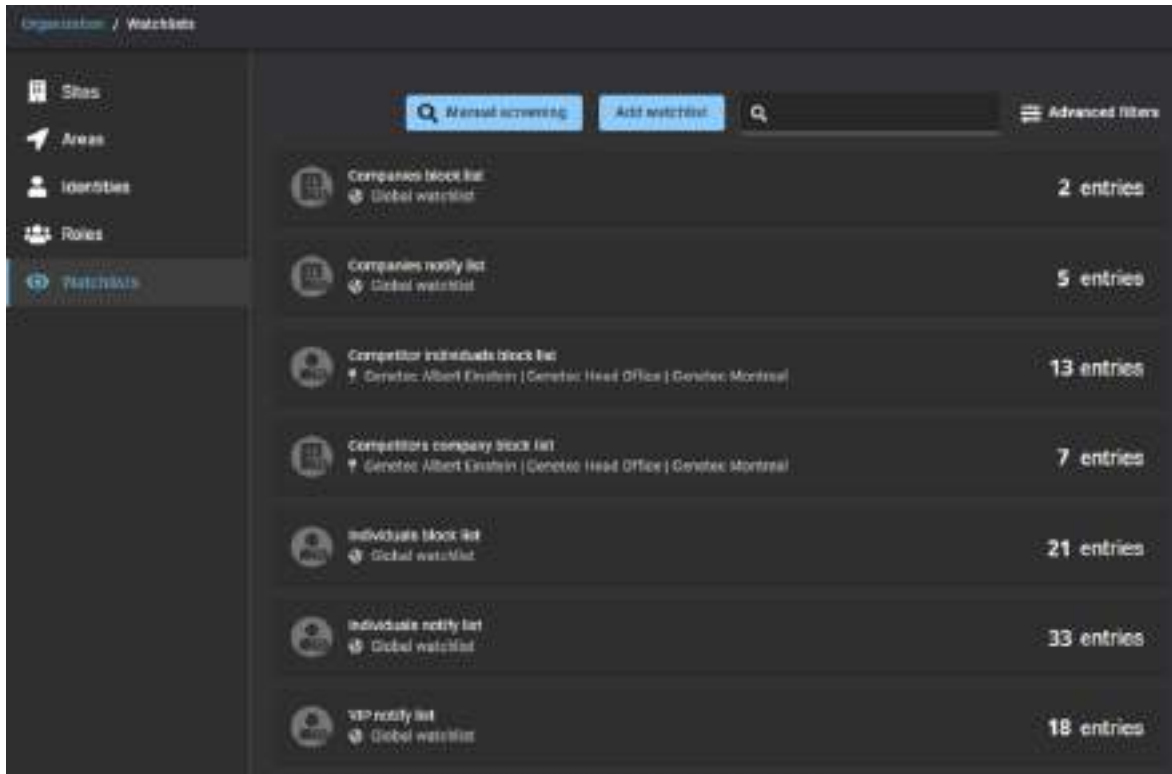
The Security Center macro is now configured. It can trigger automatic check-in and grant access to specific parking entrances or gated facilities when the relevant QR code is scanned at the entrance.

Parent topic: QR codes as a credential for visitors in ClearID

10 | Managing visitor watchlists

10.1 | About watchlists in ClearID

In Genetec ClearID™, watchlists are used to screen visitors at an individual or company level. You can configure the watchlist to perform allow, block, or notify actions at a site or global level.



Screening matches only occur when the following applies:

- Individuals: There is a First name and Last name match, First name and Last name alias match, or Email address match.
- Companies: There is a Company name, company domain, or email address domain match.

There are two types of watchlist:

- Individuals watchlist
- Companies watchlist



An Individuals watchlist is used to monitor visitor check-ins for *persons of interest* listed in a watchlist and then take action as specified in the watchlist configuration. For example, you might create an individuals watchlist to automatically block visitors listed in a watchlist and notify watchlist managers. For other situations, you might only notify watchlist managers. You might also create an individuals watchlist to notify all watchlist managers when VIPs check-in at your site.



A Companies watchlist is used to monitor visitor check-ins for *companies of interest* listed in a watchlist and then take action as specified in the watchlist configuration. For example, you might create a companies watchlist to automatically block access for people with a Company name, company domain, or email address domain that matches specific companies of interest listed in this watchlist.

NOTE: The *Individuals* or *Companies* listed in the entries inside a watchlist can be entered individually or imported as a whole using a .CSV file.

Watchlist behavior

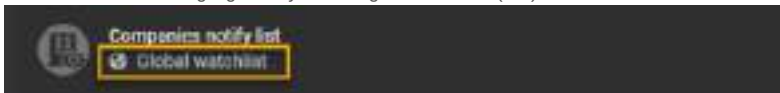
The behavior of the watchlists can be configured differently as follows:

- Notify watchlist managers.
- Automatically block visitors listed in a watchlist and notify watchlist managers.

Global watchlists

In Genetec ClearID™, a global watchlist is a watchlist that is enforced across all sites in your system.

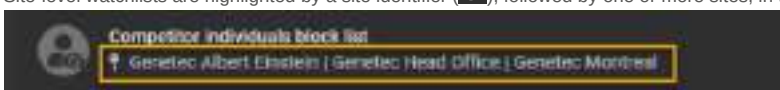
Global watchlists are highlighted by a world globe identifier (🌐) in the watchlist view as follows:



Site watchlists

If a watchlist is not configured as a *global watchlist*, it is considered a site-level watchlist and can be applied to one or more sites.

Site-level watchlists are highlighted by a site identifier (📍), followed by one or more sites, in the watchlist view as follows:



Reasons to block or notify

Reasons to block entry to visitors listed in a watchlist, or notify a watchlist manager might include one or more of the following:

- Serious criminal records by Government agency
- Violent activity or threats
- False Credentials
- Contraband items
- Theft
- Safety violation
- Other reasons

NOTE: Only a *watchlist manager* can view the reasons why visitors are in notify or block watchlists.

10.2 | Adding watchlist managers in ClearID

In Genetec ClearID™, a watchlist manager is an identity that is responsible for watchlists. A watchlist manager can create or modify watchlists and add individuals or companies to a watchlist. They are also responsible for configuring watchlists as a site-specific watchlist or a global watchlist. Before you can add or modify watchlists or configure watchlist settings, you must add your watchlist managers.

Before you begin

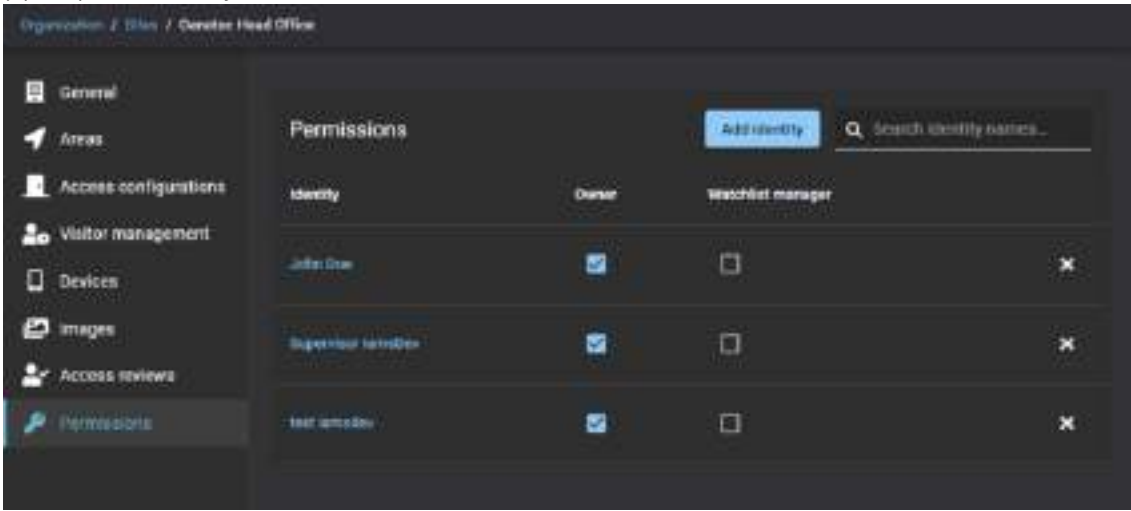
Create your sites.

What you should know

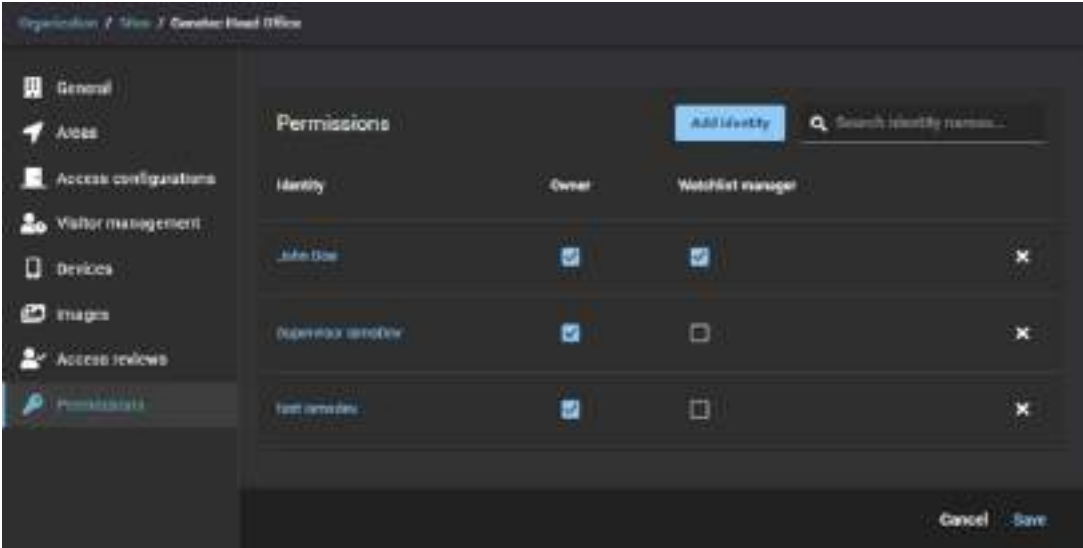
To add watchlist managers in Genetec ClearID™, you must be an account administrator.

Procedure

1. Click Organization > Sites.
2. Select your site and click Permissions.
3. (Optional) Click Add identity to add identities to the site Permissions list.



- a. Search for or select the identities that you require and click Add.
Tip: You can click the identity hyperlink in the Identity column to review identity details (company, department, home site, supervisor, and email) and to verify that you have the correct identities in the list.
4. Select the Watchlist manager check box to assign watchlist manager permissions to an identity.
 - a. (Optional) Clear a check box to remove individual permissions that are no longer required from an identity.
 - b. (Optional) Click  to remove all permissions that are no longer required from an identity.



5. Click Save.

After you finish

[Add your watchlists.](#)

10.3 | Adding watchlists in ClearID

Add individuals watchlists or companies watchlists so that you can screen visitors at an individual level or company level and automatically perform block or notify actions at a site or global level as specified in the watchlist configuration.

Before you begin

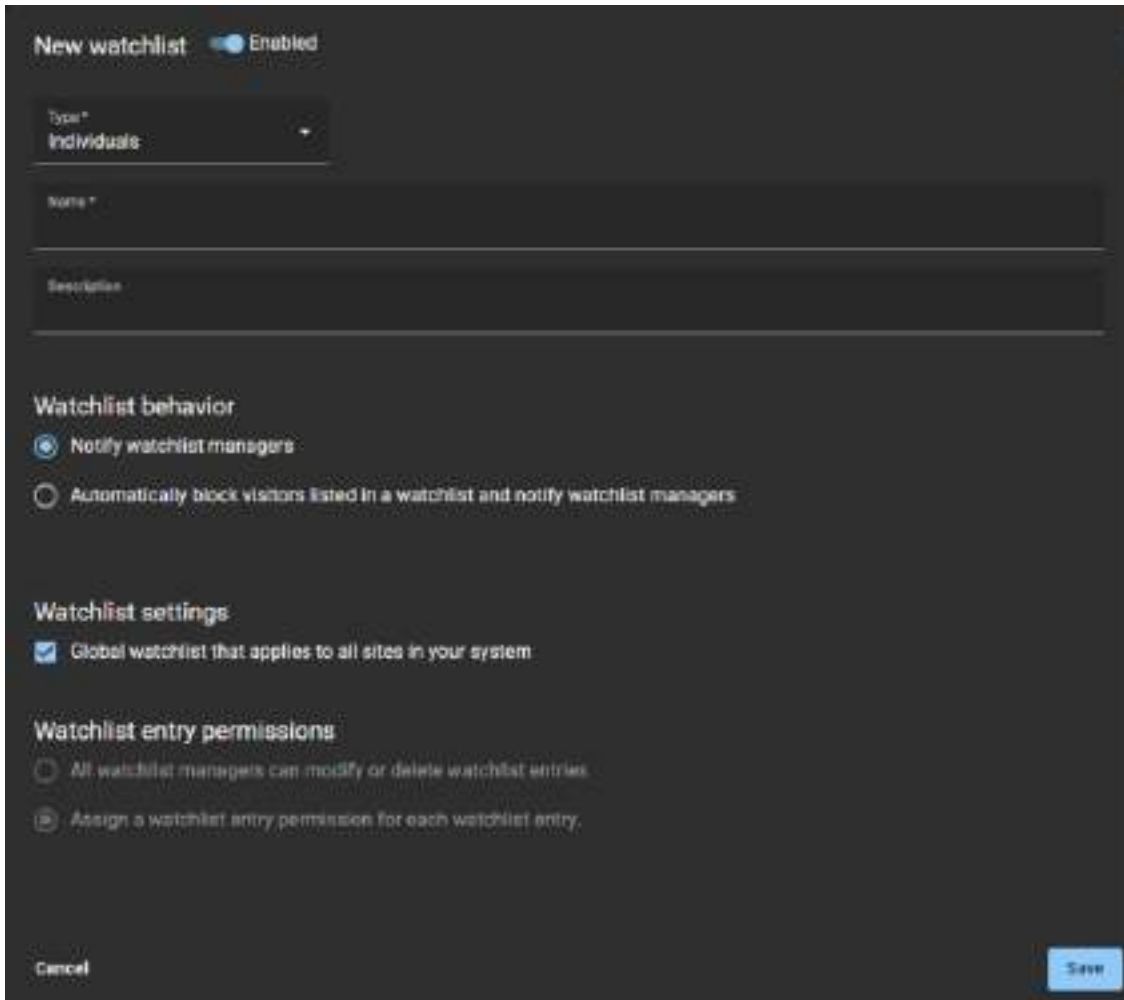
[Learn about watchlists.](#)

What you should know

- Any *watchlist manager* or account administrator can modify or delete any watchlist that is configured as a *global watchlist*.

Procedure

- Click Organization > Watchlists.
- Click Add watchlist.



3. At the top of the new watchlist, click the Enabled slider to enable or disable the watchlist.
4. In the Type field, select a watchlist type. From the list select either Individuals or Companies:

Individuals



An Individuals watchlist is used to monitor visitor check-ins for *persons of interest* listed in a watchlist and then take action as specified in the watchlist configuration. For example, you might create an individuals watchlist to automatically block visitors listed in a watchlist and notify watchlist managers. For other situations, you might only notify watchlist managers. You might also create an individuals watchlist to notify all watchlist managers when VIPs check-in at your site.

Companies



A Companies watchlist is used to monitor visitor check-ins for *companies of interest* listed in a watchlist and then take action as specified in the watchlist configuration. For example, you might create a companies watchlist to automatically block access for people with a Company name, company domain, or email address domain that matches specific companies of interest listed in this watchlist.

5. Enter a Name for the watchlist.
The name of a watchlist can be changed at any time to suit your needs.
Tip: Consider using a *discreet name* where applicable to avoid divulging sensitive information about why someone might be blocked or on a list when the notification is sent to people.
6. Enter a Description for the watchlist.
7. In the Watchlist behavior section, select one of the following:
 - Notify watchlist managers
 - Automatically block visitors listed in a watchlist and notify watchlist managers
8. In the Watchlist settings section, choose whether you want a global watchlist or a site-specific watchlist.
 - To apply the watchlist to all sites in your system, select Global watchlist that applies to all sites in your system.
 - To apply the watchlist to one or more specific sites, clear the Global watchlist that applies to all sites in your system check box.
 - a. If you chose to apply your watchlist at a site-level, add your sites and press enter.
 - b. Repeat at necessary.

NOTE: The Watchlist entry permissions section is disabled if the Global watchlist that applies to all sites in your system check box is selected.
9. If you have Watchlist entry permissions activated for your account, in the Watchlist entry permissions section, select one of the following:
 - All watchlist managers can modify or delete watchlist entries.
 - Assign a watchlist entry permission for each watchlist entry

All watchlist managers can modify or delete watchlist entries

Specifies that watchlist entries can only be modified or deleted by all watchlist managers for the specified sites.

Assign a watchlist entry permission for each watchlist entry

Specifies that watchlist entry permissions are assigned at a more granular site level in each watchlist entry. This means that only watchlist managers for the site can modify or delete entries.

Example 1: Individuals block watchlist - configured as a global watchlist to automatically block visitors and notify watchlist managers.

The screenshot shows the 'New watchlist' configuration interface. At the top, the title 'New watchlist' is followed by a toggle switch labeled 'Enabled'. Below this, there are three input fields: 'Type' with a dropdown menu showing 'Individuals', 'Name' with the text 'Individuals BLOCK list', and 'Description' with the text 'Automatic block GLOBAL watchlist all sites'. The 'Watchlist behavior' section contains two radio button options: 'Notify watchlist managers' and 'Automatically block visitors listed in a watchlist and notify watchlist managers', with the latter being selected. The 'Watchlist settings' section has a checked checkbox for 'Global watchlist that applies to all sites in your system'. The 'Watchlist entry permissions' section contains two radio button options: 'All watchlist managers can modify or delete watchlist entries' and 'Assign a watchlist entry permission for each watchlist entry', with the latter being selected. At the bottom left is a 'Cancel' button, and at the bottom right is a 'Save' button.

New watchlist ☒ Enabled

Type *
Individuals

Name *
Individuals BLOCK list

Description
Automatic block GLOBAL watchlist all sites

Watchlist behavior

☐ Notify watchlist managers

☒ Automatically block visitors listed in a watchlist and notify watchlist managers

Watchlist settings

☒ Global watchlist that applies to all sites in your system

Watchlist entry permissions

☐ All watchlist managers can modify or delete watchlist entries

☒ Assign a watchlist entry permission for each watchlist entry

Cancel Save

Example 2: Companies notify watchlist - configured as a site-specific watchlist to notify watchlist managers when visitors are from a competitors company.

New watchlist ☒ Enabled

Type*
Companies

Name*
Companies NOTIFY list

Description
Notify when visitors from Competitor company visit specific sites

Watchlist behavior

☒ Notify watchlist managers

☐ Automatically block visitors listed in a watchlist and notify watchlist managers

Watchlist settings

☐ Global watchlist that applies to all sites in your system

Watchlist sites

Genetec Albert Einstein Genetec Head Office Genetec Marinsai [Add more](#) To add a site, start typing and press Enter

Watchlist entry permissions

☒ All watchlist managers can modify or delete watchlist entries

☐ Assign a watchlist entry permission for each watchlist entry.

Cancel Save

10. Click Save.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Do one or more of the following:

- [Add your individuals watchlist entries](#)
- [Add your companies watchlist entries](#)

10.3.1 | Adding an individuals watchlist entry in ClearID

Add one or more individuals watchlist entries so that you can screen visitors at an individual level and automatically perform block or notify actions at a site or global level as specified in the watchlist configuration.

Before you begin

[Add your watchlists.](#)

What you should know

Only a *watchlist manager* can:

- Add individuals watchlist entries.
- View reasons why visitors are in notify or block watchlists.

Procedure

1. Click Organization > Watchlists.
2. Select a watchlist from the list.
3. Click Add entry.

Individual ☒ Enabled

Watchlist entry criteria

First name * Middle name Last name *

First name aliases
To add an alias, start typing and press Enter

Last name aliases
To add an alias, start typing and press Enter

Emails
To add an email, start typing and press Enter

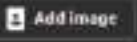
Emails to always allow

Emails
To add an email, start typing and press Enter

Additional information

Physical description

Location

 Add image

Date of birth
MM/DD/YYYY 

External reference ID

Company name

Permissions

This entry can only be modified or deleted by the watchlist manager for the following sites

Sites with watchlist entries that can be modified or deleted
To add a site, start typing and press Enter

Cancel Save

4. At the top of the watchlist entry click the Enabled slider to enable or disable the watchlist entry.

5. In the Watchlist entry criteria section, complete the fields:

First name

Enter a first name.

Middle name

Enter a middle name.

Last name

Enter a last name.

First name aliases

Add any known first name aliases and press enter. Repeat as required.

NOTE: Aliases are shown in brackets in the watchlist entries list.

Last name aliases

Add any known last name aliases and press enter. Repeat as required.

Emails

Add any known emails and press enter. Repeat as required.

Genetec ClearID™ User Guide

Displayed in the header

6. In the Emails to always allow section, add any emails that you want to exclude from the watchlist screening process.

This section is used to add any similar emails or false positive email matches that you might want to always allow. For example, a possible match that happens to have the same name details, but is a different person with a different email address that should be allowed.

7. In the Additional information section, complete any additional fields that you require:

Physical description

Enter a physical description.

Reason

Enter a reason for the block or notify.

NOTE: The Reason field can contain sensitive private information, and can only be viewed by the watchlist manager for the site.

Date of birth

Use the calendar picker to enter a date of birth.

The date of birth information is useful additional information when a visitor check-in matches multiple people with the same name. It can be used to validate an identity and also eliminate duplicates or false positive matches.

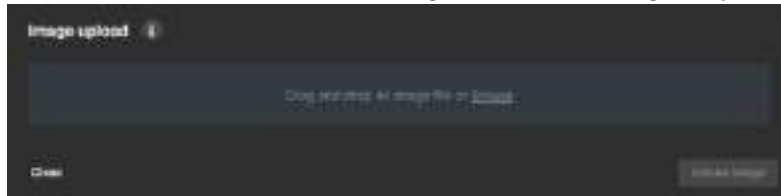
External reference ID

Enter an external reference ID.

Company name

Enter a company name.

8. In the Additional information section, Click Add image to add one or more images if required.



a. Drag and drop an image or click Browse to select the image file that you require and click Upload image.

b. Repeat for each additional image you want to upload.

c. (Optional) Click Delete image for any images you no longer require.

Tip: Click Open in new tab to view the image full size.

9. If you have Watchlist entry permissions activated for your account, in the Permissions section, add the sites that you require.

10. Click Save.

Example



After you finish

Test your watchlist entries.

Parent topic: [Adding watchlists in ClearID](#)

10.3.2 | Adding a companies watchlist entry in ClearID

Add one or more companies watchlist entries so that you can screen visitors at a company level and automatically perform block or notify actions at a site or global level as specified in the watchlist configuration.

Before you begin

Add your watchlists.

What you should know

Only a *watchlist manager* can:

- Add companies watchlist entries.
- View reasons why visitors are in notify or block watchlists.

Procedure

1. Click Organization > Watchlists.
2. Select a watchlist from the list.
3. Click Add entry.

The screenshot shows a web form for adding a watchlist entry. At the top, there is a 'Company' header with an 'Enabled' toggle switch. Below this is the 'Watchlist entry criteria' section, which includes a 'Company name' field, a 'Company aliases' field with a hint 'To add an alias, start typing and press Enter', and a 'Company domains' field with a hint 'To add a domain, start typing and press Enter' and the example 'www.example.com'. The 'Additional information' section contains a 'Reason' field with a lock icon and an 'External reference ID' field. The 'Permissions' section states 'This entry can only be modified or deleted by the watchlist manager for the following sites' and includes a list of sites with a hint 'To add a site, start typing and press Enter'. At the bottom, there are 'Cancel' and 'Save' buttons.

4. At the top of the watchlist entry click the Enabled slider to enable or disable the watchlist entry.
5. In the Watchlist entry criteria section, complete the fields:

Company name

Enter a company name.

Company aliases

Add any known company aliases and press enter. Repeat as required.

NOTE: Aliases are shown in brackets in the watchlist entries list.

Company domains

Add any known company domains and press enter. Repeat as required.

6. In the Additional information section, complete any additional fields that you require:

Reason

Enter a reason for the block or notify.

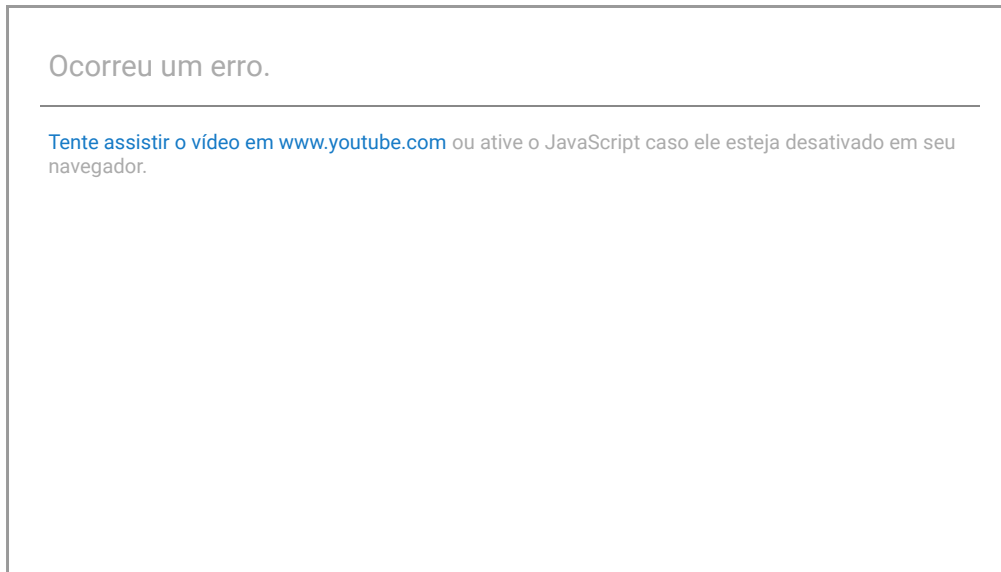
NOTE: The Reason field can contain sensitive private information, and can only be viewed by the watchlist manager for the site.

External reference ID

Enter an external reference ID.

7. If you have Watchlist entry permissions activated for your account, in the Permissions section, add the sites that you require.
8. Click Save.

Example



After you finish

Test your watchlist entries.

Parent topic: [Adding watchlists in ClearID](#)

10.3.3 | Importing watchlist entries from a file in ClearID

To accelerate your watchlist configuration and setup, you can import your watchlist entries from a .CSV file. You can also download a sample .CSV file to help you prepare your watchlist entries file in the correct format.

Before you begin

Prepare your watchlist entries in a .CSV file, ready for import.

What you should know

Only a *watchlist manager* can import watchlist entries.

You can import pre-existing watchlist entry data using a .CSV file from one or more of the following sources:

- Sharepoint
- Excel
- Be on (the) look-out (BOLO) list - a watchlist term typically used in the field of policing.
- No entry list
- Deny entry list (DEL)

Procedure

1. Click Organization > Watchlists.
2. Select a watchlist.
3. Click  and click Import from file.

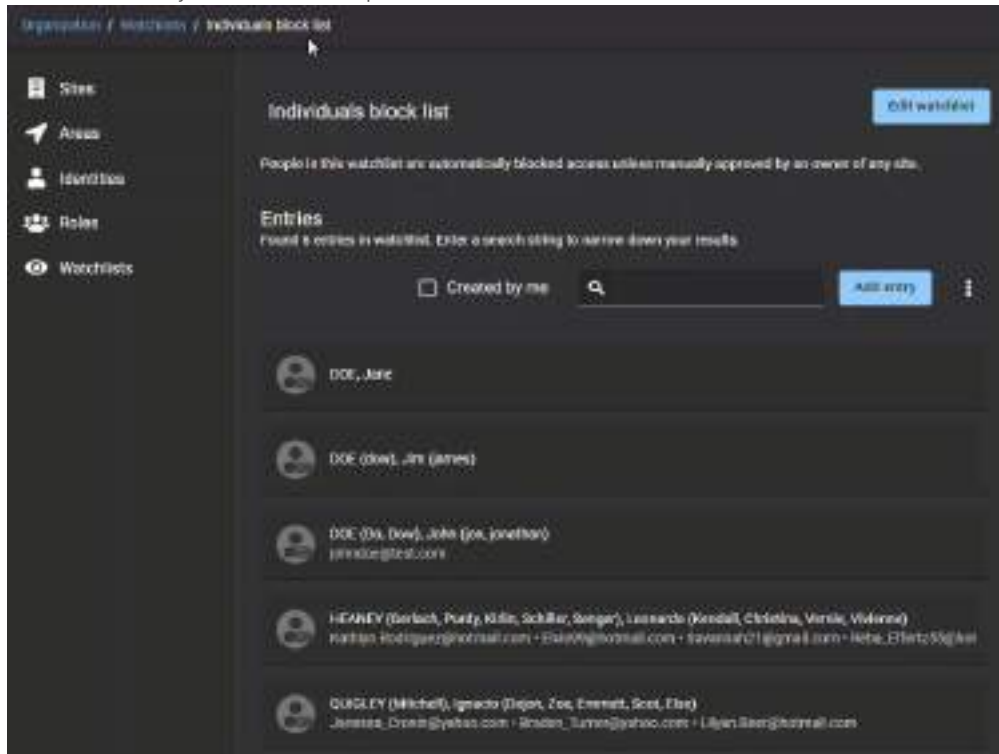


4. (Optional) Click Download a sample CSV file to help you prepare a watchlist entries file in the correct format.

Genetec ClearID™ User Guide

Displayed in the header

NOTE: The columns and entries in the sample CSV file (watchlist-sample.csv) can vary depending on the watchlist type (Individuals or Companies) you have selected when you download the sample.

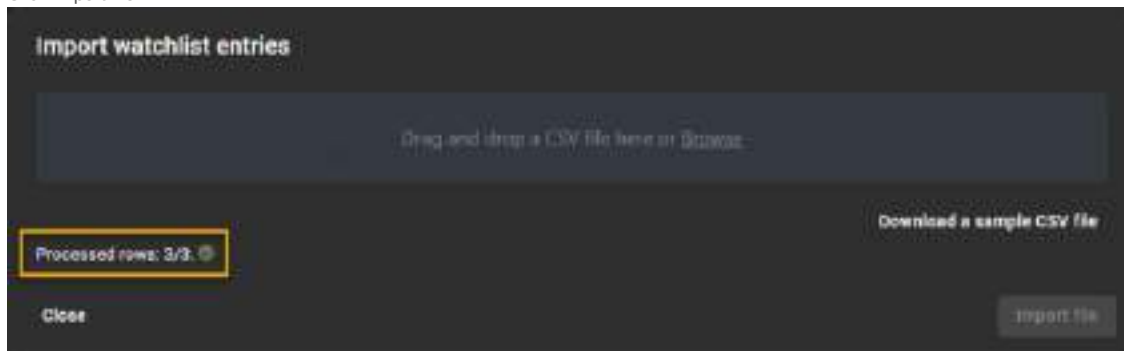


Tip: Click the animation to view full size.

5. In the Import watchlist entries dialog, drag and drop a CSV file or click Browse to select a file.



6. Click Import file.



NOTE: The Processed rows field in the Import watchlist entries dialog indicates how many watchlist entries have been processed.

After you finish

Test your watchlist entries.

Parent topic: Adding watchlists in ClearID

10.3.4 | Exporting watchlist entries to a file in ClearID

You can export your watchlist entries to a .CSV file for mass editing or backup purposes. For example, you could export your watchlist entries to Microsoft Excel, edit the entries, remove any duplicates, and then merge watchlists or consolidate watchlist entries into a new watchlist.

Before you begin

Do one or more of the following:

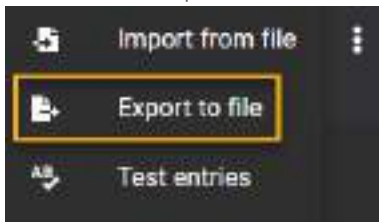
- [Add your individuals watchlist entries.](#)
- [Add your companies watchlist entries.](#)
- [Import your watchlist entries.](#)

What you should know

Only a *watchlist manager* can export watchlist entries.

Procedure

1. Click Organization > Watchlists.
2. Select a watchlist.
3. Click  and click Export to file.



The file is exported as a .CSV file to your browsers default download location. By default the exported file is created using the name of your watchlist. For example, Individuals block list.csv.

4. Follow your browser prompts to complete downloading the exported file.

After you finish

(Optional) Manipulate the watchlist entry data as required.

Parent topic: [Adding watchlists in ClearID](#)

10.3.5 | Testing watchlist entries in ClearID

To test new watchlist entries, you can enter the details of a person of interest or a company of interest to verify if there is a screening match.

Before you begin

Do one or more of the following:

- [Add individuals watchlist entries](#)
- [Add companies watchlist entries](#)

What you should know

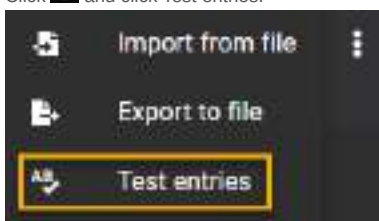
Only a *watchlist manager* can test watchlist entries.

Screening matches only occur when the following applies:

- Individuals: There is a First name and Last name match, First name and Last name alias match, or Email address match.
- Companies: There is a Company name, company domain, or email address domain match.

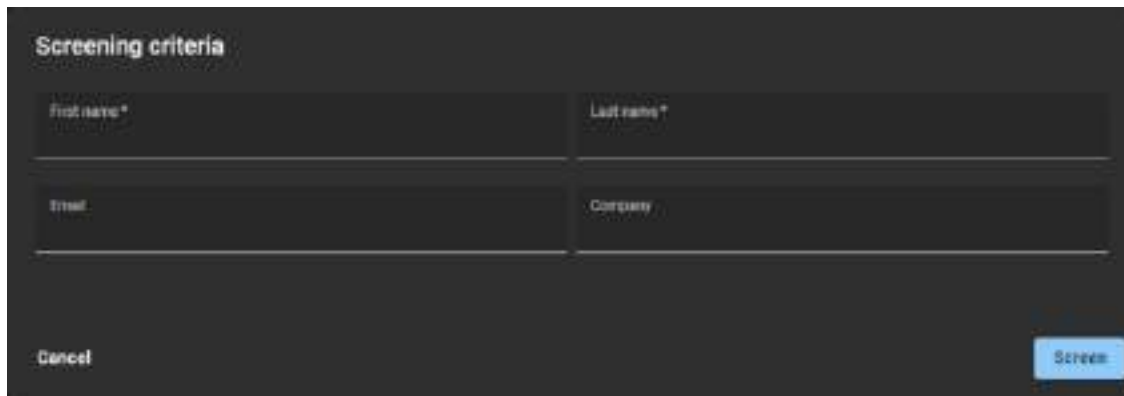
Procedure

1. Click Organization > Watchlists.
2. Select a watchlist.
3. Click  and click Test entries.



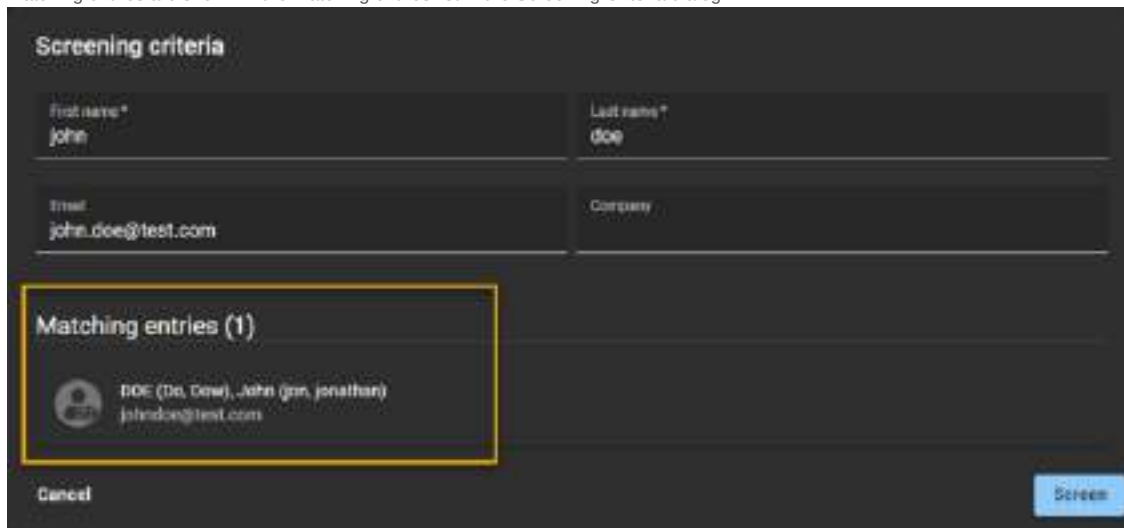
4. In the Screening criteria dialog, enter the details of the entry that you want to test

NOTE: Mandatory fields are highlighted by an asterisk (*).



5. Click Screen.

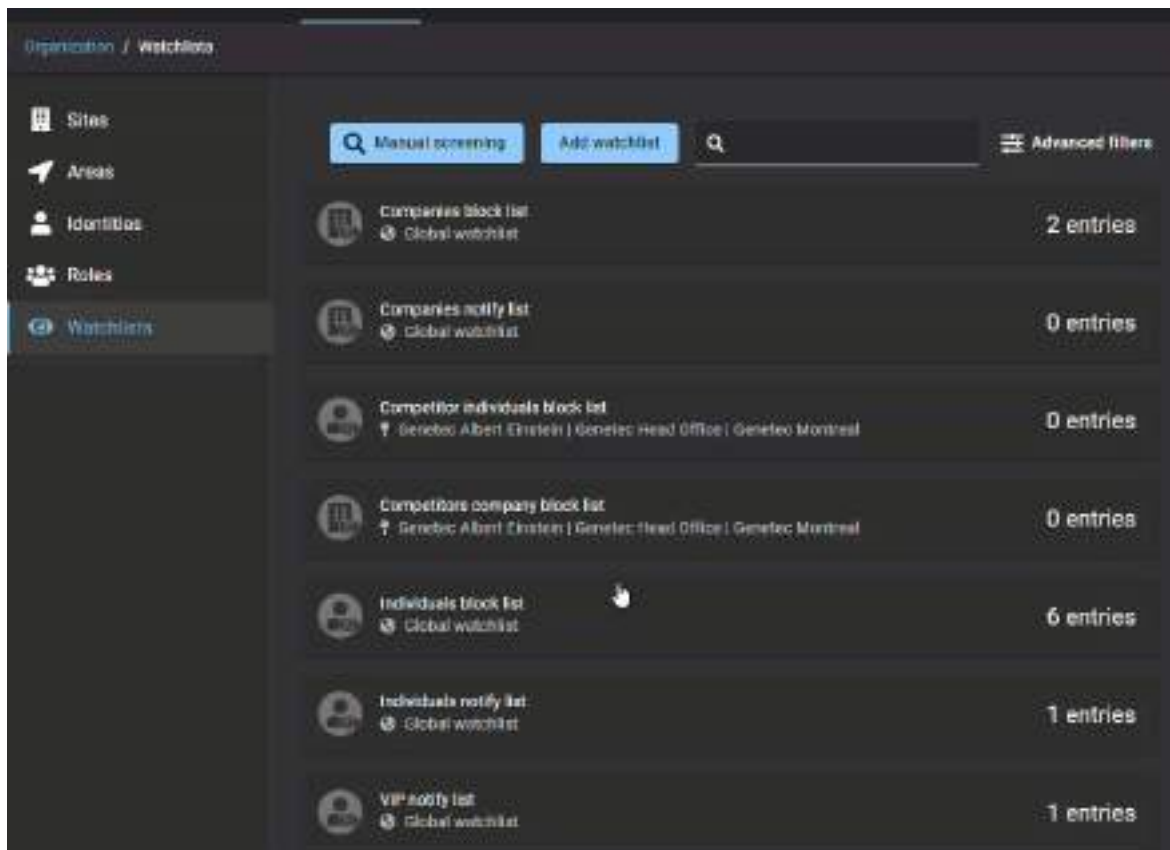
Matching entries are shown in the Matching entries list in the Screening Criteria dialog.



6. (Optional) Click a matching entry in the list to view the complete details of the watchlist entry.

7. Click Cancel to exit the Screening Criteria dialog.

Example



Watchlist Name	Global Watchlist	Entries
Companies block list	Global watchlist	2 entries
Companies notify list	Global watchlist	0 entries
Competitor individuals block list	Global watchlist	0 entries
Competitors company block list	Global watchlist	0 entries
Individuals block list	Global watchlist	6 entries
Individuals notify list	Global watchlist	1 entries
VIP notify list	Global watchlist	1 entries

Parent topic: Adding watchlists in ClearID

10.3.6 | Deleting watchlist entries in ClearID

A watchlist manager can delete individuals watchlist entries or companies watchlist entries that have become obsolete or are no longer required.

Before you begin

Do one or more of the following:

- Add individuals watchlist entries
- Add companies watchlist entries

What you should know

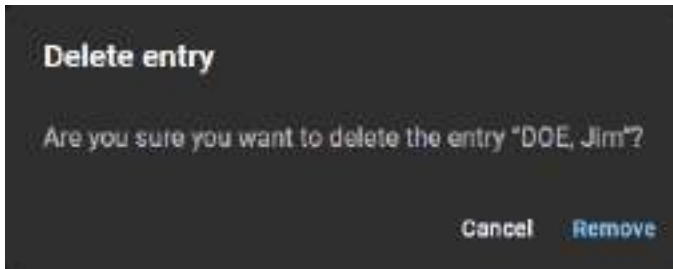
A watchlist entry can only be deleted by the *watchlist manager* who created it.

Procedure

1. Click Organization > Watchlists.
2. Select a watchlist from the list.
3. (Optional) If the watchlist entries list is long, select Created by me to reduce the displayed results.
4. Do one of the following:
 - Click to select a watchlist entry in the list
 - Search for the entry that you want to delete.
5. Scroll to the bottom of the watchlist entry and click Delete entry.

The screenshot shows a 'Delete entry' dialog box for an individual. At the top left, it says 'Individual' with a toggle switch set to 'Enabled'. At the top right is a red 'Delete entry' button. The main section is titled 'Watchlist entry criteria' and contains three input fields: 'First name *' with the value 'Jim', 'Middle name', and 'Last name *' with the value 'Doe'. Below these are two sections for aliases: 'First name aliases' and 'Last name aliases', each with a text input field and a 'done' button. There are also sections for 'Emails' and 'Emails to always allow', each with a text input field. The 'Additional information' section at the bottom includes a profile picture of a man with a beard, a 'Physical description' field, a 'Reason' field with a lock icon, a 'Date of birth' field with a calendar icon and the format 'MM/DD/YYYY', an 'External reference ID' field, and a 'Company name' field. At the bottom left is a 'Cancel' button and at the bottom right is a 'Save' button. A page indicator '1 / 3' is visible at the bottom center.

6. In the Delete entry dialog, click Remove to confirm your deletion.



Parent topic: [Adding watchlists in ClearID](#)

10.4 | Modifying watchlists in Genetec ClearID

After you add your watchlists, you can modify some of the watchlist settings. A watchlist manager can disable a watchlist, change the Name or Description, and change watchlist behavior.

Before you begin

[Add your watchlists.](#)

What you should know

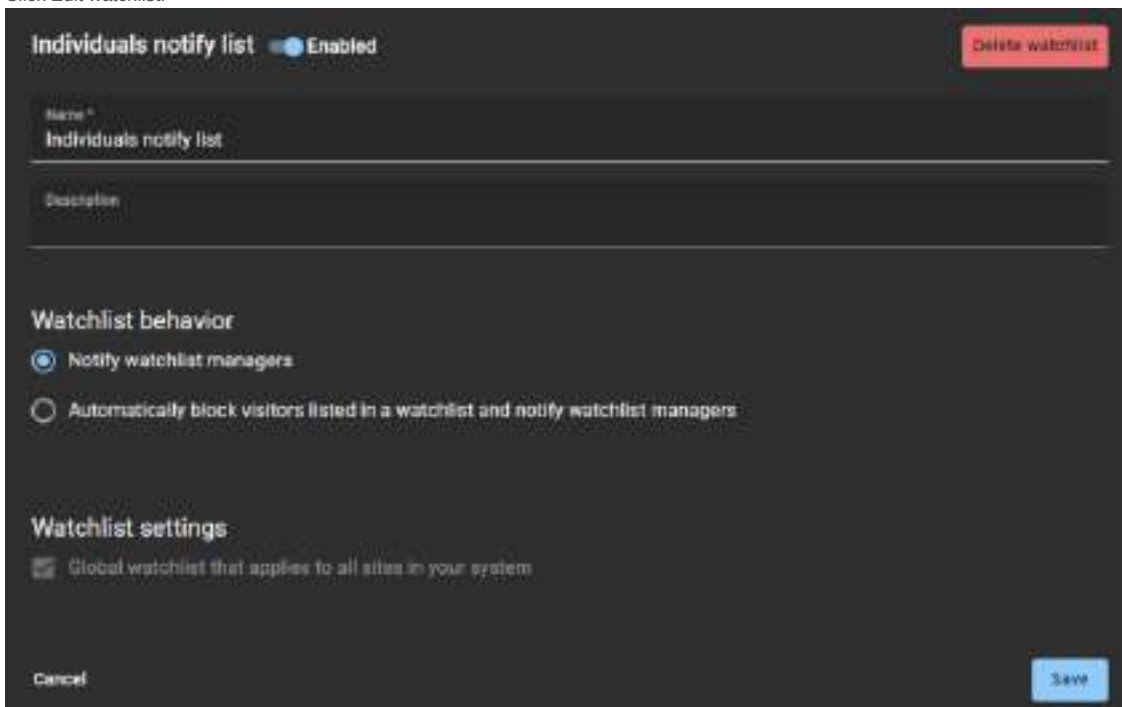
When modifying a watchlist the following applies:

- You cannot change a *global watchlist* to become a *site watchlist*.
- You cannot change a *site watchlist* to become a *global watchlist*.
- You cannot modify Watchlist entry permissions after a watchlist is created.

Any *watchlist manager* or account administrator can modify any watchlist that is configured as a *global watchlist*.

Procedure

1. Click Organization > Watchlists.
2. (Optional) Use the search box to find a specific watchlist.
3. (Optional) Click Advanced filters to filter the list results by Site or Watchlist type.
Select the filter options that you require:
 - a. From the Site list, select a site.
 - b. From the Watchlist types list, select a watchlist type.
 - c. Click Close.
4. Select a watchlist from the list.
5. Click Edit watchlist.



6. Modify the watchlist as required by doing one or more of the following:
 - a. At the top of the Watchlist dialog, click the Enabled slider to enable or disable the watchlist.

For example, you might want to disable a large watchlist and refer to it while restructuring entries into other watchlists.

b. In the Name field, change the watchlist Name.

c. In the Description field, change the watchlist Description.

d. In the Watchlist behavior section, modify the Watchlist behavior. Select either Notify watchlist managers or Automatically block visitors listed in a watchlist and notify watchlist managers.

7. Click Save.

10.5 | Deleting watchlists in Genetec ClearID

A watchlist manager can delete watchlists that have become obsolete or are no longer required. Or a watchlist might need to be deleted in situations where you need to change a *site watchlist* to a *global watchlist* or vice versa.

Before you begin

Add your watchlists.

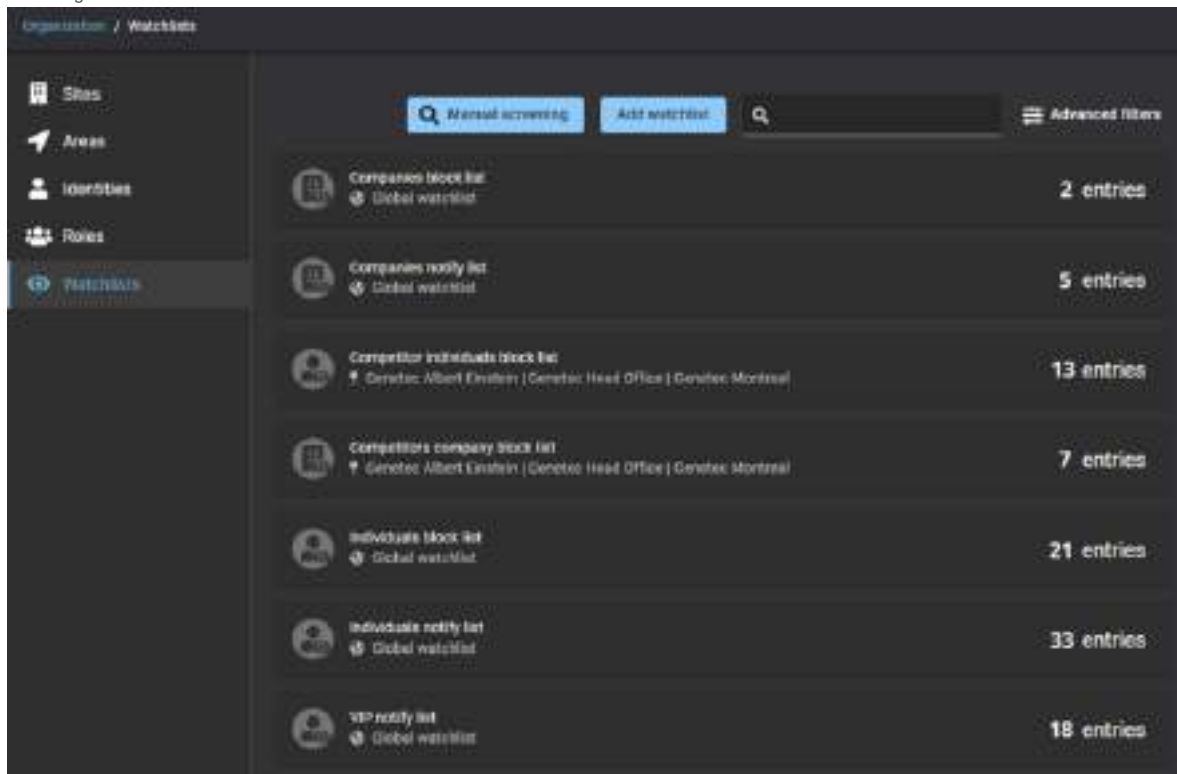
What you should know

A watchlist can only be deleted by the *watchlist manager* who created it.

NOTE: Any watchlist manager or account administrator can delete any watchlist that is configured as a global watchlist.

Procedure

1. Click Organization > Watchlists.



2. (Optional) Use the search box to find a specific watchlist.

3. (Optional) Click Advanced filters to filter the list results by Site or Watchlist type.

Select the filter options that you require:

a. From the Site list, select a site.

b. From the Watchlist types list, select a watchlist type.

4. Select a watchlist from the list.

5. Click Edit watchlist.

6. Verify you have the required watchlist and click Delete watchlist.

Do one of the following:

- a. In the Delete watchlist dialog, click Delete watchlist to confirm the deletion.

- b. (Optional) Click Cancel to abandon the deletion.

10.6 | Screening visitors manually in ClearID

To manually screen a visitor, you can enter the visitor details to check if there is a screening match. For example, testing a new watchlist to find watchlists that contain a person or company of interest, or to validate a new hire against an internal watchlist.

Before you begin

Add your individual watchlist entries.

What you should know

Only *watchlist managers* or account administrators can manually screen visitors for the following:

- Finding watchlists that contain a person of interest.
- Validating a new hire against an internal Individuals watchlist or Companies watchlist.

Screening matches only occur when the following applies:

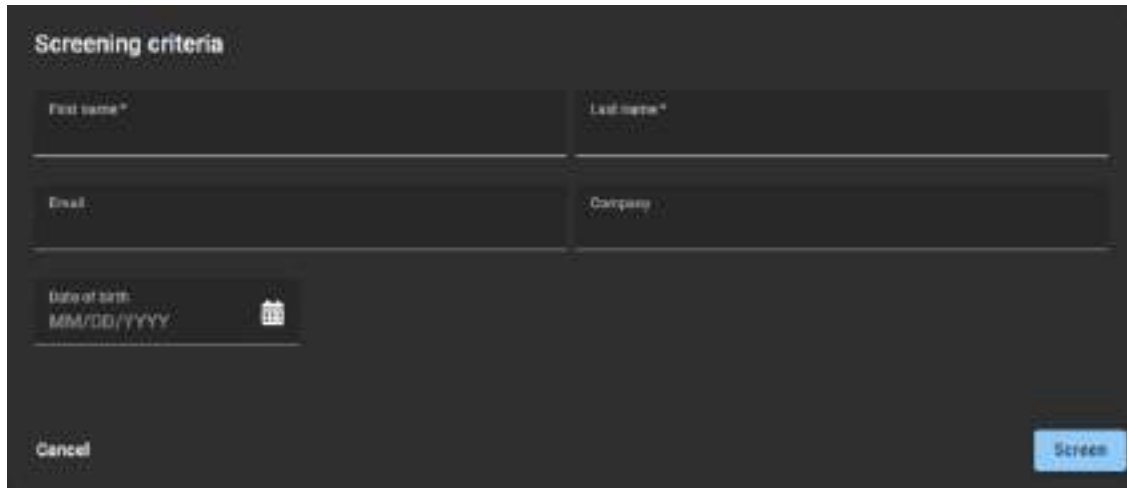
- Individuals: There is a First name and Last name match, First name and Last name alias match, or Email address match.
- Companies: There is a Company name, company domain, or email address domain match.

If *security* or *reception* need to manually screen visitors, the *Watchlist manager* permission must be added to their identity.

Procedure

1. Click Organization > Watchlists.
2. Click Manual screening.
3. In the Screening criteria dialog, complete the details for the visitor that you want to manually screen.

NOTE: Mandatory fields are highlighted by an asterisk (*).



Screening criteria

First name *

Last name *

Email

Company

Date of birth
MM/DD/YYYY

Cancel

Screen

First name

Enter a first name.

Last name

Enter a last name.

Email

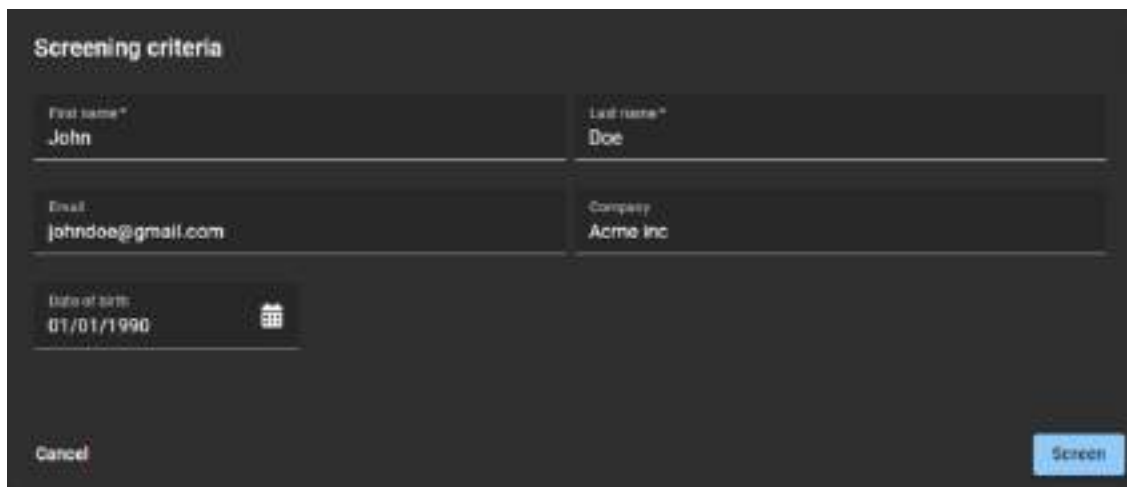
Enter the visitor's email address.

Company

Enter the visitor's company name.

Date of birth

Use the calendar picker to select the visitor's date of birth. The date of birth information is useful additional information when a visitor check-in matches multiple people with the same name. It can be used to validate an identity and also eliminate duplicates or false positive matches.



Screening criteria

First name *

John

Last name *

Doe

Email

johndoe@gmail.com

Company

Acme Inc

Date of birth
01/01/1990

Cancel

Screen

4. Click Screen.

Matching entries for individuals or companies are shown in the *Matching entries* list in the *Screening Criteria dialog*.

Screening criteria

First name *
John

Last name *
Doe

Email
john.doe@gmail.com

Company
Acme inc

Date of birth
01/01/1990

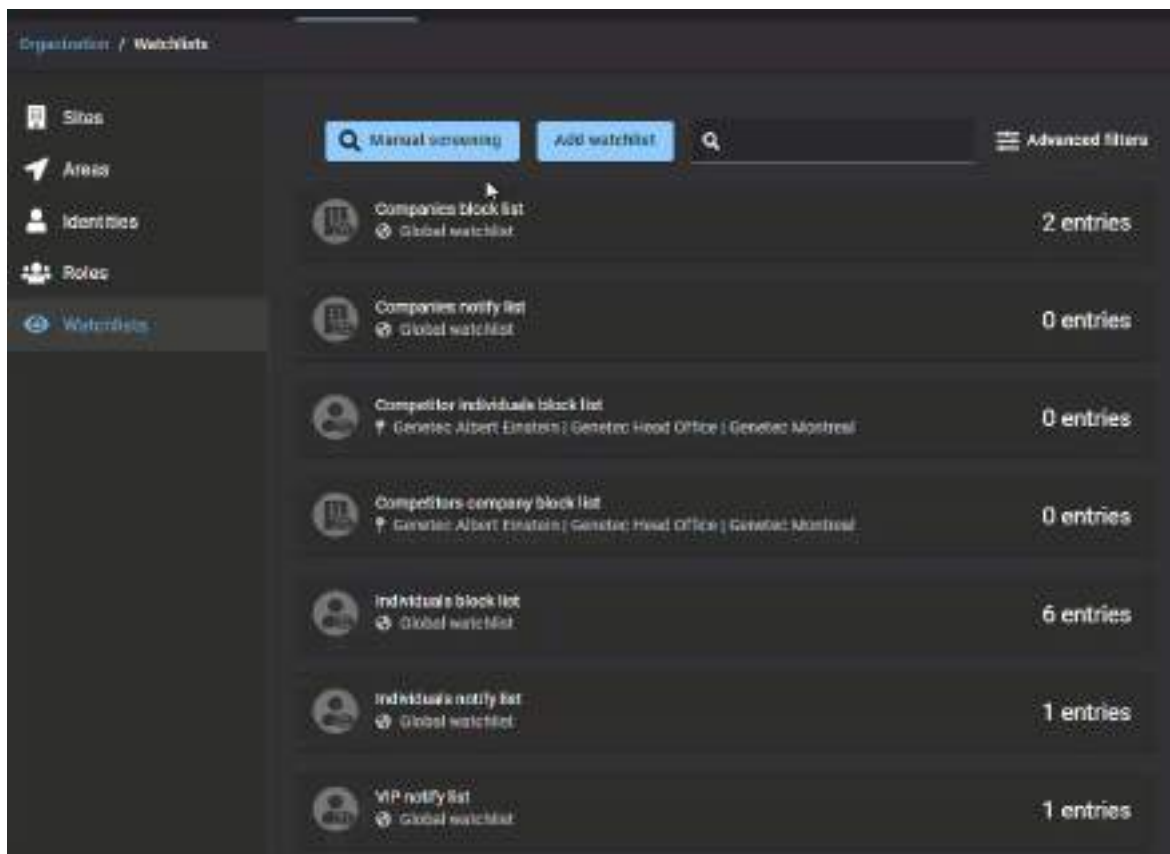
Matching entries (2)

- DOE, John (son, Jonathan, Jonathan)
- Acme inc (some, acme incorporated, Acme inc.)
WWW.ACME.CORP

Cancel Screen

5. (Optional) Click an individual in the Matching entries list to view the complete details of the individuals watchlist entry.
6. (Optional) Click a company in the Matching entries list to view the complete details of the companies watchlist entry.
7. Click Cancel to exit the *Screening Criteria* dialog.

Example



Tip: Click the animation to view full size.

Browse

- Adding watchlist managers in ClearID

10.7 | Unblocking visitors blocked by a watchlist in ClearID

To unblock visitors incorrectly blocked by a watchlist, you can add the visitors email to an always allow list.

Before you begin

Add your individuals watchlist entries.

What you should know

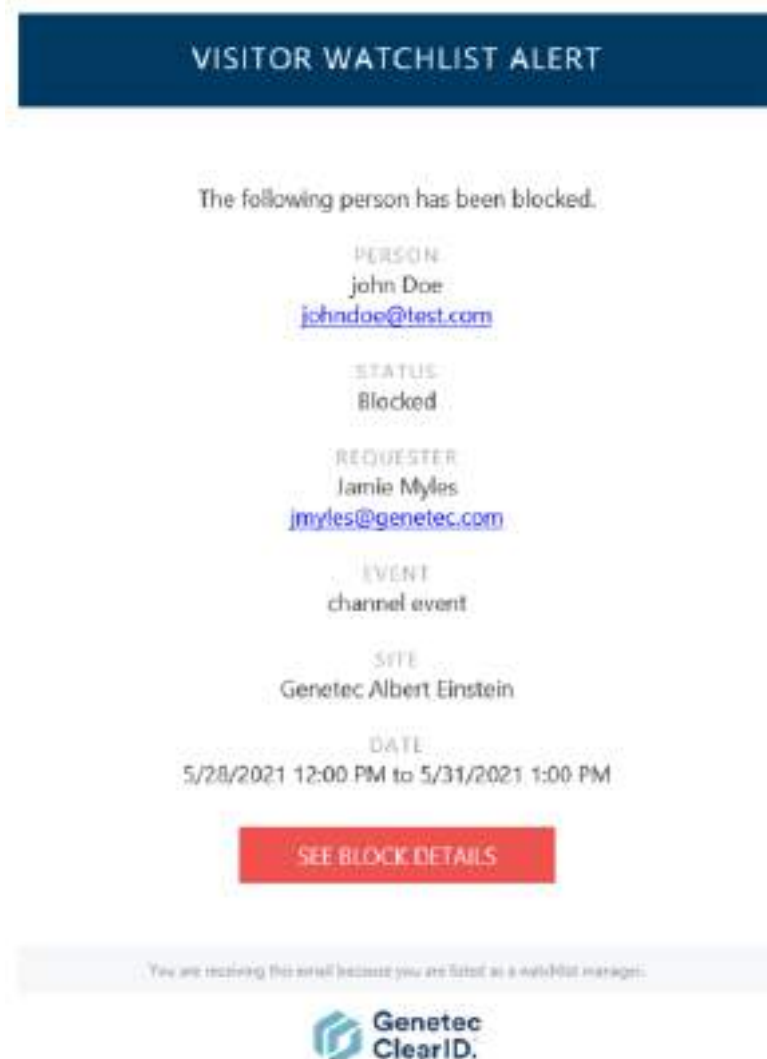
Only a *watchlist manager* or account administrator can unblock a blocked visitor.

- Individuals watchlist email match cannot be set to Always allow.
- Company watchlist entry matches cannot be set to Always allow.
- Notify watchlist entry matches cannot be set to Always allow.

Use this procedure to add any similar emails or false positive email matches for visitors that you might want to allow once or always allow. For example, a possible match that happens to have the same name details, but is a different person with a different email address that should be allowed.

Procedure

1. In your Visitor watchlist alert for <person or company of interest> email, click SEE BLOCK DETAILS.



The visitor watchlist alert dialog opens in the Genetec ClearID™ web portal.

Visitor watchlist alert

Requested by Jamie Myles

Site and areas
Genetec Albert Einstein (America/Toronto)
Main Entrance

Event date and time
From: May 28, 2021 12:00 PM
To: May 31, 2021 1:00 PM

Visitor
First name: John
Last name: Doe
Email: johndoe@test.com
Company:

Hosts + 1 Hosts
Jamie Myles

Matching watchlist entries Always allow all

	DOE, John (Joe, Jonathan, Jonathan) johndoe@test.com	Individuals notify list	John Doe	☐	
	DOE (Do, Dow), John (Jon, Jonathan) johndoe@test.com	Individuals block list	John Doe	☐	

Close **Allow entry**

- In the Matching watchlist entries section, hover over the info icon to see the watchlist entry details that matched this visitor.
- (Optional) Click a matching watchlist entry in the list to open and view the watchlist entry details.

The watchlist entry opens in a new browser tab.

- Choose whether you want to allow entry one time or always allow entry. Do one of the following:
 - If you want to allow entry one time only for this visitor watchlist alert, click Allow entry.
 - If you want to always allow specific future matching entries for this visitor, in the Matching watchlist entries list, move the Always allow slider to the enabled position for each entry you want to always allow, then click Allow entry.
 - If you want to always allow all future matching watchlist entries for this visitor, in the Matching watchlist entries section, move the Always allow all slider to the enabled position, then click Allow entry.

NOTE: Only the slider controls for the watchlist entries that can be set to Always allow will be moved to the enabled position.

- In the Reason field, enter a reason why the blocked visitor was unblocked and allowed to visit.

Visitor watchlist alert

? Requested by: Jamie Myles

Blocked

Site and areas
Genetec Albert Einstein (America/Toronto)
Main Entrance

Event date and time
From: May 28, 2021 12:00 PM
To: May 31, 2021 1:00 PM

Visitor

First name	Last name
John	Doe
Email	Company
johndoe@test.com	

Hosts + 1 Hosts
Jamie Myles

Matching watchlist entries Always allow all

	DOE, John (Jon, Jonathan, Jonathan) johndoe@test.com	Individuals notify list	John Doe		
	DOE (Do, Dow), John (Jon, Jonathan) johndoe@test.com	Individuals block list	John Doe		

Allow reason ✕

Reason:
johndoe@test.com is not the BLOCKED johndoe@competitor.com and should always be allowed.

88 / 300

Confirm

- (Optional) In the Allow reason section, click  to cancel the unblock, then click Close.
- Click Confirm.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

11 | Role-based access control

11.1 | About role-based access control in ClearID

Role-based access control uses identities with various attributes to automatically manage access control. Defining provisioning policies ensures that people in your organization always have up-to-date access permission levels. If an employee changes job title, department, or moves to a different site, the system automatically adjusts their access when their identity attributes are changed.



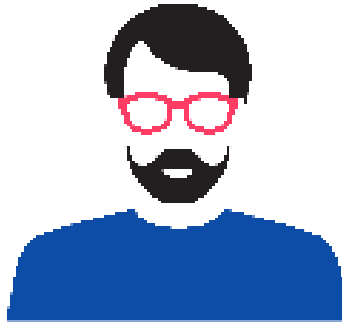
Role-based provisioning policies can be used to automatically assign or revoke access in different situations:

- Grant or revoke access based on employees locations.
- Grant or revoke access based on specific *roles* or job titles in the organization, or who they report to.
- Grant access to a zone only if people have specific training or certifications.
- Grant or revoke access based on a list of custom attributes synchronized from an external source.

NOTE: Many other scenarios might also be possible depending on your requirements and current setup. You can also manually add, modify, or remove access at any time.

What is an identity?

In Genetec ClearID™, an identity represents a person and defines what they can do across various platforms, security systems, business systems, and functions. Each identity has one or more access control badges (credentials) and is linked to a cardholder in Synergis™. For example, these credentials could be a Windows user (Active Directory), an employee (Human Resources and Payroll), a sales person (CRM and Quoting Tool), and a cardholder (Physical Security).



An identity interacts across many security and business systems and functions

A windows user

Microsoft Active Directory

An employee

Employee roles

A cardholder

Physical security

An identity is much more than the profile of a cardholder, it is a unique digital profile. The identity represents a person that either has an access control badge, uses the self-service portal, or both.

NOTE: In ClearID, a visitor or a temporary badge holder is not an identity.

- An identity is a person who has a permanent badge assigned to them.
- A visitor is a person who has a paper badge or a temporary badge credential assigned to them.
- A contractor can be either an identity or a visitor. When a contractor is defined as a visitor, they receive a one-day HID card entered as a visitor in ClearID.

Access is typically permanent for employees, semi-permanent for contractors, and temporary for guests.

Identity attributes

In Genetec ClearID™, attributes are the traits or characteristics that make up an identity. Examples of attributes include department, location, role, seniority, pay grade, training certifications, and security clearance.

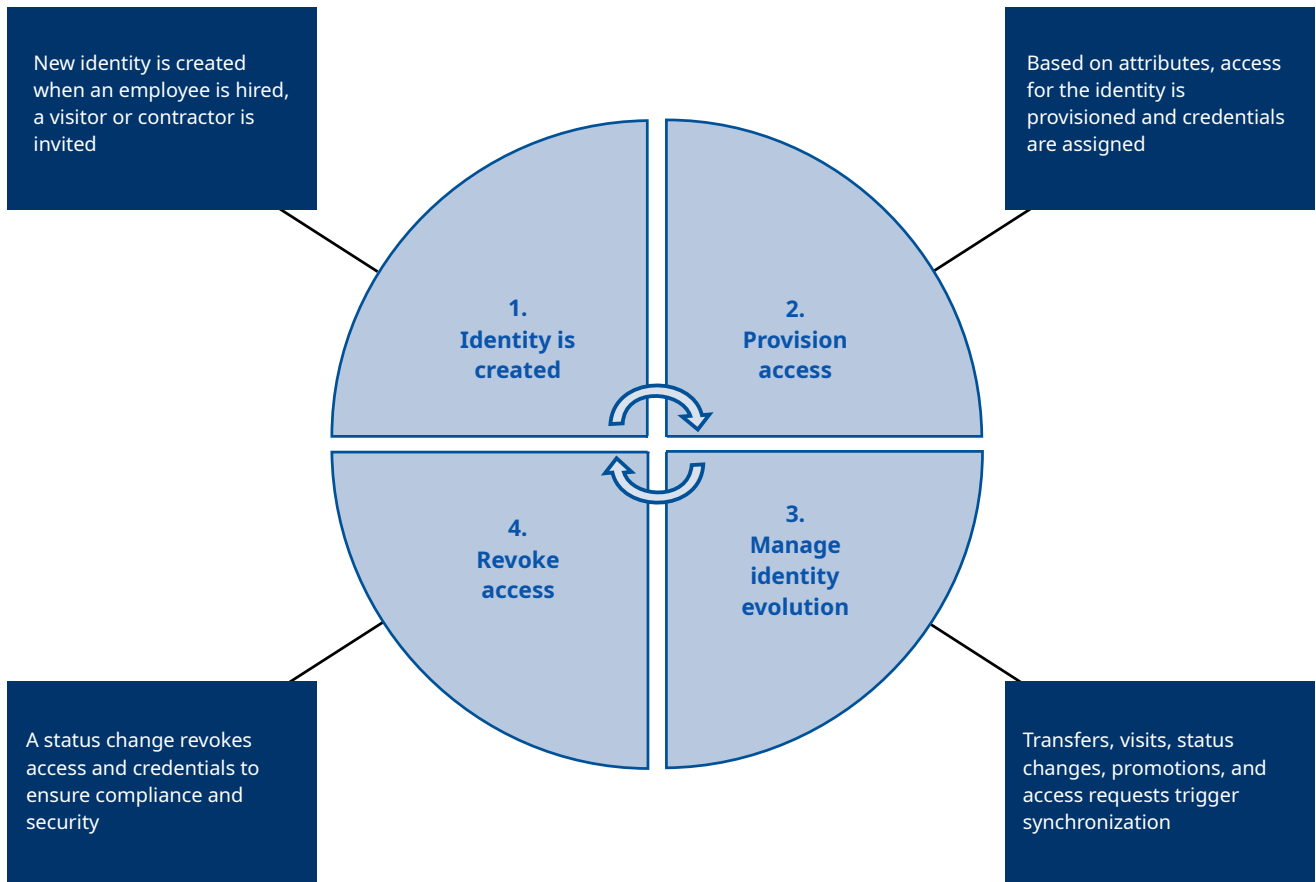
Role based access control relies on policies (*provisioning rules*) that automatically assign rights to identities (people) based on attributes (traits or characteristics).

In Genetec ClearID™, a role manager is an identity that has authority over who is assigned to a role. A role manager can add people to and remove people from a role. They are also responsible for role access review approvals.

The life cycle of an identity

In ClearID, the entire life cycle of an identity can be automatically managed.

The following diagram illustrates the life cycle of an identity when a provisioning policy is activated:



11.2 | Adding roles in ClearID

Before you can configure your role-based automatic access control policies, you must define your roles.

Before you begin

Familiarise yourself with role-based access control.

What you should know

In Genetec ClearID™, a role is a group of people who are assigned the same access. A person can be assigned multiple roles. Roles are linked to cardholder groups in Synergis™. A role manager controls who is granted access to the group.

- Only account administrators can add roles.
- Consider creating roles for each department, group, or job title in your organization. For example, you might create roles for HR, IT, marketing, developer teams, payroll, contractors, and so on.

Procedure

1. From the homepage, click Organization > Roles.
2. Click Add role.
3. In the General section, complete the fields.
 - a. Enter a name for the role.
 - b. Enter a meaningful description.
 - c. Add any internal notes.

NOTE: The internal notes field is used to store special instructions or details only visible to the account administrator, role owner, and role manager. Other users of the system cannot view internal notes. For example, the internal notes field could contain the following:

Only permanent employees based in Montreal should be in this role. Discuss with security before adding employees to this role.

4. (Optional) In the Notifications section, Select the notifications options that you require.

The screenshot shows the 'General' tab for a role named 'Information Technology'. The breadcrumb navigation at the top reads 'Organization / Roles / Information Technology'. On the left sidebar, there are links for 'General', 'Managers', 'Members', and 'Provisioning policy'. The main content area has a 'Save role' button in the top right corner. The 'General' section contains three fields: 'Name' (Information Technology), 'Description' (IT department), and 'Internal roles' (N/A). Below this is a 'Notifications' section with a description: 'Send an email notification to the associated role members and their supervisors, role owners, and role managers when:'. There are two checkboxes: 'Role members are manually added' and 'Role members are manually removed', both of which are currently unchecked.

5. Click Save.

Example



After you finish

Configure your role-based access control policies.
Browse

- [Viewing a role activity report in ClearID](#)

11.3 | Configuring role managers in ClearID

Role managers are composed of two distinct roles: role owners and role managers. Before you can define policies for a role or add or remove identities from a role, you must assign one or more employees as role managers.

Before you begin

[Add your roles.](#)

What you should know

- Only role owners can configure role managers.

Procedure

1. From the Home page, click Organization > Roles and select a Role.
2. Click Managers to configure role manager settings.
 - a. Use the search field to find existing managers, or click Add (+).
 - b. Select the required user or users and click Confirm.
3. Choose the Role type for the user or users you just added from the following:

Manager

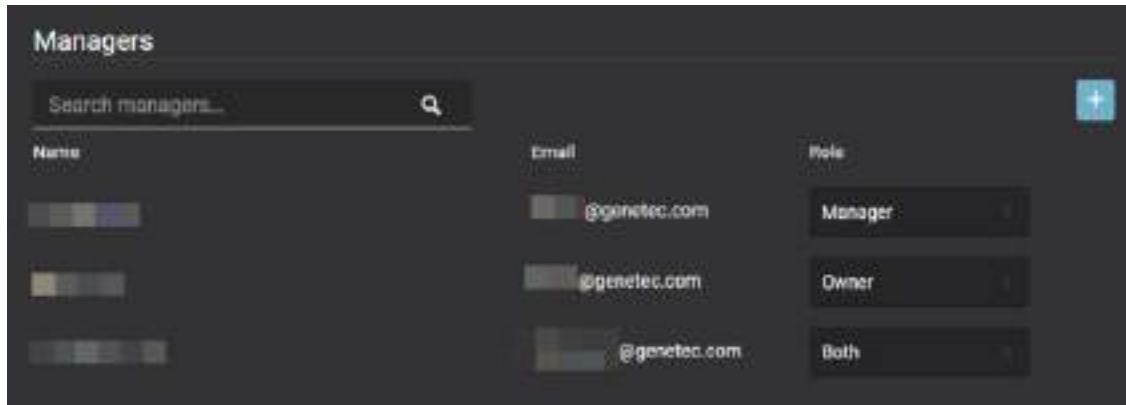
A role manager is an identity that has authority over who is assigned to a role. A role manager can add people to and remove people from a role.

Owner

A role owner is responsible for assigning role managers and configuring role-based policies.

Both

Use when one person is responsible for managing roles, assigning role managers, and configuring policies.



4. (Optional) To remove any managers that you no longer require, hover over a name and click ✖.
5. Click Save.

Results

The selected people are added to the list as either a manager, an owner, or both.

After you finish

Add role members.

Browse

- Viewing a role activity report in ClearID

11.4 | Configuring role-based access control policies in ClearID

To ensure that people in your organization always have up-to-date access permission levels, you can define provisioning policies that automatically assign people to specific roles based on their identity attributes. If an employee changes job title, department, or moves to a different site, the system automatically adjusts their access.

Before you begin

- Add your roles.

What you should know

- Only account administrators, or role owners can create or modify provisioning policies that automatically associate people with a specific role.
- A maximum of 25 policies with a maximum of 25 policy conditions can be defined for each role.

Procedure

1. From the Home page, click Organization > Roles and select a Role.
2. Click Provisioning policy and click or slide the toggle to Active.
3. In the Description field, enter a meaningful policy description.
4. (Optional) Configure your automatic removal settings for role members:



- a. Select the Automatically remove members that no longer match checkbox option.
- b. Specify when to automatically remove your role members. Choose one of the following:
 - o After a specified number of days. The default is 7 days.
 - o Immediately.

For example, an IT role with access to server rooms. When an IT role member moves to a Developer job, they might still require access to server rooms for 7 days for support or skill transfer purposes. Role members are removed when their identity settings no longer match the policy settings for role-based access control.

5. Add the policy rules for the role that you are configuring.

- a. Select the Property type that you require.

The property types listed here are the default identity field attributes that can be found in the General details of any identity.

NOTE: Only roles that you are a role manager for can be selected.

Company

Enter the company name.

Country

Select a country from the list.

Department

Enter a department name.

Description

Enter a description.

Extended grant time

Used to select True or False.

External ID

Enter an external ID

Job title

Enter a job title.

Primary site

Enter or select the primary office location.

Provisioning attributes

Type a custom provisioning attribute and press enter. Some examples might include: background check, drug and alcohol tests, NDA, Safety training, site induction training, and so on.

Status

Choose either Active or Inactive.

Supervisor name

Enter a name.

Supervisors

Add multiple supervisors.

Worker type code

Enter a worker type code

Worker type description

Enter a meaningful description for the worker type.

- b. Select an Operator from the following:

Genetec ClearID™ User Guide

Displayed in the header

- o Contains
- o Does not contain
- o Is
- o Is not

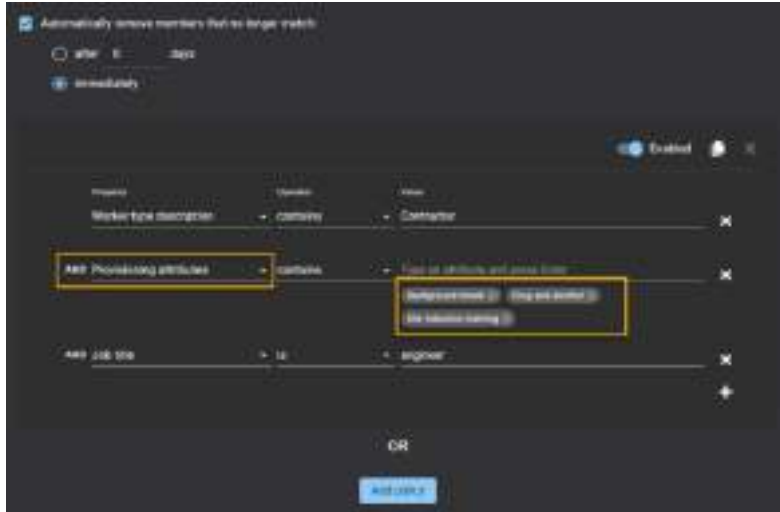
NOTE: The Operators that are displayed vary depending on the Property type that you select.

- a. Enter a value or select an option that relates to the Property type you selected.

NOTE: The Value options or fields that are displayed vary depending on the Property type that you select.

6. (Optional) Add custom provisioning attributes to your provisioning policy.

- a. Select the Provisioning attributes property.
- b. Select an Operator from the following:
 - Contains
 - Does not contain
- c. Enter the custom attribute values that you require.



NOTE: For custom attributes, the provisioning policy is only triggered when an identity includes as a minimum all the provisioning attribute values specified in this policy.

7. (Optional) To temporarily disable a policy rule, set the Enabled slider to Disabled.
8. (Optional) Click Copy policy (📋) when you want to copy a rule or set of rules.
9. (Optional) Click ✕ to remove any policy rules that you no longer require.
10. Click Save.

Results

Users can now be automatically assigned to or removed from specific roles based on their identity attributes.

Example



After you finish

Add role managers.
Browse

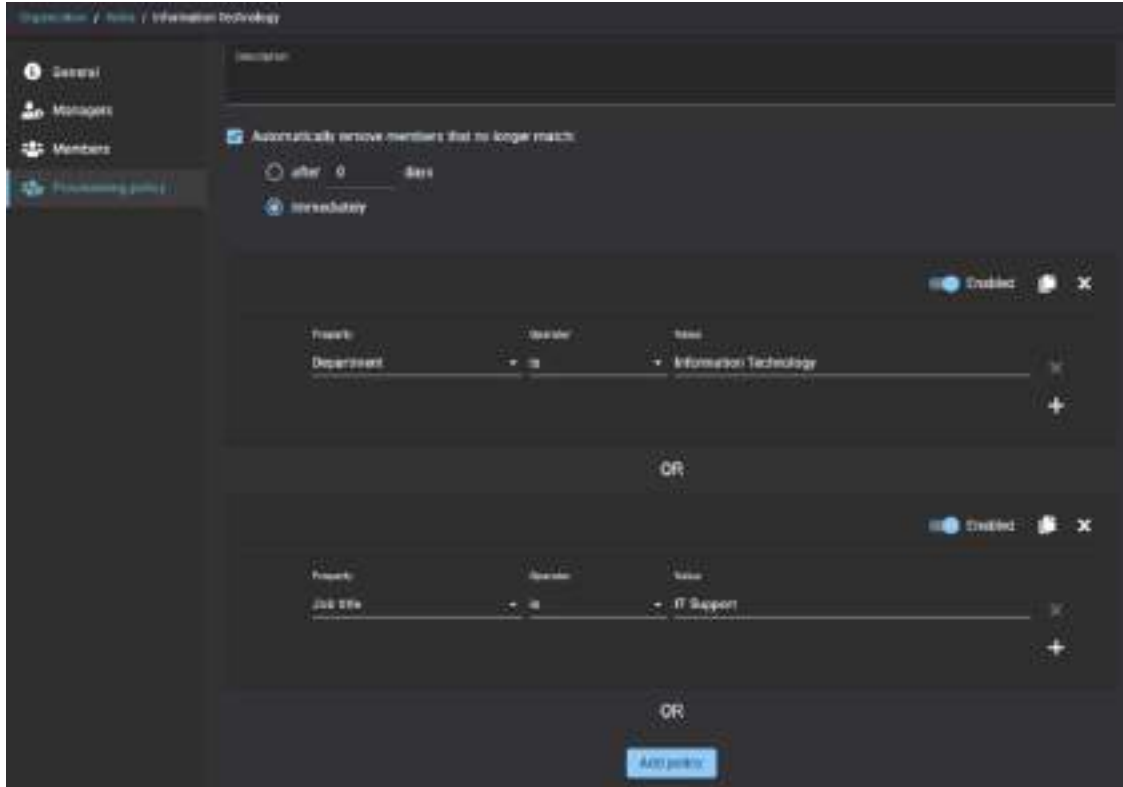
- Adding roles in ClearID
- Identity fields in ClearID

11.4.1 | Scenario 1: Adding employees to an IT role in ClearID

In this example, a policy is used to automatically assign employees to an IT role based on their identity attributes.

The following example shows a policy configured to automatically add employees to an Information Technology role if the following policy rule criteria are met:

- Department is Information Technology
- Job title is IT Support.



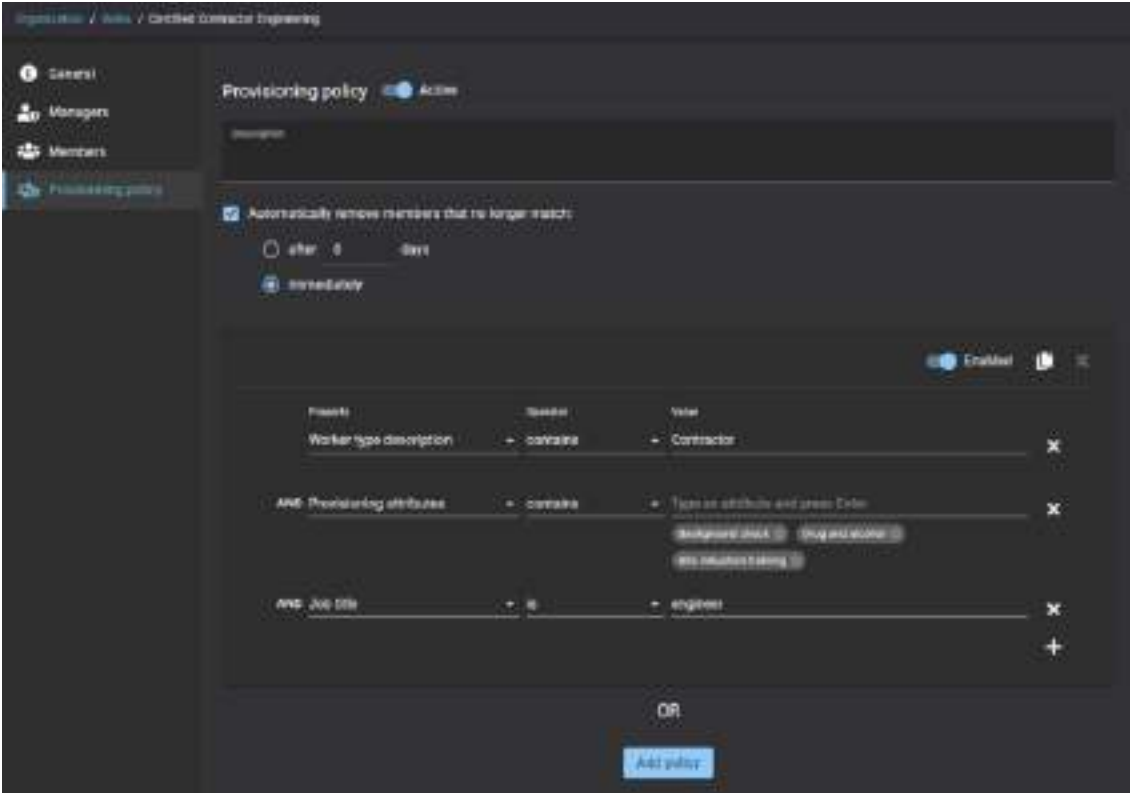
Parent topic: [Configuring role-based access control policies in ClearID](#)

11.4.2 | Scenario 2: Adding contractors to a certified contractor engineering role in ClearID

In this example, a policy is used to automatically assign contractors to a certified contractor engineering role based on their identity attributes.

The following example shows a policy configured using custom attributes to automatically add contractors to a certified contractor engineering role if the following policy rule criteria are met:

- Identity contains worker type contractor
- Provisioning attributes are found
- Their job title is engineer.

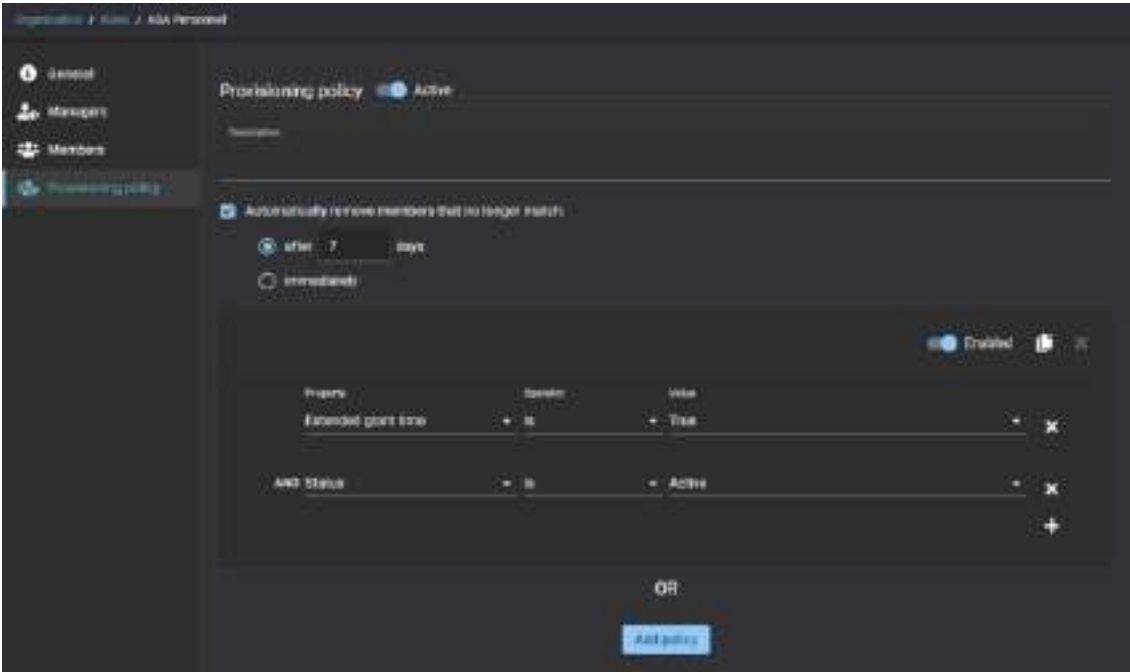


Parent topic: Configuring role-based access control policies in ClearID

11.4.3 | Scenario 3: Adding employees to an ADA personnel role in ClearID

In this example, a policy is used to automatically assign employees that require accessibility assistance to an ADA personnel role based on their identity attributes. The following example shows a policy configured to automatically add employees to an ADA personnel role if the following policy rule criteria are met:

- The extended grant time property is found.
- Their status is active.



Parent topic: Configuring role-based access control policies in ClearID

11.5 | Adding custom provisioning attributes to an identity in ClearID

When the default Genetec ClearID™ policy attributes do not meet your needs, you can manually assign custom provisioning attributes to an employee's identity record. These attributes can then be used in a role-based access control policy.

Before you begin

- Add your roles.

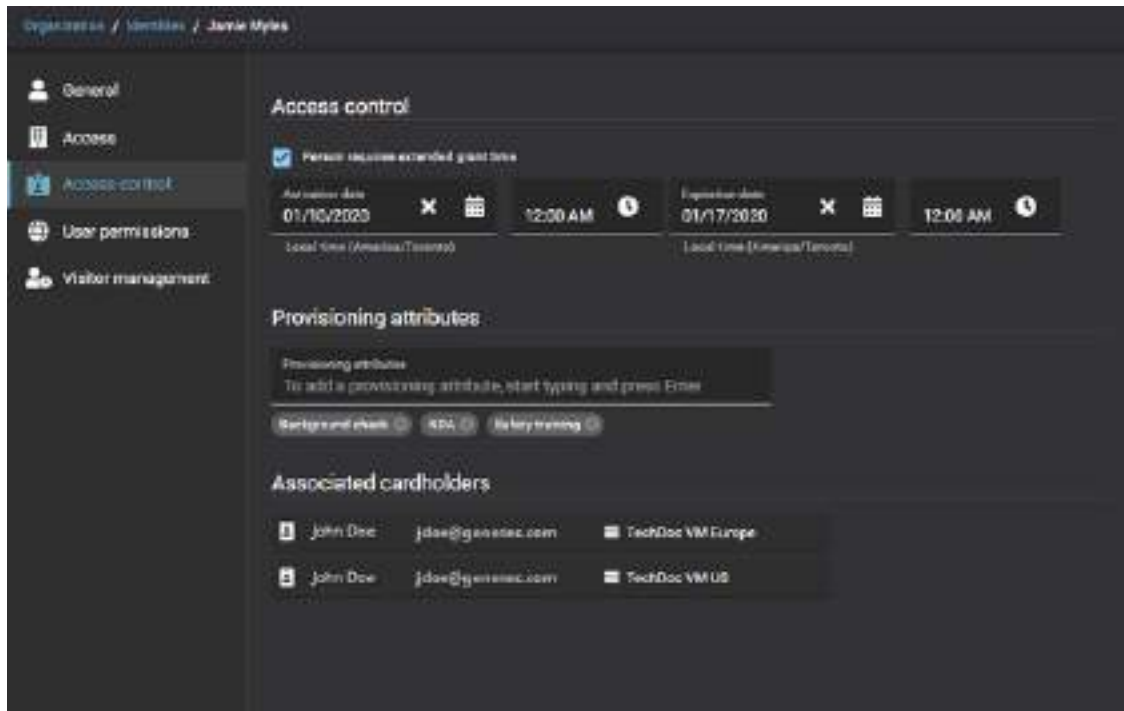
What you should know

- Only account administrators can add custom attributes.
- Custom attributes are typically used when you import or synchronize your attributes from an external source.
- The current status of custom attributes can be managed using an integration, and any that become obsolete are removed automatically.
- Custom attributes can also be added or removed manually.

Some example custom provisioning attributes might include: background checks, drug and alcohol tests, NDA, safety training, site induction training, and so on.

Procedure

1. From the Home page, click Organization > Identities and select an identity.
2. Click Access control.
3. In the Provisioning attributes section, start typing and press enter to add your custom attributes.
4. (Optional) Add additional custom attributes if required.
5. (Optional) Click  to remove any attributes that have expired or are no longer applicable.
6. Click Save.



11.6 | Adding role members in ClearID

To add role members who do not fit the default role-based provisioning policy criteria, you must add them manually.

Before you begin

Add role managers.

What you should know

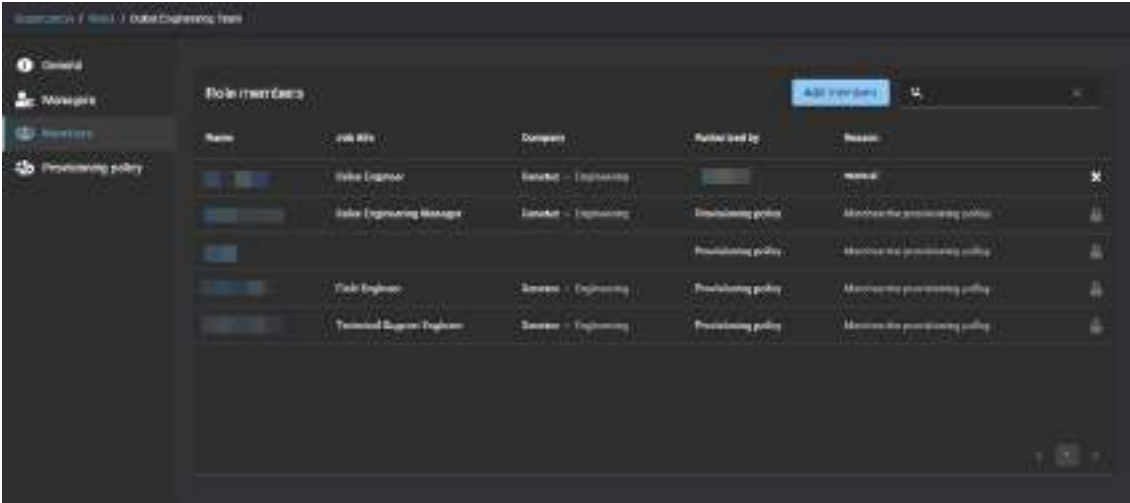
- Only role managers can add role members.
- When a provisioning policy is enabled, role members are added automatically based on rules defined in the policy. Role members that are automatically added are shown in Authorized by column as Provisioning policy.
- Role members can also be added manually. Role members that are manually added are shown in the Authorized by column as Manual.
- Role members that match a provisioning policy are locked and cannot be removed.
- Role members that no longer match a provisioning policy are immediately unlocked. They are automatically removed after the period specified in a provisioning policy.

Procedure

1. From the Home page, click Organization > Roles and select a role.
2. Click Members to configure the list of role members.
3. Click Add members.
4. Search for or select one or more members.
5. Enter a reason and click Add.

The following example shows the Dubai Engineering Team role members.

NOTE: The Authorized by column shows four members that were added automatically (Provisioning policy) and one that was added manually (Manual).



Tip: You can click the blue text in the Name column to view or modify the identity details.

6. (Optional) To immediately remove any role members who no longer meet the policy criteria, or role members that were added manually, click  then click Remove.

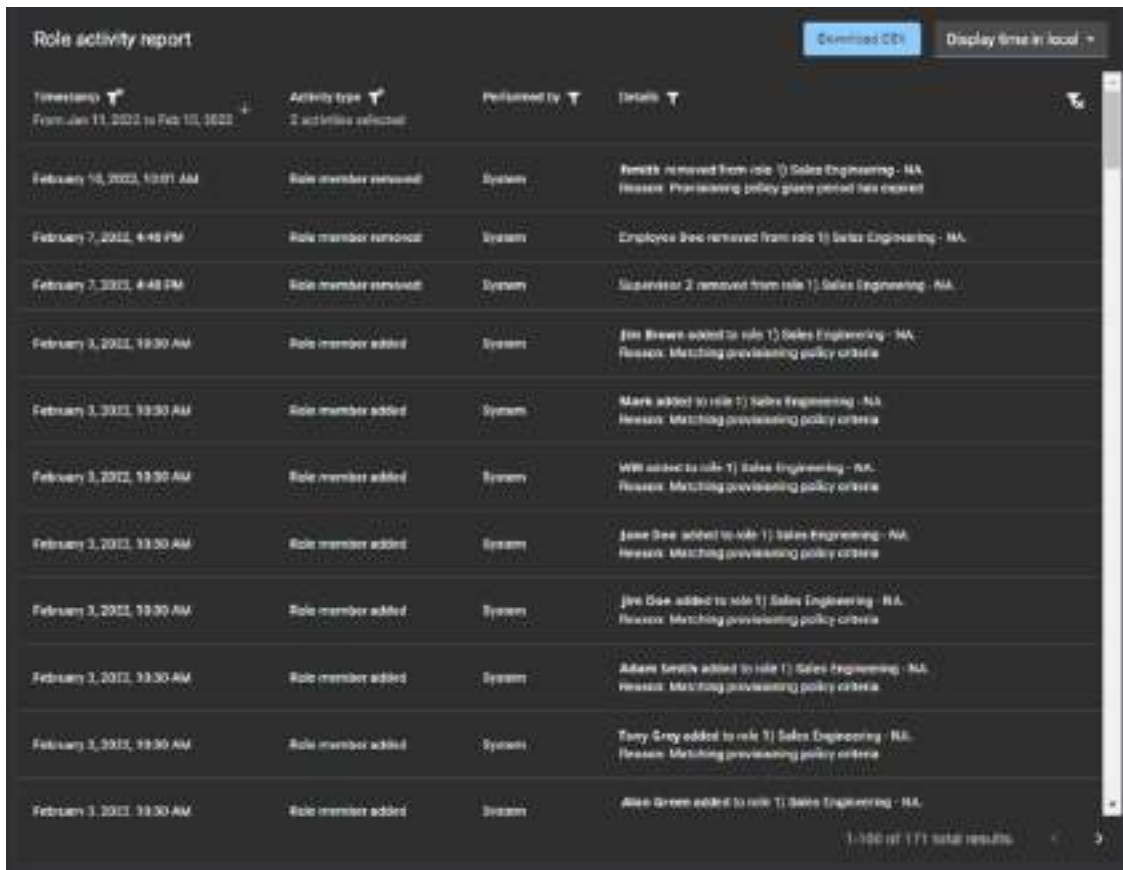
Browse

- Viewing a role activity report in ClearID

11.7 | About role activity report in ClearID

In Genetec ClearID™, a role activity report is an audit trail of all activities related to roles. The report includes timestamp information, activity type, who activity was performed by, and a details section including reason information.

Role activity report



Timestamp	Activity type	Performed by	Details
From Jan 11, 2022, to Feb 10, 2022	2 activities selected		
February 10, 2022, 10:01 AM	Role member removed	System	Breath removed from role 1) Sales Engineering - NA. Reason: Provisioning policy grace period has expired
February 7, 2022, 4:48 PM	Role member removed	System	Employee Doc removed from role 1) Sales Engineering - NA.
February 7, 2022, 4:48 PM	Role member removed	System	Supervisor 2 removed from role 1) Sales Engineering - NA.
February 3, 2022, 10:30 AM	Role member added	System	Jim Brown added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Mark added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Will added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	June Doe added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Jim Doe added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Adam Smith added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Tony Gray added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Alice Green added to role 1) Sales Engineering - NA.

1-100 of 171 total results

The role activity report is used by account administrators to review all activities related to roles. When the report is used by role managers or role owners, only the activity for their roles is shown. For example, role access granted or removed, role manager added or removed, role owner added or removed, and role member added or removed.

Filters can be used to help refine the report search results by timestamp, activity type, performed by, and details.

Browse

- [Viewing a role activity report in ClearID](#)

11.8 | Viewing a role activity report in ClearID

As an *Account administrator*, *Role manager*, or *Role owner*, you can view an audit trail of role-related activities such as timestamp information, activity type, who performed the activity, and more.

Before you begin

You must be an *Account administrator*, *Role manager*, or *Role owner* to view a Role activity report and review audit trail information for role-related activities.

Procedure

1. From the Home page, click Organization > Roles.
2. Search for or select the role that you require from the Name column.
3. Click Role activity.
4. From the Display time menu, select the required display time format.

Display time in local

Report times are displayed using the system time from the computer of the logged-in user.

Display time in UTC

Report times are displayed using Coordinated Universal Time (UTC).

5. Filter the report based on your required criteria:

Role activity report			
Timestamp 		Activity type 	Performed by 
From: Jan 11, 2022 to Feb 10, 2022 		Details 	
		2 activities selected	
February 10, 2022, 10:01 AM	Role member removed	System	Remith removed from role 1) Sales Engineering - NA. Reason: Provisioning policy grace period has expired
February 7, 2022, 4:48 PM	Role member removed	System	Employee Blec removed from role 1) Sales Engineering - NA.
February 7, 2022, 4:48 PM	Role member removed	System	Supervisor 2 removed from role 1) Sales Engineering - NA.
February 3, 2022, 10:30 AM	Role member added	System	Jim Brown added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Mark added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Will added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Jose Blec added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Jim Doe added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Adam Smith added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Tony Gray added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Alan Green added to role 1) Sales Engineering - NA.
1/100 of 171 total results			

Timestamp

In the Timestamp column, click  to filter the results by date. Select a pre-defined date range from the choices available or enter a specific date range using the date range picker.

☐ Last 24 hours
 ☐ Last 7 days
 ☐ Last 30 days
 ☐ Last 90 days
 ☐ Last 365 days

☒ Date range (UTC)

From *
10/21/2021

To *
10/22/2021

From *
6:25 PM

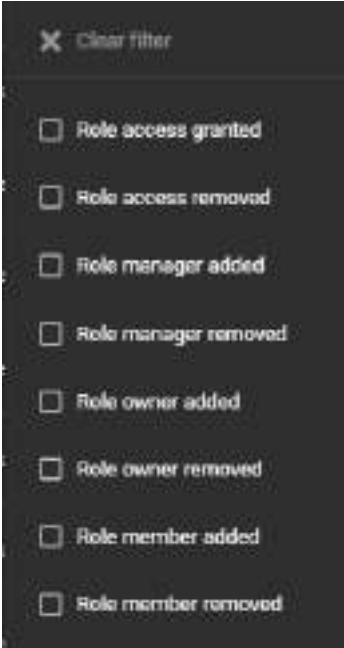
To *
6:25 PM

Time period limited to a maximum of one year

(Optional) Use the sort icons ( and ) to display the results in descending or ascending order.

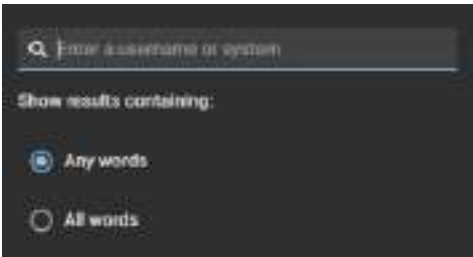
Activity type

(Optional) Use the sort icons  and  to display the results in descending or ascending order.



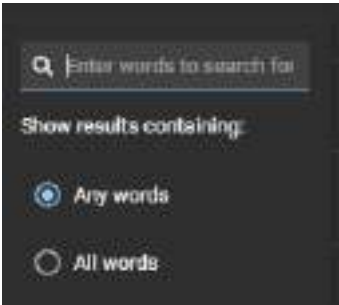
Performed by

In the Performed by column, click  to open a search dialog and filter the results by who performed an activity. For example, tasks performed by a particular user, or tasks performed automatically by the system.



Details

In the Details column, click  to open a search dialog to search the details or reason using a search criteria.



(Optional)

Click  to reset filter selections.

6. Click Download CSV, to download a copy of the role activity report in CSV format. The report can then be used for auditing purposes, to keep a physical copy, to attach to an audit request, to review offline, or to manipulate or consolidate data in a spreadsheet for other audiences.
 - a. Follow your browser prompts to complete downloading the exported file.

The file is exported as a .CSV file to the default download location for your browser. By default the exported file is created using the name of your site. For example, RoleActivity_rolename_fromdate_to_todate_SiteActivityReport.csv (RoleActivity_All active contracotrs_2024-09-23.csv).

NOTE: The columns and entries in the CSV file can vary depending on the filters you've selected when you download the report.

Browse

- About role activity report in ClearID
- Adding role members in ClearID
- Configuring role managers in ClearID
- Adding roles in ClearID

12 | Connecting to other systems

12.1 | Authenticating your connection with ClearID

Before you can connect with Genetec ClearID™ to synchronize data or issue API commands, you must first authenticate your applications (or API environment) so that your applications or API can communicate with ClearID.

What you should know

Use the API integration key to authenticate your applications when making requests to your ClearID account.

- The OAUTH 2.0 protocol is used to authenticate non-user system communications or connections with ClearID.
- Store your key securely and don't share it.

IMPORTANT: When you regenerate your key, you must update any applications that access this account to use the new key.

You can create an API integration to authenticate communications for the following:

- Genetec ClearID™ API
- System for Cross-domain Identity Management (SCIM) integration
- Genetec ClearID™ One Identity Synchronization Tool (Azure AD, Database, File)
- Genetec ClearID™ LDAP Synchronization Agent

Procedure

1. Add an API integration.
 - a. In ClearID, click Administration > API integrations.
 - b. Click Add API integration.

Name
Enter a name for the API integration. For example, Active Directory LDAP Synchronization, API user connection, or One Identity Synchronization.
Description
Enter a meaningful description for the API integration.
 - c. Click Save.
2. Select a user from the API integration list.
 - a. Click Generate key and then click Confirm, to generate the authentication key for your API integration.

CAUTION:
The current API integration key immediately becomes invalid and isn't recoverable.
 - b. Click Download authentication key.

Tip: Make a note of the downloaded file location for later use.

By default, the authentication key for your API integration is named key-systemID-APIintegrationname.json.

Results

You're now ready to configure your applications to synchronize data or issue API commands.

Example



After you finish

Depending on how attributes are set up in your organization, do one of the following:

- Synchronize identity attributes using REST API commands.
- Synchronize identity attributes using the SCIM integration.
- Synchronize identity attributes using One Identity (Azure AD, Database, File).
- Synchronize identity attributes using LDAP.

Browse

- [About ClearID information security](#)
- [Logging on to ClearID](#)

12.2 | Setting up data synchronization

Setting up data synchronization in Genetec ClearID™ involves learning some concepts, configuring the synchronization solution for your identity data, and the webhook integration options that are relevant for your organization.

1. Review the firewall port requirements.
2. Sign in to ClearID.
3. Grant access to the web portal.
4. Authenticate your non-user system connections to synchronize data or issue API commands.
5. Choose a synchronization solution for your identity data:
 - Synchronize identity attributes using the ClearID API:
 - Synchronize identities using an API.
 - [Learn about the ClearID API.](#)
 - Synchronize identity attributes using the ClearID SCIM integration:
 - Synchronize identities using the SCIM Integration.
 - [Learn about the SCIM standard.](#)
 - [Learn about Microsoft Entra ID attribute fields.](#)
 - [Configure the ClearID SCIM integration.](#)
 - [Generate a SCIM key.](#)
 - [Create a Microsoft Azure enterprise application.](#)
 - [Connect your ClearID SCIM integration to Microsoft Azure.](#)
 - [Disable your Microsoft Entra ID groups setting.](#)
 - [Configure your Microsoft Entra ID user settings.](#)
 - [Configure your ClearID SCIM integration synchronization settings.](#)
 - (Optional) [Reset your ClearID SCIM integration identity data.](#)
 - [Review the ClearID SCIM integration synchronization status.](#)
 - Synchronize identity attributes using the ClearID One Identity Synchronization Tool:
 - Synchronize identities using the One Identity Synchronization Tool.
 - [Learn about the One Identity Synchronization Tool.](#)
 - [Learn about the One Identity Synchronization Tool Attribute fields.](#)
 - [Learn about the Azure web app.](#)
 - [Install the One Identity Synchronization Tool.](#)
 - [Configure the One Identity Synchronization Tool.](#)
 - [Review your synchronization status.](#)
 - [Learn about One Identity Synchronization Tool logs.](#)
 - [View the One Identity Synchronization Tool logs.](#)
 - [Update existing identities from an external data source.](#)
 - Synchronize identity attributes using the ClearID LDAP Synchronization Agent:
 - [Learn about the ClearID LDAP Synchronization agent.](#)
 - [Learn about LDAP attributes to ClearID attribute mapping.](#)
 - [Configure the ClearID LDAP Synchronization Agent.](#)
6. Configure and manage your webhook integrations:
 - [Learn about webhooks.](#)
 - [Create your webhooks.](#)
 - [Modify your webhooks.](#)
 - [View the webhook logs.](#)
7. (Optional) Troubleshooting information.
 - a. [One Identity Synchronization Tool: Connectivity issues](#)
 - b. [One Identity Synchronization Tool: Data Synchronization issues](#)

12.3 | Synchronizing identities using an API in ClearID

Use the Genetec ClearID™ API to code your own solutions to automate various functions in ClearID. The primary use for the REST API is synchronizing identities, however many other scenarios are also possible.

12.3.1 | About the ClearID API

The Genetec ClearID™ API is an Application Programming Interface that developers can use to help customers and partners integrate additional software or perform custom functions.

For more information about automating functions using the ClearID REST API, see the [Genetec™ Developer](#) documentation.

Parent topic: [Synchronizing identities using an API in ClearID](#)

12.4 | Synchronizing identities using the SCIM integration in ClearID

To synchronize external system attributes from a supported identity provider into Genetec ClearID™ identity attributes, you can use the System for Cross-domain Identity Management (SCIM) integration. These identity attributes can then be used in ClearID to assign people to roles and automate role-based access control.

What you should know

Only Microsoft Entra ID is currently supported. If you want to integrate another supported identity provider, contact your deployment representative.

Procedure

- 1. Learn about the SCIM standard.
- 2. Learn about Microsoft Entra ID attribute fields.
- 3. Configure the SCIM integration.
- 4. (Optional) Reset the SCIM integration identity data.
- 5. Review SCIM integration synchronization status.

12.4.1 | About the SCIM standard in ClearID

The System for Cross-domain Identity Management (SCIM) standard is an open-standard protocol for exchanging identity information between entities. It's widely used to automate the process of managing user identities in IT systems. The SCIM integration ensures that any changes are automatically synchronized to other systems when identity attributes change.

System

SCIM creates a common format for how identity data is exchanged.

Cross-domain

SCIM securely communicates identity data across platforms.

Identity management

SCIM automates the flow of information between an identity provider or [identity and access management \(IAM\) system](#) and cloud-based applications.

Benefits

- Using SCIM reduces the effort that it takes to create, modify, and synchronize identity data.
- Because the SCIM integration uses Microsoft Entra ID in the cloud, there's no machine or infrastructure to manage.
- There are no firewall ports to configure.

NOTE: The SCIM integration only synchronizes the identity attributes that have changed. This approach results in a significant reduction in throughput and processing overheads. Other solutions typically synchronize all identity attributes at a specified time to get all the latest identity data.

Parent topic: [Synchronizing identities using the SCIM integration in ClearID](#)

12.4.2 | About Microsoft Entra ID attribute fields in Microsoft Azure

When you synchronize an external system with Genetec ClearID™ using the System for Cross-domain Identity Management (SCIM) standard, your external system attributes are imported into ClearID identity attributes. The import uses the field mappings in Microsoft Entra ID.

Most of the ClearID identity fields are created as custom attributes.

You must prefix each field with: `urn:ietf:params:scim:schemas:extension:clearid:2.0:User`

Identity attributes	
Attribute fields	Notes

Genetec ClearID®; User Guide

Displayed in the header

Attribute fields	Notes
Basic fields: active username displayName	- These basic fields are the only fields that we use from the SCIM base schema. - displayName is required in the mapping.
Base identity fields: urn:ietf:params:scim:schemas:extension:clearid:2.0:User:description urn:ietf:params:scim:schemas:extension:clearid:2.0:User:firstName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:lastName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:middleName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:countryCode urn:ietf:params:scim:schemas:extension:clearid:2.0:User:email	- firstName or lastName must be supplied in the mapping (the same as in the portal identity form). - email must be a valid email format to be created in the identity properly. - countryCode must be a 3-letter code. It's best to use a constant value from Microsoft Entra ID for now.
CompanyData fields: urn:ietf:params:scim:schemas:extension:clearid:2.0:User:employeeNumber urn:ietf:params:scim:schemas:extension:clearid:2.0:User:secondaryEmail urn:ietf:params:scim:schemas:extension:clearid:2.0:User:cityOfResidence urn:ietf:params:scim:schemas:extension:clearid:2.0:User:stateOfResidence urn:ietf:params:scim:schemas:extension:clearid:2.0:User:zipCode urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberPrimary urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberSecondary	secondaryEmail must be a valid email format to be created in the identity properly.
PrivateData fields: urn:ietf:params:scim:schemas:extension:clearid:2.0:User:supervisorName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:departmentName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:jobTitle urn:ietf:params:scim:schemas:extension:clearid:2.0:User:companyName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeDescription urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeCode	
SystemData fields: urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasExtendedTime urn:ietf:params:scim:schemas:extension:clearid:2.0:User:externalId	- Boolean fields only work with the SCIM 2.0 feature flag. - externalId is required and needs to be unique. This value is used to manage the creation of identities (same way in Onelidentity). The easiest way to use this value is to map with an email or username.
Other custom fields: (that aren't directly part of the identity model) urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasWebPortalAccess urn:ietf:params:scim:schemas:extension:clearid:2.0:User:isAdmin	Boolean fields only work with the SCIM 2.0 feature flag.

Attribute fields that are not supported

Date fields:

- birthday
- activationDateUtc
- expirationDateUtc
- externalSyncTimeUtc

Fields with ids (reference to identityIds):

- creationOnBehalf
- approvers
- siteId
- provisioningAttributes
- customFields

Parent topic: [Synchronizing identities using the SCIM integration in ClearID](#)

12.4.3 | Configuring the SCIM integration in ClearID

Before you can synchronize an external system with Genetec ClearID™, you must first configure the System for Cross-domain Identity Management (SCIM) integration in ClearID and Microsoft Azure.

Before you begin

- [Learn about the SCIM standard.](#)
- [Learn about Microsoft Entra ID attribute fields.](#)

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

Only Microsoft Entra ID is currently supported. If you want to integrate another supported identity provider, contact your deployment representative.

IMPORTANT: Do not skip the disable groups step. ClearID does not support the synchronization of groups.

Procedure

1. Generate your SCIM key.
2. Create your Microsoft Azure enterprise application.
3. Connect your ClearID SCIM integration to Microsoft Azure.
4. Configure your attribute mappings.
 - a. Disable the Microsoft Entra ID groups setting.
 - b. Configure the Microsoft Entra ID user settings.
5. Configure the ClearID SCIM integration synchronization settings.

After you finish

Review the SCIM integration synchronization status.

Parent topic: [Synchronizing identities using the SCIM integration in ClearID](#)

12.4.3.1 | Generating a SCIM key in ClearID

[Synchronizing identities using the SCIM integration in ClearID](#) >

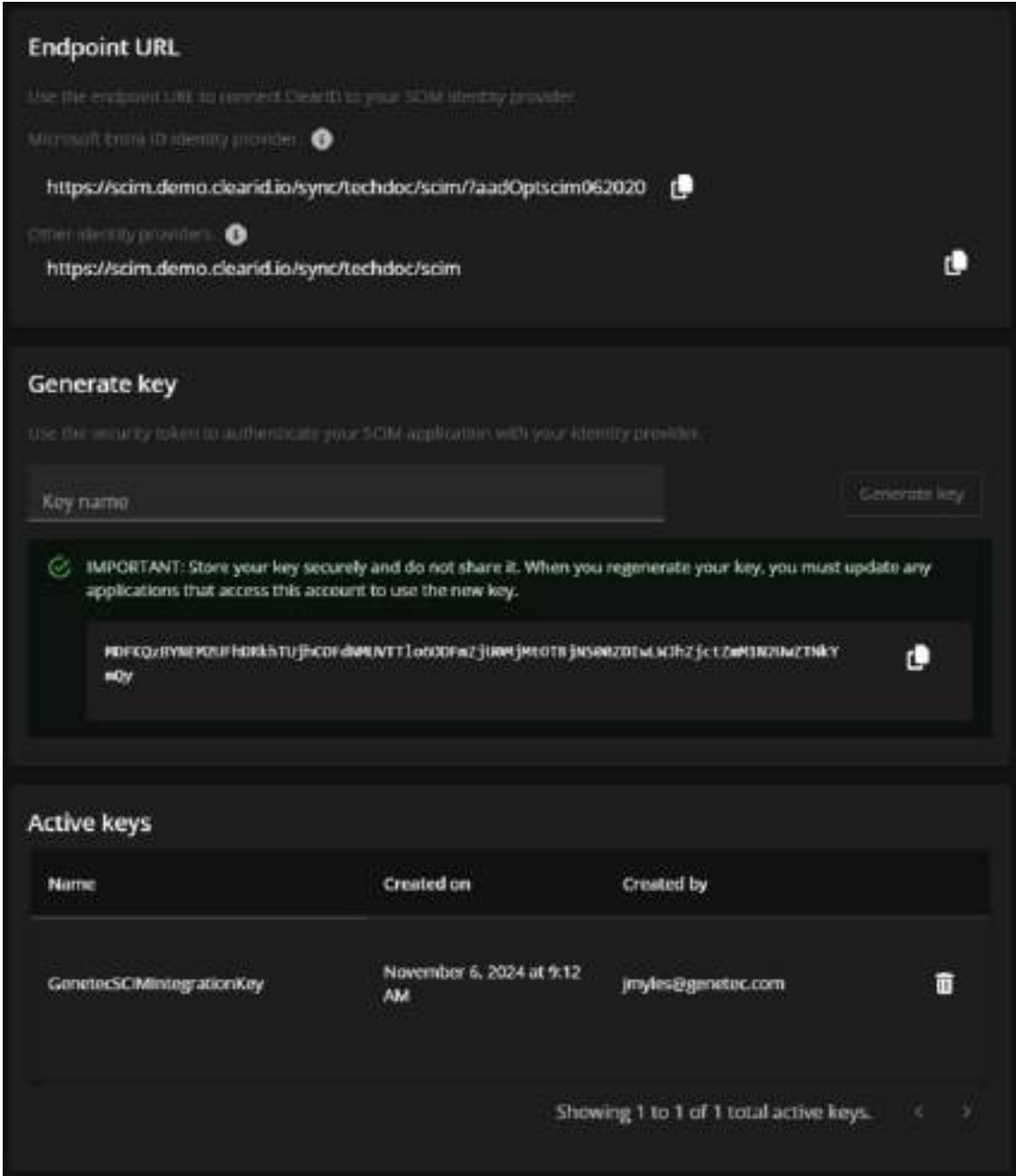
For your Genetec ClearID™ SCIM integration to communicate with Microsoft Entra ID, you must generate a System for Cross-domain Identity Management (SCIM) key.

What you should know

Only a ClearID portal *administrator* can perform this task.

Procedure

1. In the ClearID portal, click Administration > SCIM Integration.
2. In the Generate key section, enter a key name and click Generate Key.
For example, the key name could be GenetecSCIMIntegrationKey.



After you finish

Create your Microsoft Azure enterprise application.
Parent topic: Configuring the SCIM integration in ClearID

12.4.3.2 | Creating an enterprise application in Microsoft Azure

Synchronizing identities using the SCIM integration in ClearID >

Your organization can automate identity attribute provisioning using the Genetec ClearID™ SCIM integration with Microsoft Entra ID as the identity provider. To use the integration, you must first create an enterprise application in Microsoft Azure.

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

Procedure

- 1. In the Microsoft Azure portal, search for and click Enterprise applications.
- 2. In the Enterprise applications section, click New application.
- 3. Click Create your own application.

4. Select Integrate any other application you don't find in the gallery (Non-gallery).
5. Enter your application name and click Create.

For example, the application name could be ClearID SCIM Integration.

Create your own application ×

[Got feedback?](#)

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

ClearID SCIM Integration ✓

What are you looking to do with your application?

☐ Configure Application Proxy for secure remote access to an on-premises application

☐ Register an application to integrate with Microsoft Entra ID (App you're developing)

☒ Integrate any other application you don't find in the gallery (Non-gallery)

Create

NOTE: Watch for a successfully added notification in the upper right of the screen.

After you finish

Connect your ClearID SCIM integration to Microsoft Azure.

Parent topic: Configuring the SCIM integration in ClearID

12.4.3.3 | Connecting your ClearID SCIM integration to Microsoft Entra ID

[Synchronizing identities using the SCIM integration in ClearID >](#)

Before you can use the SCIM integration in Genetec ClearID™ to synchronize identity attributes, you must provide your credentials that connect the ClearID SCIM Integration API to Microsoft Entra ID.

Before you begin

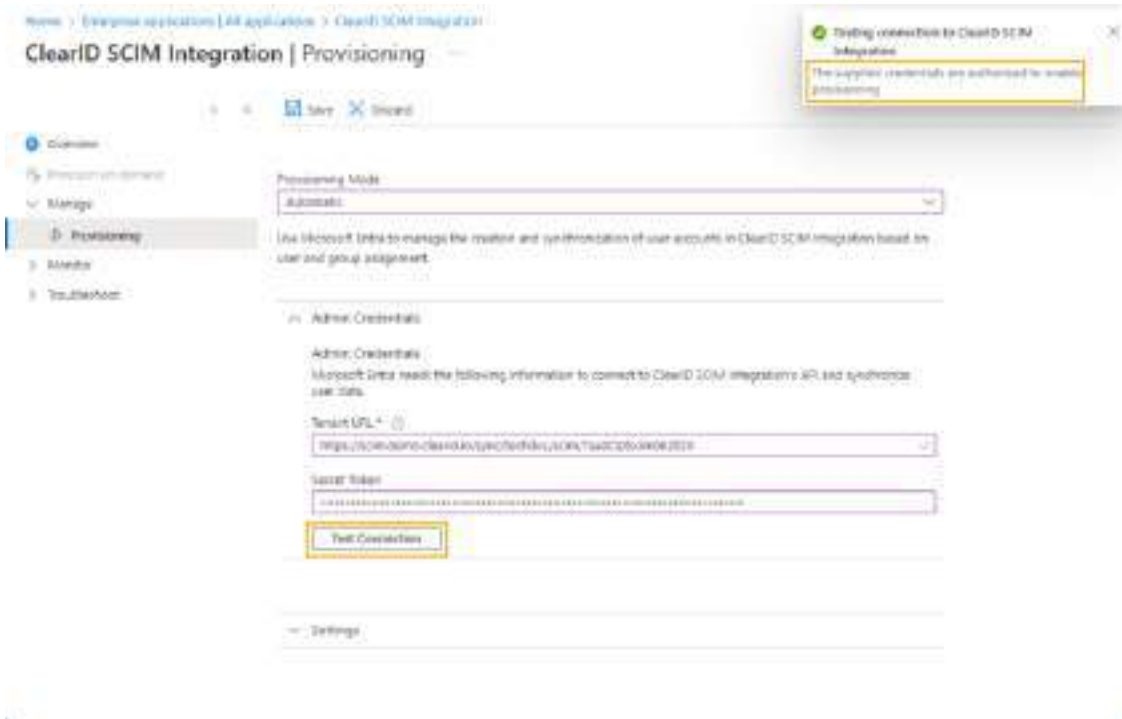
Create your Microsoft Azure enterprise application.

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

Procedure

1. In the Microsoft Entra ID portal, find and click Enterprise applications.
2. In the Enterprise applications section, search for and select your ClearID SCIM integration application.
3. In the Manage section, click Provisioning and then click Provisioning again.
4. From the Provisioning Mode list, select Automatic.
5. Expand the Admin Credentials section.
6. In the ClearID portal SCIM integration tab, locate the Endpoint URL section and click Copy to clipboard next to the Microsoft Entra ID identity provider.
The endpoint URL is copied to your clipboard.
7. Return to the Microsoft Entra ID Provisioning page and paste into the Tenant URL.
The endpoint URL is used to connect ClearID to SCIM authentication systems and Microsoft Entra ID.
8. In the ClearID portal SCIM integration tab, locate the Generate key section and click Copy to clipboard.
9. Return to the Microsoft Entra ID Provisioning page and paste into the Secret Token field.
The SCIM key is used to authenticate your application with Entra ID.
10. Click Test Connection.



11. Click Save.
Tip: Watch for a successful update notification in the upper right of the screen.

After you finish

Disable your Microsoft Entra ID group settings.
Parent topic: [Configuring the SCIM integration in ClearID](#)

12.4.3.4 | Disabling Microsoft Entra ID groups setting in Microsoft Azure

[Synchronizing identities using the SCIM integration in ClearID](#) >

Genetec ClearID™ doesn't support the synchronization of groups. To prevent group settings or attributes from being synchronized, disable the Microsoft Entra ID Groups setting in your Microsoft Azure enterprise application.

Before you begin

Connect your [ClearID SCIM integration](#) to Microsoft Azure.

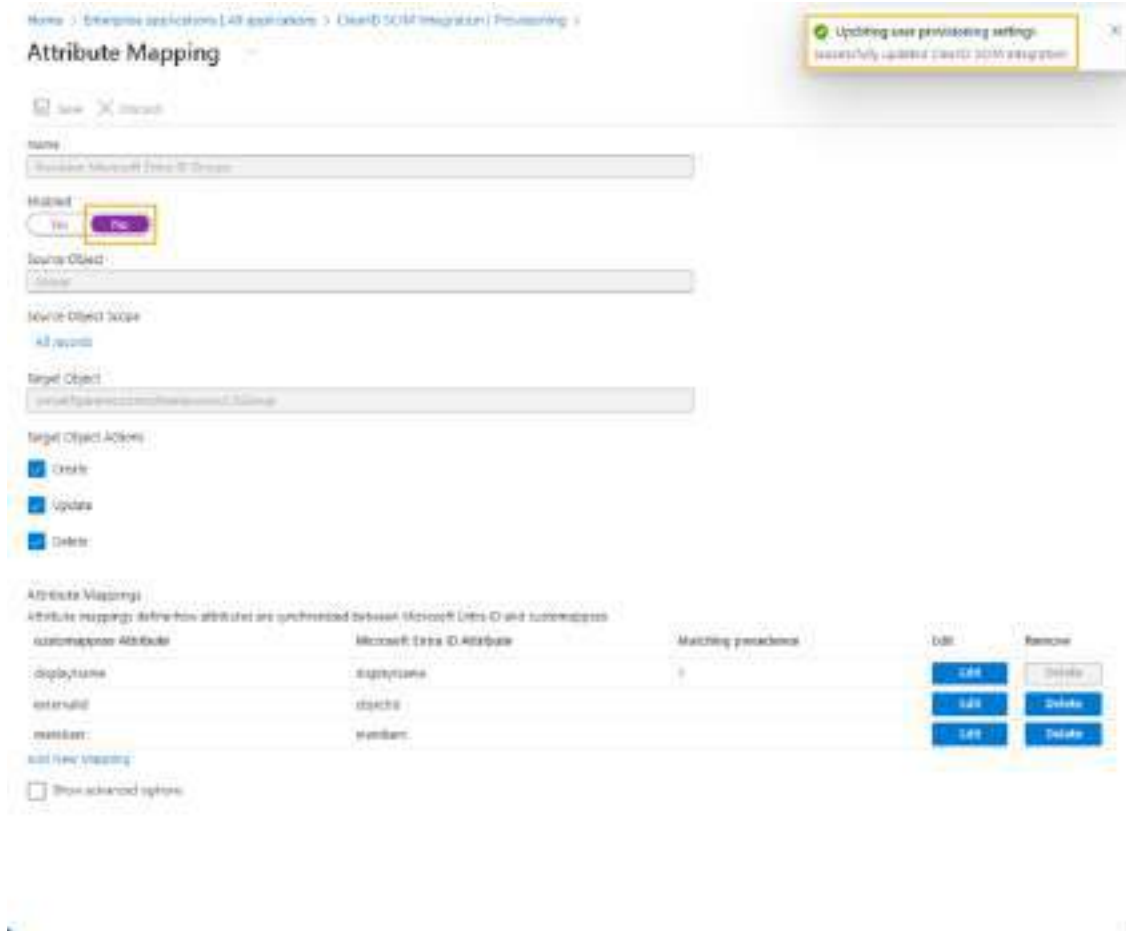
What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.
IMPORTANT: ClearID doesn't support group synchronization. This setting must be disabled.

Procedure

1. In the Microsoft Azure portal, search for and click Enterprise applications.
2. In the Enterprise applications section, search for and select your ClearID SCIM integration application.

3. In the Manage section, click Provisioning and then click Provisioning again.
4. Expand the Mappings section of the Provisioning page.
5. Click Provision Microsoft Entra ID Groups.
6. Move the Enabled slider to No.



7. Click Save and then click Yes to confirm your changes.
8. Close the window and return to the Provisioning page.
It might take a moment to refresh the page.

After you finish

Configure your Microsoft Entra ID user settings.
Parent topic: [Configuring the SCIM integration in ClearID](#)

12.4.3.5 | Configuring Microsoft Entra ID user settings in Microsoft Azure

Synchronizing identities using the SCIM integration in ClearID >

To define how identity data flows between Microsoft Entra ID and Genetec ClearID™, you must configure your user settings and map attributes for automatic synchronization.

Before you begin

Disable your Microsoft Entra ID groups setting.

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

Procedure

1. In the Microsoft Azure portal, search for and click Enterprise applications.
2. In the Enterprise applications section, search for and select your ClearID SCIM integration application.
3. In the Manage section, click Provisioning and then click Provisioning again.
4. Expand the Mappings section and click Provision Microsoft Entra ID Users.
5. Modify the default attribute mappings.
 - a. On the Attribute Mapping page, click Delete to remove unused default attributes.

Only keep the following:

- userName
- active
- displayName

b. Click Save and then click Yes to confirm your changes.

6. Modify the customappsso user attributes.

a. On the Attribute Mapping page, click Show advanced options.

b. Click Edit attribute list for customappsso, and then click Delete to remove all the unused default attributes.

Only keep the following:

- id
- active
- displayName
- title
- userName

c. Click Save and then click Yes to confirm your changes.

7. Add the ClearID schema attributes.

Only include the list of attributes available to ClearID:

Code

```
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:description
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:firstName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:lastName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:middleName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:countryCode
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:email
```

Genetec ClearID®; User Guide

Displayed in the header

```
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:employeeNumber
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:secondaryEmail
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:cityOfResidence
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:stateOfResidence
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:zipCode
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberPrimary
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberSecondary
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:supervisorName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:departmentName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:jobTitle
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:companyName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeDescription
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeCode
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasExtendedTime
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:externalId
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasWebPortalAccess, Boolean
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:isAdmin, Boolean
```

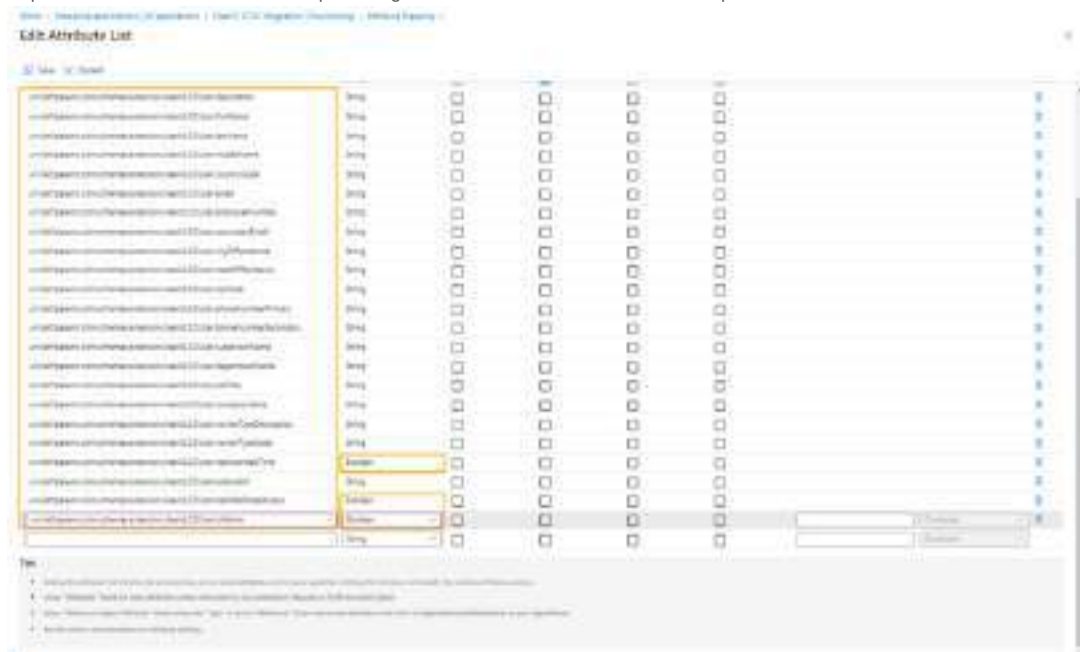


- a. On the Edit Attribute List page, copy and paste an attribute name from the preceding ClearID schema attributes code example into the Name field and select the attribute Type.

Almost every attribute has the type String, except for three attributes that have the Boolean type: hasExtendedTime, hasWebPortalAccess, and UserisAdmin.

IMPORTANT: The ClearID externalId attribute is the unique identifier that ClearID uses for synchronization. It's mapped to the unique objectId attribute in Microsoft Entra ID.

- b. Repeat for each attribute listed in the preceding ClearID schema attributes code example.



- c. Click Save and then click Yes to confirm your changes.

8. Add the ClearID attribute mappings.

- a. On the Attribute Mapping page, click Add New Mapping.

- b. On the Edit Attribute page, add the attributes that you require from the attributes added earlier in step 7.

Include the following:

- Mapping type: Direct
- Source attribute: objectId
- Target attribute: <your attribute value>

- c. Click OK.

- d. Repeat for each attribute added earlier and replace the target attribute value with the next attribute you want to add.

For a successful first synchronization, you need the following attributes. You can add more attributes later.

e. Click **Save** and then click **Yes** to confirm your changes.
You can now close the window and return to the Provisioning page.

Configure the ClearID SCIM integration synchronization settings.

Parent topic: [Configuring the SCIM integration in ClearID](#)

Synchronizing identities using the SCIM integration in ClearID >

Configure your Microsoft Entra ID user settings.

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

1. On the Provisioning page, click Settings and choose which users to synchronize to ClearID:

Synchronizes everything in Microsoft Entra ID.

Only selected users and groups are synchronized.

2. If you chose Sync all users and groups, in the Provisioning status section, move the slider to On and click Save.

Home > Enterprise applications > All applications > ClearID SCIM integration

ClearID SCIM Integration | Provisioning

Save Discard

- Overview
- Provision on demand
- Manage
 - Provisioning
 - Users and groups
 - Expression builder
 - Monitor
 - Troubleshoot

Provisioning Mode:
Automatic

Use Microsoft Entra to manage the creation and synchronization of user accounts in ClearID SCIM integration based on user and group assignment.

Admin Credentials

Mappings

Mappings allow you to define how data should flow between Microsoft Entra ID and your app(s).

Name	Enabled
Provision Microsoft Entra ID groups	No
Provision Microsoft Entra ID users	No

☐ Restore default mappings

Settings

☐ Send an email notification when a failure occurs

☐ Prevent accidental deletion ⓘ

Scope ⓘ

Sync all users and groups

Provisioning Status ⓘ

On Off

3. If you chose Sync only assigned users and groups, complete the provisioning settings.
 - a. Click Users and groups in the left navigation bar.
 - b. Click Add group.
 - c. Click None selected, search for and select the group you want to add, and click Select.
 - d. Click Assign and repeat for each group that you want to add.
 - e. Return to the Provisioning page and click Settings.
 - f. In the Provisioning status section, move the slider to On and click Save.

Home > Enterprise applications > All applications > ClearID SCIM integration

ClearID SCIM Integration | Provisioning

Save Discard

- Overview
- Provision on demand
- Manage
 - Provisioning
 - Users and groups
 - Expression builder
 - Monitor
 - Troubleshoot

Provisioning Mode:
Automatic

Use Microsoft Entra to manage the creation and synchronization of user accounts in ClearID SCIM integration based on user and group assignment.

Admin Credentials

Mappings

Settings

☐ Send an email notification when a failure occurs

☐ Prevent accidental deletion ⓘ

Scope ⓘ

Sync only assigned users and groups

Provisioning Status ⓘ

On Off

After you finish

Review the ClearID SCIM integration synchronization status.
Parent topic: [Configuring the SCIM integration in ClearID](#)

12.4.4 | Resetting SCIM integration identity data in ClearID

To resolve issues with identity data, you can reset and replace all System for Cross-domain Identity Management (SCIM) integration identity data in Genetec ClearID™. This reset process uses the latest values from Microsoft Entra ID.

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

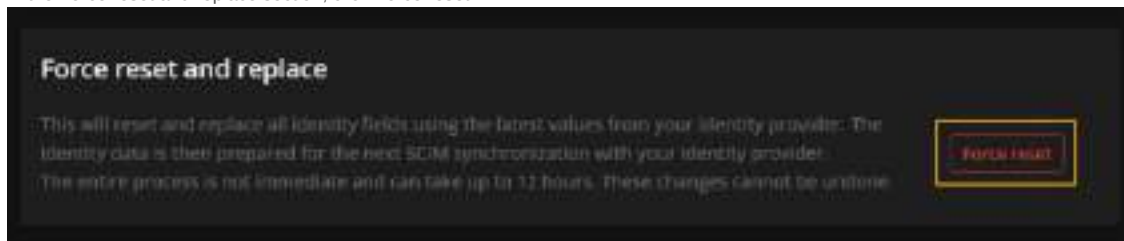
Only use this reset to resolve an identity data issue. For example, after your identity data has been manually manipulated, when there's a discrepancy, or when identity data has been deleted in ClearID.

The reset will prepare identity data for the next SCIM synchronization between ClearID and Microsoft Entra ID. This process only pushes identity data changes in one direction, to Entra ID.

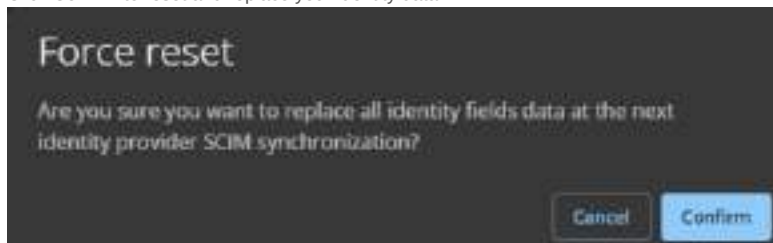
IMPORTANT: The entire process can take up to 12 hours. These changes can't be undone.

Procedure

1. In the ClearID portal, click Administration > SCIM Integration.
2. In the Force reset and replace section, click Force reset.



3. Click Confirm to reset and replace your identity data.



After you finish

Check the SCIM integration synchronization status to confirm that your identity data has been reset.
Parent topic: [Synchronizing identities using the SCIM integration in ClearID](#)

12.4.5 | Reviewing the SCIM integration synchronization status in Microsoft Azure

You can check the overall status of the System for Cross-domain Identity Management (SCIM) integration identity synchronization. You can also review the provisioning logs in Microsoft Azure to see more granular details about Genetec ClearID™ SCIM integration synchronization activities related to a specific person or identity.

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

The provisioning logs can be used to verify whether the ClearID SCIM integration is correctly configured and operational. If there are any issues with the configuration, error messages are generated and recorded in the provisioning logs.

Procedure

1. In the Microsoft Azure portal, find and click Enterprise applications.
2. In Enterprise applications, select your SCIM integration application.

3. On the Overview page, check whether the last synchronization completed successfully and when the last synchronization occurred.



4. (Optional) Click View provisioning logs to see more granular information about identity synchronization.



NOTE: If the log details are long, the Provisioning Logs page includes useful filters to manipulate the data for your needs.

Parent topic: Synchronizing identities using the SCIM integration in ClearID

12.5 | Synchronizing identities using One Identity Synchronization Tool in ClearID

Use the Genetec ClearID™ One Identity Synchronization Tool to synchronize external system attributes into Genetec ClearID™ identity attributes. These identity attributes in ClearID can then be used to assign people to roles and automate role-based access control.

What you should know

Using the One Identity Synchronization Tool you can synchronize external system attributes from the following data sources:

- Azure AD
- Database (Microsoft SQL Server, Oracle Database, ODBC)
- File (CSV)

Procedure

1. Learn about the One Identity Synchronization Tool.
2. Learn about One Identity attribute fields.
3. Learn about the Azure web app.
4. Install the One Identity Synchronization Tool.
5. Configure the One Identity Synchronization Tool.
6. Review synchronization status.

Browse

- ClearID One Identity Synchronization Tool connectivity issues
- ClearID One Identity Synchronization Tool data synchronization issues

12.5.1 | About the ClearID One Identity Synchronization Tool

The Genetec ClearID™ One Identity Synchronization Tool is a Windows service that you can use to import identities information from an external system into Genetec ClearID™.

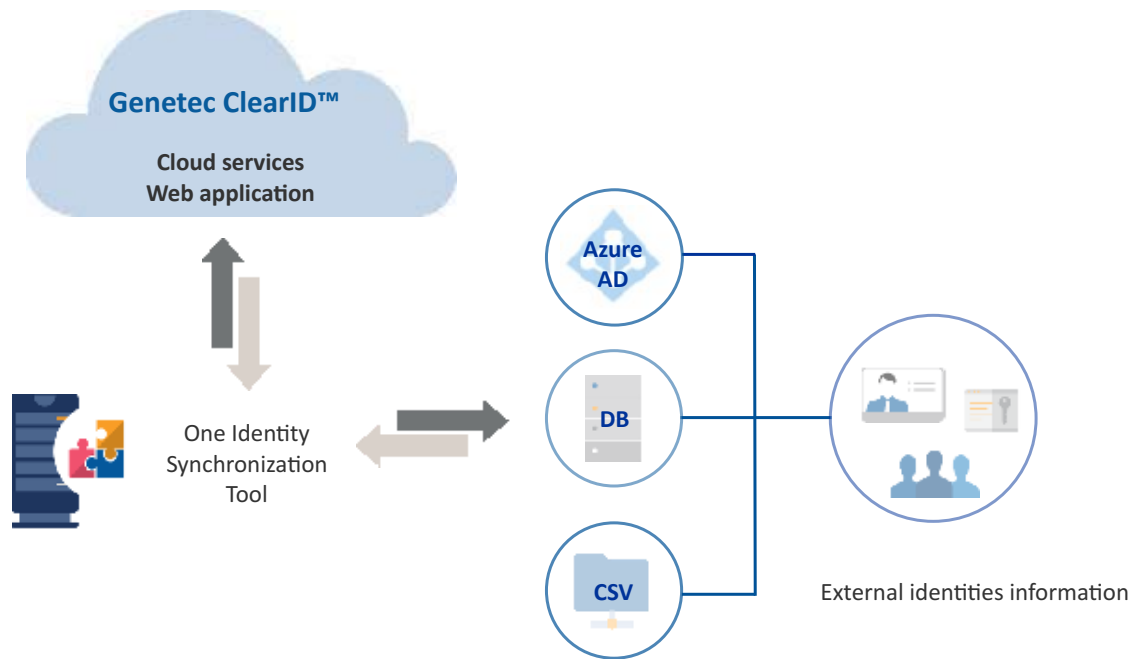


The ClearID One Identity Synchronization Tool includes the following components:

- Genetec.ClearID.OneIdentity.SynchronizationTool (OneIdentityConfigurationTool.exe) is the user interface component of the windows application that is used to configure the Synchronization Tool.
- Genetec.ClearID.OneIdentity.SynchronizationService (OneIdentityService.exe) is the Windows service component of the application that performs external system attributes to ClearID identity attributes synchronization automatically in the background at intervals specified in the Synchronization Tool.

Data sources

You can select one or more data sources to be synchronized from an external system. Using the Data sources configuration dialog you configure the Data sources and map the One Identity attributes to their associated external system attributes.



Azure Active Directory

The Azure AD data source is an Azure Active Directory that you can import identities information from. For example, importing identities, credentials, and pictures into ClearID.

Database

The database data source can be a Microsoft SQL Server database, an Oracle database, or an ODBC-compliant database that follows the one identity attribute mapping. The database must be accessible from the server where the ClearID One Identity Synchronization Tool is installed. One database can contain one table or view for identities information.

File

The file data source is a delimited text file. For example, a CSV file that follows the one identity attribute mapping, and must be accessible from the server where the ClearID One Identity Synchronization Tool is installed. Each file contains identities information.

Synchronization

Identities in ClearID can come from a variety of data sources (Databases, HR, External Sources) and can be synchronized using various tools (Genetec ClearID™ LDAP Synchronization Agent, Genetec ClearID™ API, or Genetec ClearID™ One Identity Synchronization Tool).

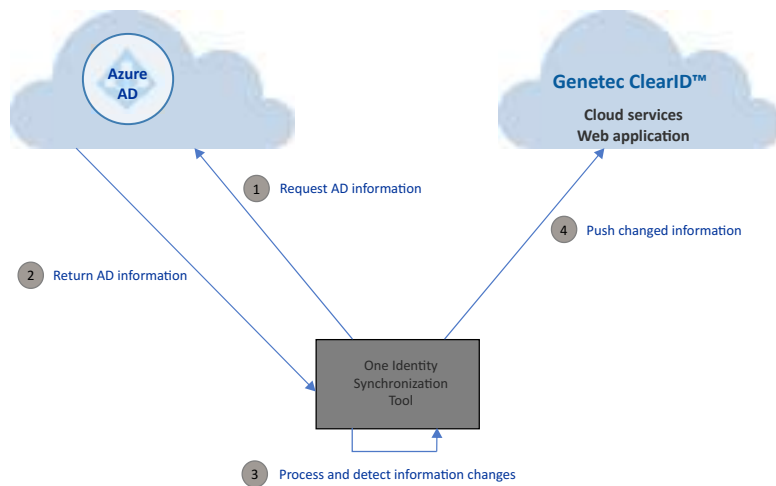
- LDAP is typically used for Active Directory attributes synchronization into ClearID identities.
- API is typically used for real-time updates. For example, to remove people quickly. This API synchronization option is the most flexible but it is expensive.
- One Identity is typically used for HR systems. For example, to synchronize all employees every day or every 4hrs. The ClearID One Identity Synchronization Tool is configured to synchronize at the same frequency.

One Identity data synchronization

The following information describes One Identity synchronization:

- Synchronization of external system attributes into ClearID identity attributes is INBOUND only.
CAUTION:
Any changes only made to identities in ClearID can be overwritten by the next synchronization from the external system.
- Synchronization can be performed manually using the Synchronize now (🔴) option, or automatically at the Automatic synchronization intervals specified in the One Identity Synchronization Tool.
 - For each One Identity field that is configured, a custom mapping to the External field in the external system is created. This mapping ensures that the external system attributes can be synchronized into the One Identity attribute fields.

The following diagram illustrates an Azure AD data synchronization:



The synchronization workflow is essentially the same for all data sources:

1. Data source information is requested.
2. Data source information is returned.
3. Any information changes are processed and detected.
4. Data source information is pushed to the ClearID web application.

Sample SQL files

For the Database data source option, sample SQL script files are provided with the tool and can be found here:

Code

C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service



- Identities_Oracle.sql
- Identities_SqlServer.sql

The sample SQL script files can be used to test the Database data source solution, or to help you understand the SQL data format.

Sample CSV files

For the File data source option, a sample CSV file is provided with the tool and can be found here:

Code

C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service



- Identities.csv

The sample CSV files can be used to test the File data source solution, or to help you understand the CSV data format.

Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.2 | About ClearID One Identity Synchronization Tool attribute fields

When you synchronize an external system with Genetec ClearID™ using the Genetec ClearID™ One Identity Synchronization Tool, your external system attributes are synchronized (imported) into ClearID identity attributes using the field mappings in the One Identity Synchronization Tool.

NOTE: The data source order is important because the first data source always overrides common fields.

Identity attributes

One Identity field	Data type	Description
Unique ID*	Text field	A unique ID for the identity. The unique ID can be an alphanumeric code or an email address. For example, Employee number xyz12345. IMPORTANT: (Azure Active Directory only) If you ever change the mapping of the Unique ID it can cause duplicate data issues.
* This field is mandatory.		

Genetec ClearID®; User Guide

Displayed in the header

One Identity field	Data type	Description
Activation date	DateTime	The date that the identity is activated. For example, 1/11/2022. NOTE: All invariant culture DateTime formats are supported.
City	Text field	The city where the identity is located. For example, Paris.
Company	Text field	The company name. For example, Genetec™.
Country code	Text field	The three letter country code (UPPERCASE). For example, the USA or CAN. NOTE: The three-letter country codes are based on the Alpha-3 codes in the ISO 3166-1 country codes standard.
Date of birth	DateTime	The identity's date of birth. For example, 7/21/2022. NOTE: All invariant culture DateTime formats are supported.
Department	Text field	The department name. For example, IT or Marketing.
Description	Text field	The identity description.
Email address	Text field	The primary email address (business email) for the identity. For example, johndoe@test.com
Employee number	Text field	The identity's employee number.
Expiration date	DateTime	The date that the identity expires. NOTE: All invariant culture DateTime formats are supported.
First name	Text field	The first name of the identity.
Job title	Text field	The job title of the identity.
Last name	Text field	The last name of the identity.
Middle name	Text field	The middle name of the identity
Mobile phone number	Text field	The secondary phone number (Mobile phone number) For example, 555-555-5555.
Personal email	Text field	The secondary email address (personal email) for the identity. For example, johndoe2@test.com
Phone number	Text field	The primary phone number (Office phone number) For example, 555-555-5555.
Picture	Image	A picture in the format of a blob, a base64 string, or a path to an image. Supported values: - File path - uses a standard windows file path. The path must be accessible from the server. - base64 encoded string - uses a standard base 64 encoding. - Binary - binary data. Supported Image formats: png, jpeg, and bmp.
Preferred name	Text field	The preferred name of the identity.
Provisioning attributes	Text field	Provisioning attributes as defined and configured by the customer for their environment. The list items are separated by a pipe character " ". For example, A1 A2 A3.
State or province	Text field.	The state or province where the identity is located.
Status	Text field	The Identity activation status. For example, Active or Inactive.
Supervisor name	Text field	The name of the identity's supervisor.
Supervisors	Text field	The list of unique supervisor IDs for the identity. The list items are separated by a pipe character " ". For example, A1 A2 A3.
Use extended grant time	Boolean value	The value that enables or disables the Use extended grant time option. For example, TRUE or FALSE.

One Identity field	Data type	Description
User type	Text field	The type of user. For example, Admin or User.
Username	Text field	The email used by the identity to log on to ClearID.
Web portal access	Text field	The value that enables or disables web portal access. For example, 0 FALSE or 1 TRUE.
Worker type code	Text field	The worker type code.
Worker type description	Text field	The worker type description.
Zip or postal code	Text field.	The Zip or postal code of the identity's location.

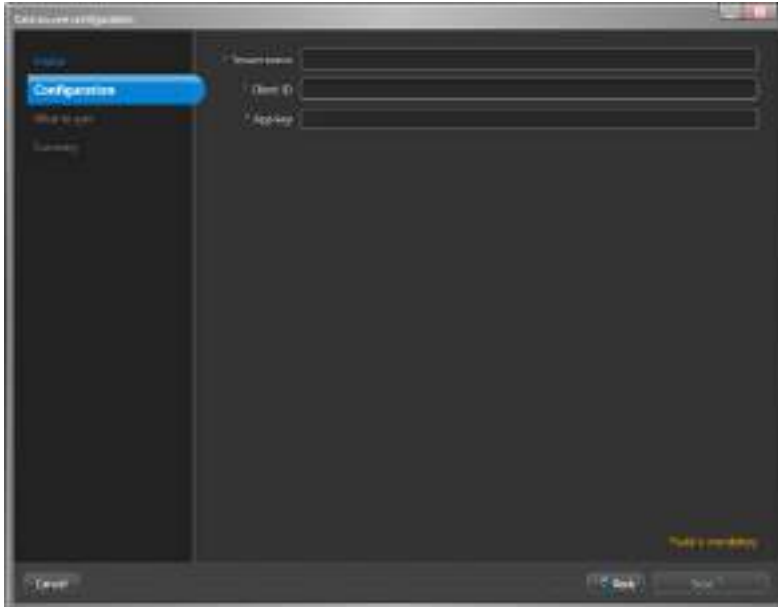
Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.3 | About the Azure web app for ClearID One Identity Synchronization Tool

The Azure web app is a web application that is used to connect Genetec ClearID™ One Identity Synchronization Tool to the Azure AD data so that the Active Directory user information can be accessed and synchronized.

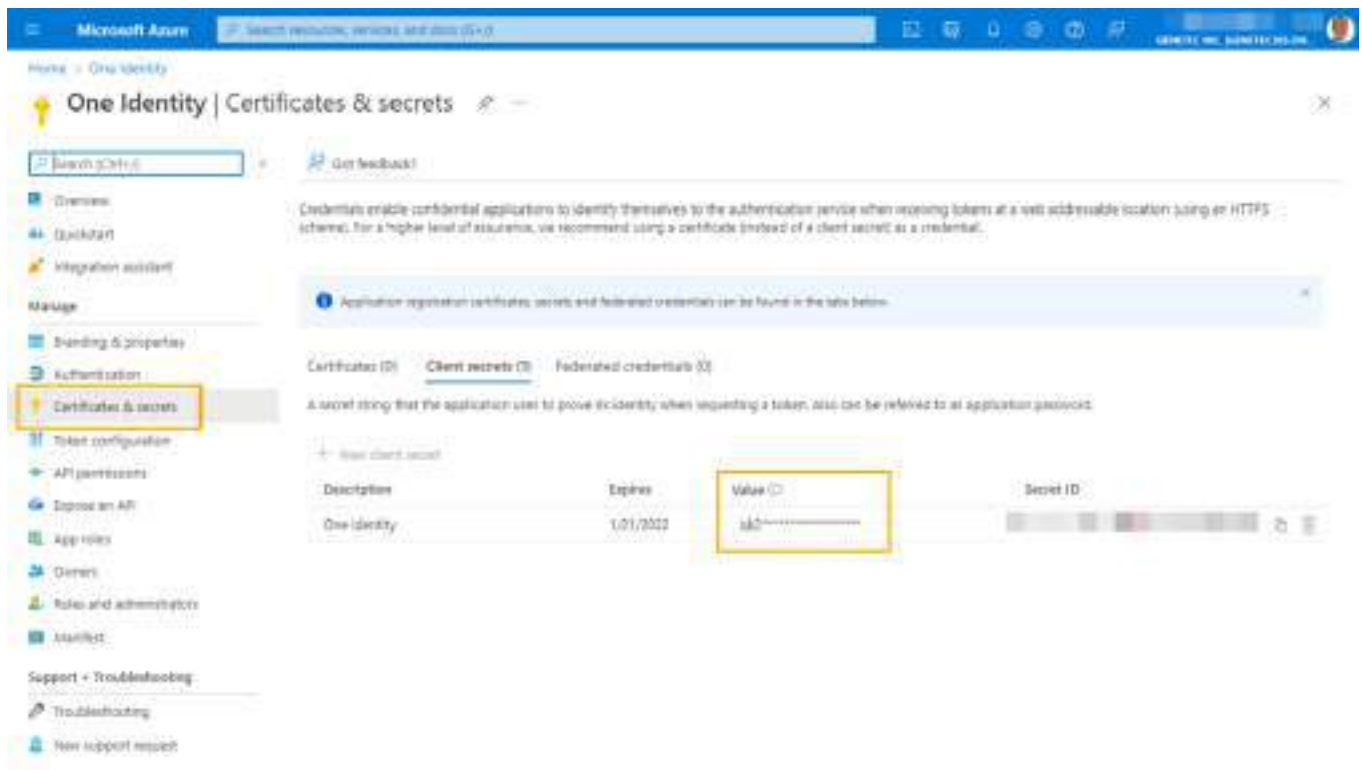
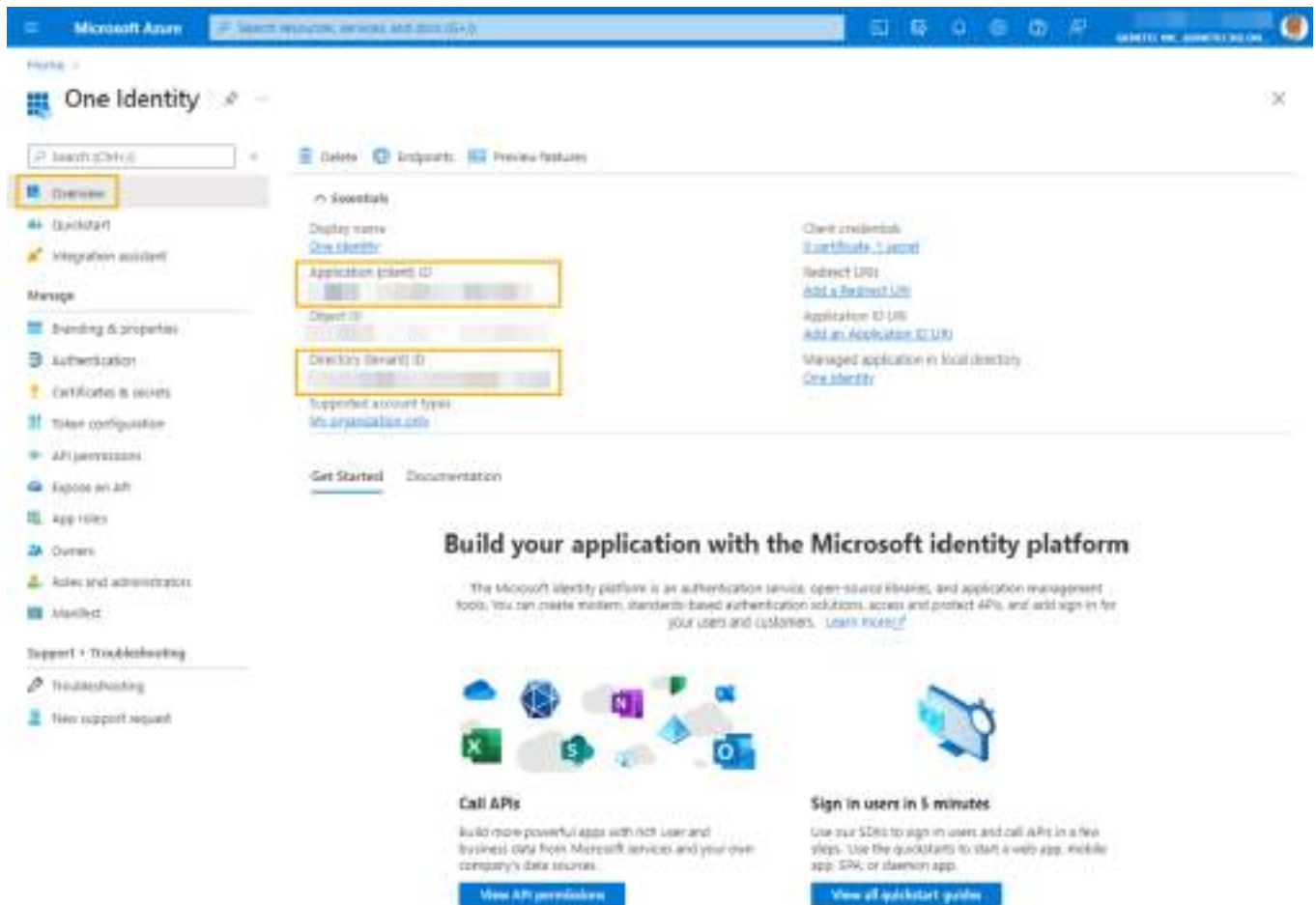
Connection information for Azure web app

To connect the Azure web app to the ClearID One Identity Synchronization Tool, you need the following information:



- Tenant name (Directory ID for account)
- Client ID (Application ID)
- App key (Client secret value)

Tip: The Tenant name, Client ID, and App key can be obtained from your Azure Active Directory application registration.



Azure AD API permissions

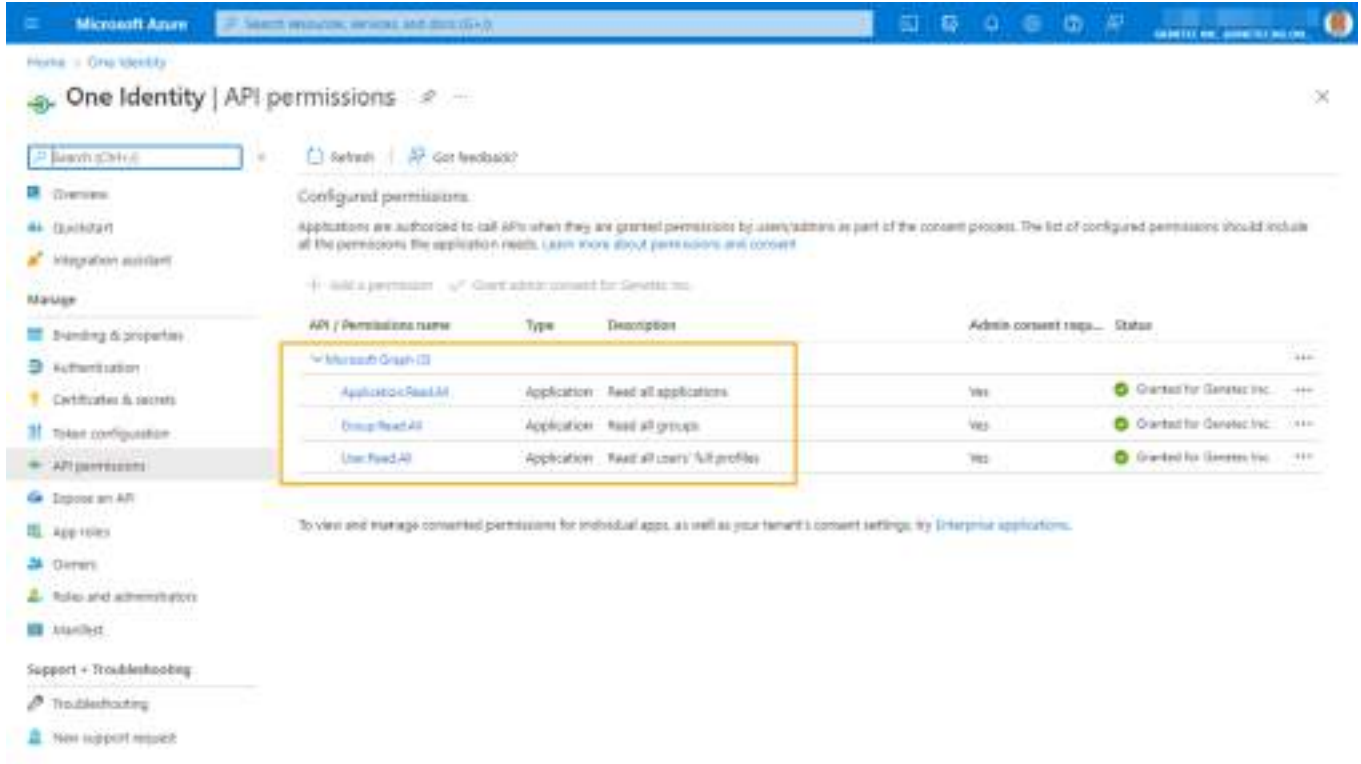
Before you can synchronize data with ClearID, an external system attributes administrator (IT or security personnel) must set up and configure the following API read permission privileges in Azure AD.

Microsoft Graph (minimum requirements):

- *Application.Read.All* - Used to get extensions attributes.
 - Allows the app to read applications and service principals without a signed-in user.

For more information, see [List extensionProperties \(directory extensions\)](#)

- *User.Read.All* - Used to get user information.
 - Allows the app to read identity user risk information for all users in your organization without a signed-in user.
- *Group.Read.All* - Used to get group information.
 - Allows the app to read group properties and memberships, and read conversations for all groups, without a signed-in user.



For more information, see [Microsoft Graph permissions reference](#).

Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.4 | Installing the ClearID One Identity Synchronization Tool

Before you can import identities information from an external system into Genetec ClearID™, you must first install the Genetec ClearID™ One Identity Synchronization Tool.

Before you begin

Obtain the latest installer package from your deployment contact.

What you should know

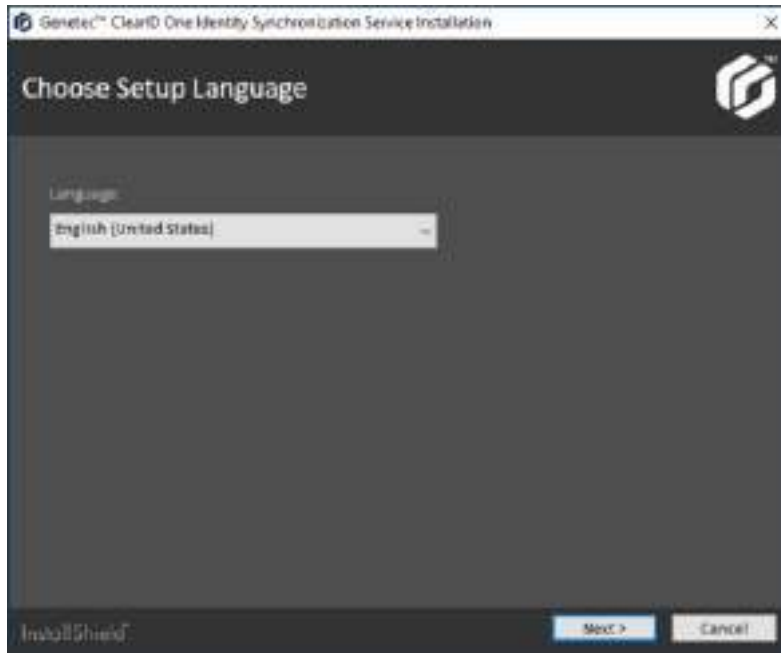
This procedure is for IT or security personnel responsible for external system attributes administration.

Install the One Identity Synchronization Tool on its own dedicated server. It does not require a Security Center server.

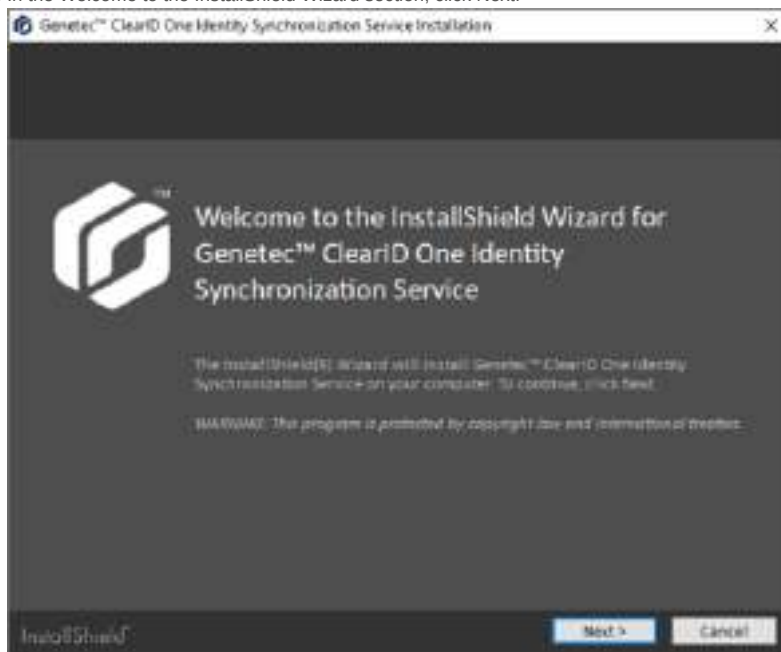
NOTE: The One Identity Synchronization Tool is not generally available as a public download. The synchronizer download is supplied by your Deployment contact when needed.

Procedure

1. Navigate to the ClearID One Identity Synchronization Tool installer supplied by your deployment contact.
2. Right-click the setup.exe file. Then click Run as administrator and follow the installation instructions.
3. In the Genetec ClearID™ One Identity Synchronization Service Installation dialog, select a setup language and click Next.



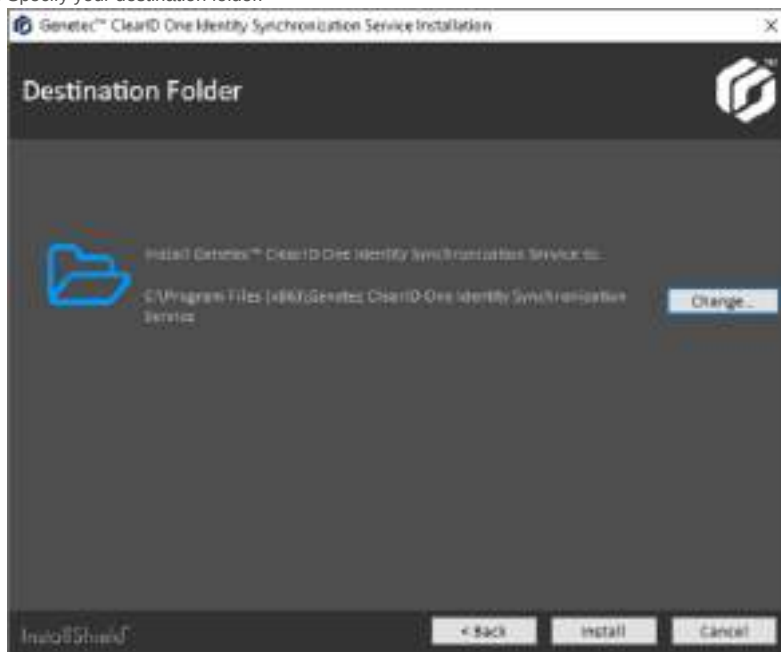
4. In the Welcome to the InstallShield Wizard section, click Next.



5. Review and accept the license agreement, then click Next.



6. Specify your destination folder.

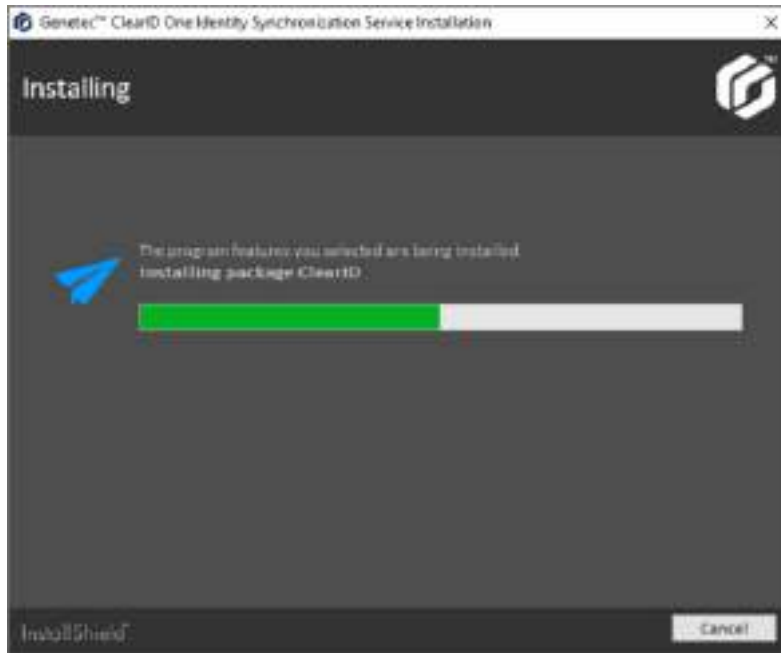


By default the service is installed at C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service.

7. (Optional) Click Change to modify the destination folder.

a. In the Browse For Folder dialog, browse to and select the folder where you want the service installed and click OK.

8. Click Install.



9. Click Finish to complete the installation.



Results

The ClearID One Identity Synchronization Tool is now installed.

After you finish

Configure the synchronization tool.

Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.4.1 | Uninstalling the ClearID One Identity Synchronization Tool

[Synchronizing identities using One Identity Synchronization Tool in ClearID](#) >

From time to time, you might want to uninstall the Genetec ClearID™ One Identity Synchronization Tool to fix a problem or install an updated version.

Before you begin

The Genetec ClearID One Identity Synchronization Tool must be installed.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

Genetec ClearID®; User Guide

Displayed in the header

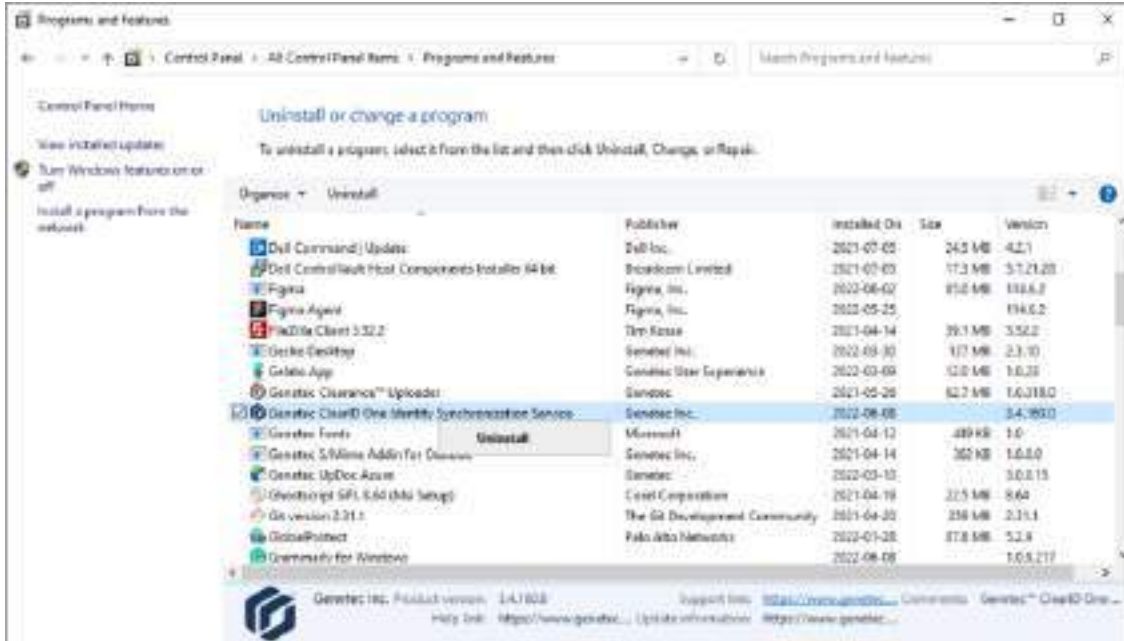
- The options that you encounter while uninstalling a program (service) might vary depending on the version of Windows that you are running.
- This procedure describes how to uninstall the synchronization tool (service) from a Windows 10 client.

CAUTION:

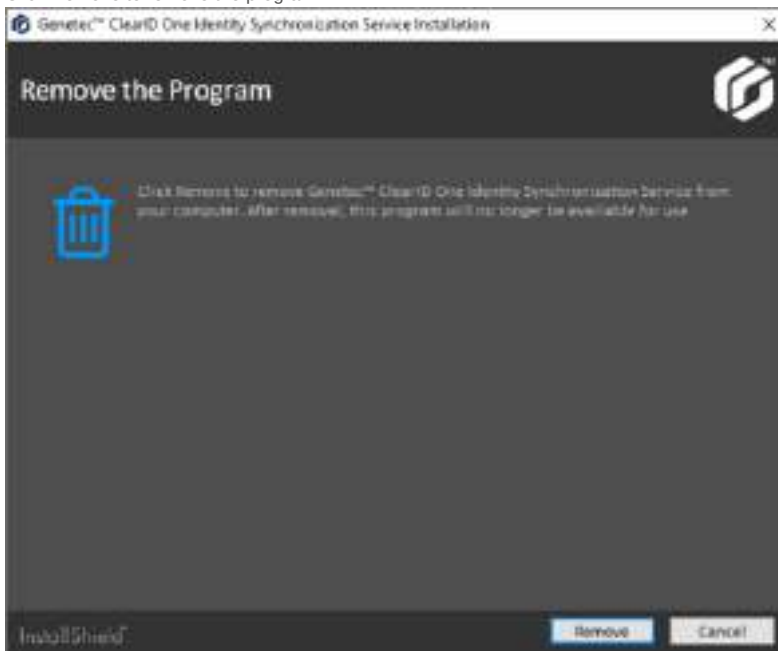
The uninstall process deletes all configuration data. If you are upgrading, make sure that you back up your program data in the configuration folder C:\ProgramData\Genetec\OneIdentity\Configuration.

Procedure

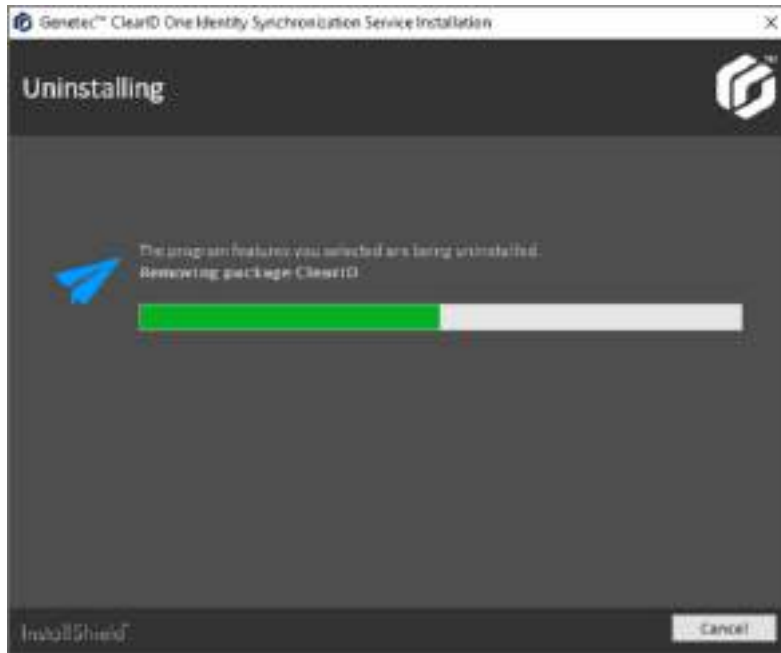
1. Open the Windows Control Panel, and in the Programs section click Uninstall a program to access Programs and Features.
2. Find the ClearID One Identity Synchronization Tool service and right-click to display the Uninstall option, then click Uninstall.



3. Click Remove to remove the program.



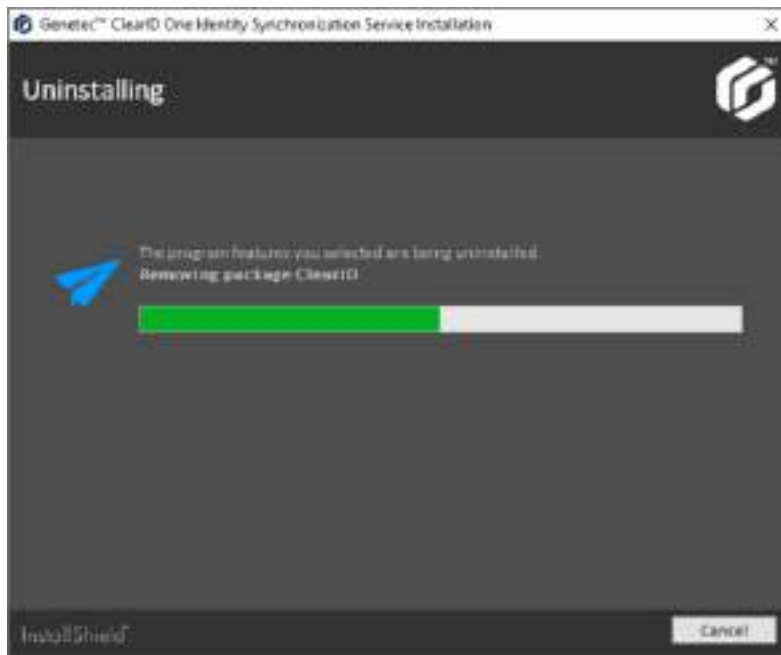
The program uninstall begins.



4. (Optional) If the following dialog is displayed, select Automatically close and attempt to restart applications then click OK.



The package continues to uninstall.



5. Click Finish to complete the uninstall.



Results

The ClearID One Identity Synchronization Tool has now been uninstalled.
Parent topic: [Installing the ClearID One Identity Synchronization Tool](#)

12.5.4.2 | Upgrading the ClearID One Identity Synchronization Tool

[Synchronizing identities using One Identity Synchronization Tool in ClearID >](#)

Upgrade Genetec ClearID™ One Identity Synchronization Tool to the latest version when it becomes available so that you can use new features.

Before you begin

The Genetec ClearID One Identity Synchronization Tool must be installed.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

Procedure

1. Back up the configuration folder C:\ProgramData\Genetec\OneIdentity\Configuration.
The folder contains configuration settings. For example, ApiConfiguration.dat, ClearIdEntityMappingFile.xml, Configuration.xml, and SingleCardEntityMapping.xml.
NOTE: The .dat or .xml files that you encounter in the configuration folder vary depending on the settings that you configure in the ClearID One Identity Synchronization Tool.
2. Uninstall ClearID One Identity Synchronization Tool (previous version).
3. Install ClearID One Identity Synchronization Tool (latest version).
4. Validate the ClearID One Identity Synchronization Tool is working as expected.
NOTE: You should have the same data source configurations as before the upgrade.

Results

The ClearID One Identity Synchronization Tool has now been upgraded.
Parent topic: [Installing the ClearID One Identity Synchronization Tool](#)

12.5.5 | [Configuring the ClearID One Identity Synchronization Tool](#)

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool.

Before you begin

- [Familiarize yourself with the One Identity attribute fields.](#)
- Verify the identities attributes values that you want to import and synchronize before synchronizing.
- [Download a service authentication key.](#)
- [Install the One Identity Synchronization Tool.](#)
- Check your license information: Part number CD-IDSYNC-SERVICE-1Y is required for One Identity Synchronization Tool import.

IMPORTANT: Make sure that the file is not being edited and is closed, because the synchronization tool locks the file during the synchronization process.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.
Synchronization of external system attributes into ClearID identity attributes is INBOUND only.
CAUTION:
Any changes only made to identities in ClearID can be overwritten during the next synchronization from the external system.

Procedure

1. [Configure your connection settings.](#)
2. Configure data source settings for one of the following sources:
 - [Azure AD](#)
 - [Database \(Microsoft SQL Server, Oracle Database, ODBC\)](#)
 - [File \(CSV\)](#)
3. Configure your synchronization settings.
4. Click Save.

After you finish

[Verify that the new attributes from the external system have been synchronized and contain the correct attributes.](#)
Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.5.1 | [Configuring connection settings for the ClearID One Identity Synchronization Tool](#)

[Synchronizing identities using One Identity Synchronization Tool in ClearID](#) >

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool connection settings.

Before you begin

- [Verify the identities attributes values that you want to import before synchronizing.](#)
- [Download a service authentication key.](#)
- Check your license information: Part number CD-IDSYNC-SERVICE-1Y is required for One Identity Synchronization Tool import.

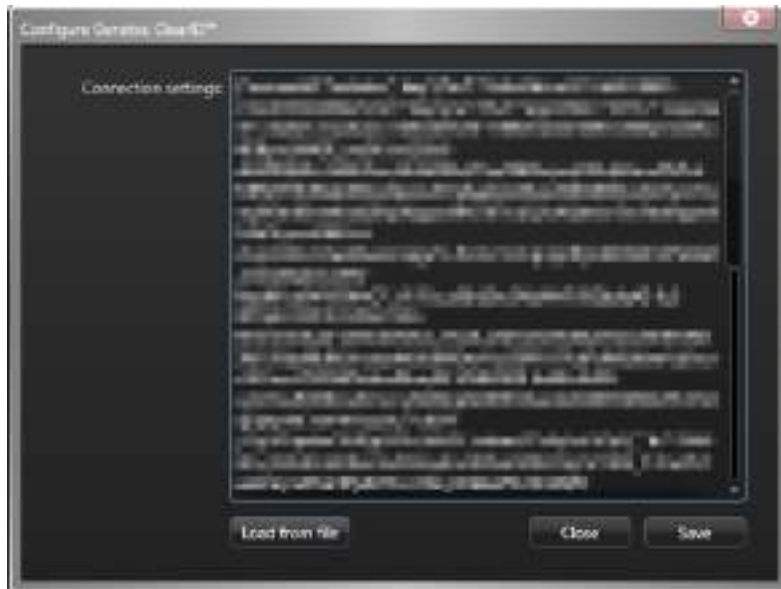
What you should know

Procedure

1. Open the One Identity Synchronization Tool (OneIdentityConfigurationTool.exe) and configure your settings.



2. Configure your connection settings.
 - a. In the One Identity Synchronization Tool, click Configure.
 - b. In the Configure Genetec ClearID™ dialog, click Load from file.
 - c. Navigate to and select your authentication key.



3. Click Save.

NOTE: The One Identity service is automatically restarted when the connection settings for the authentication key are changed.

Results

Your One Identity Synchronization Tool is now connected to ClearID.



After you finish

Configure your data sources. Choose one of the following:

- [Configuring the data source for Azure AD synchronization in the ClearID One Identity Synchronization Tool](#)
- [Configuring the data source for Database synchronization in the ClearID One Identity Synchronization Tool](#)
- [Configuring the data source for File synchronization in the ClearID One Identity Synchronization Tool](#)

Parent topic: [Configuring the ClearID One Identity Synchronization Tool](#)

12.5.5.2 | [Configuring the data source for Azure AD synchronization in the ClearID One Identity Synchronization Tool](#)

[Synchronizing identities using One Identity Synchronization Tool in ClearID >](#)

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool data sources for Azure Active Directory synchronization.

Before you begin

- Familiarize yourself with the One Identity attribute fields.
- Familiarize yourself with the Azure web app.
 - Make a note of the Azure web app connection settings for later use.
 - Make sure that the Azure AD API permissions are set up.
- Prepare an Azure Active Directory containing the identities attributes that you want to import and synchronize.
- Check your license information: Part number CD-IDSYNC-SERVICE-1Y is required for One Identity Synchronization Tool import.

What you should know

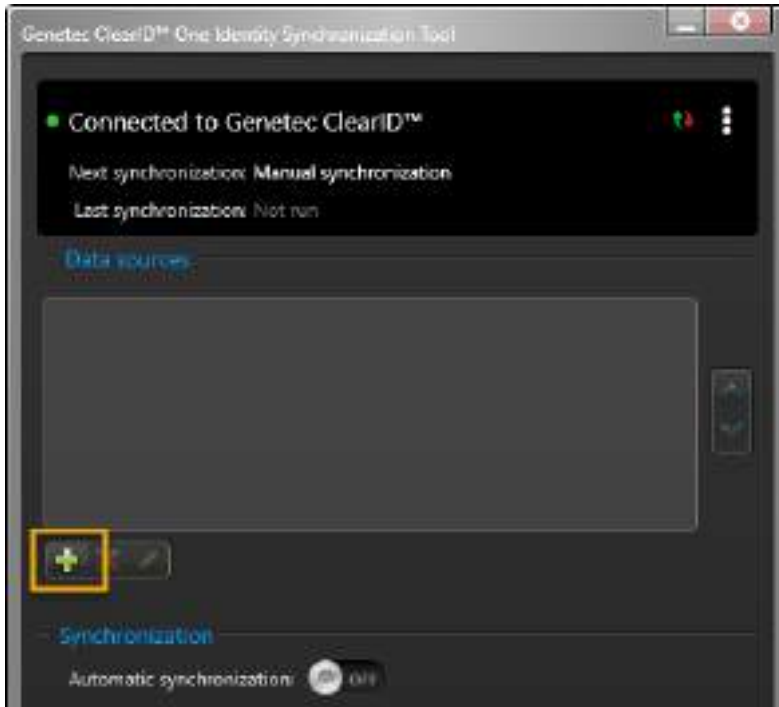
This procedure is for IT or security personnel responsible for external system attributes administration.

This procedure describes how to configure the data source for Azure AD.

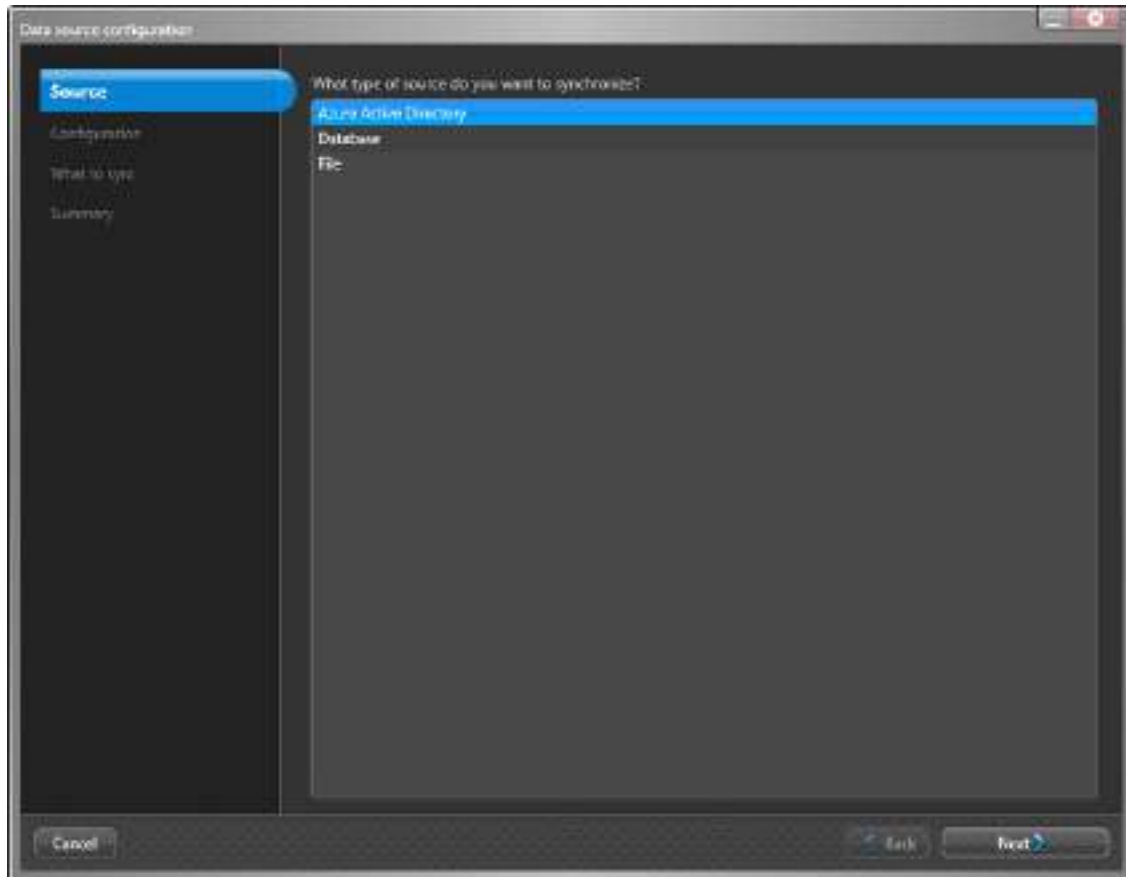
- The data source order is important because the first data source always overrides common fields.
- There is no limit to the number of data sources. However, the larger the data source, the memory requirements increase.
- When using an Azure data source to synchronize identities, the only possible field for Unique ID is the UserId field. When the Azure data source is selected, the Unique ID fields cannot be configured and use of the Azure UserId field is triggered by default.

Procedure

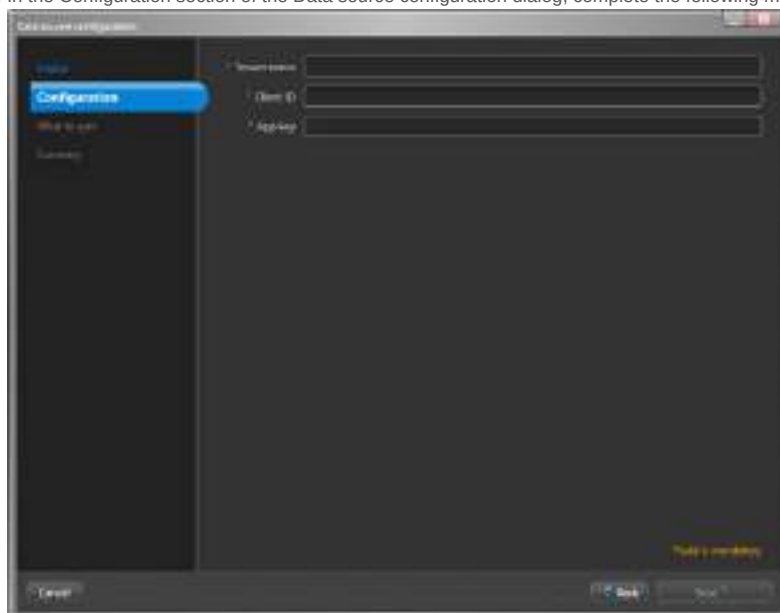
1. In the One Identity Synchronization Tool Data sources section, click Add data source (+).



2. In the Source section of the Data source configuration dialog, select Azure Active Directory and click Next.



3. In the Configuration section of the Data source configuration dialog, complete the following mandatory fields:



Tenant name

In the Tenant name field, enter your tenant name (account name). The tenant name is used to connect to the directory for the account. For example, a host address account.onmicrosoft.com or a GUID nxxxxnxxx-nnnn-nxnn-nnnx-nxxxxnxxxxnnn.

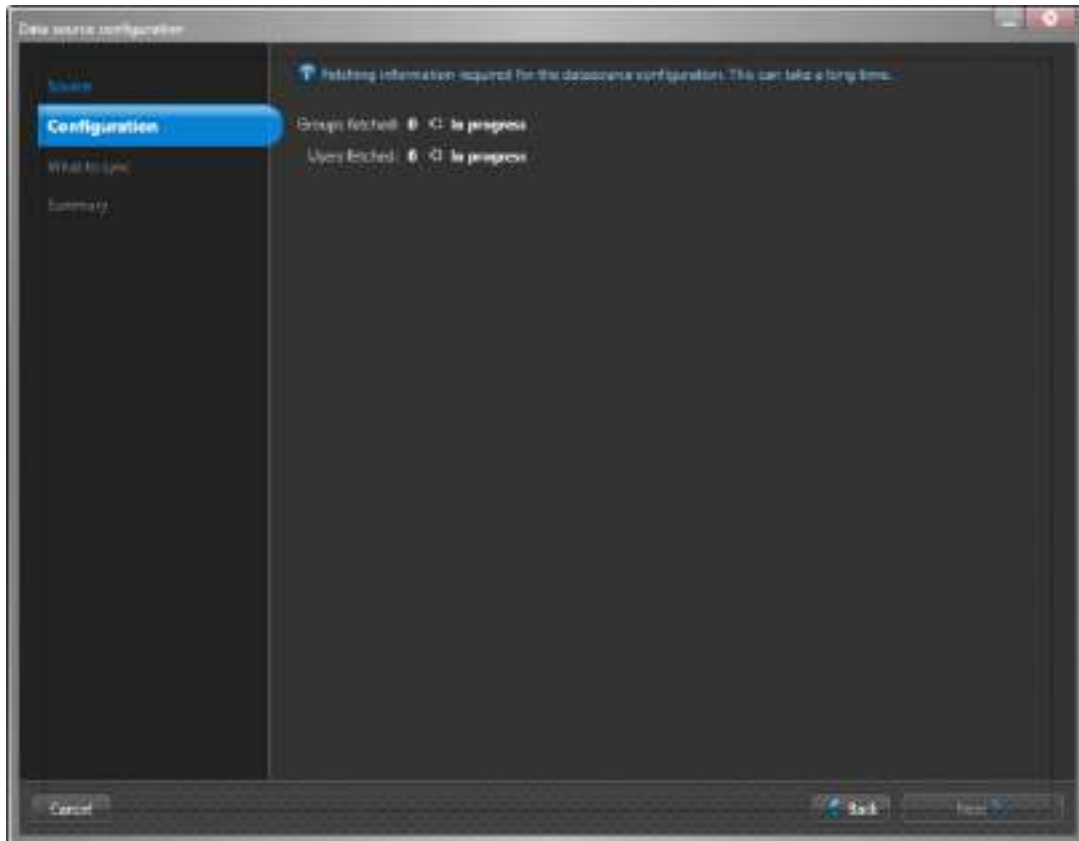
Client ID

In the Client ID field, enter your client ID. The client ID is used to connect to the client application. The Client ID format is an alpha-numeric format as follows: nxxxxnxxx-nxnn-nnnx-nxnn-nxxxxnxxxxnnn.

App key

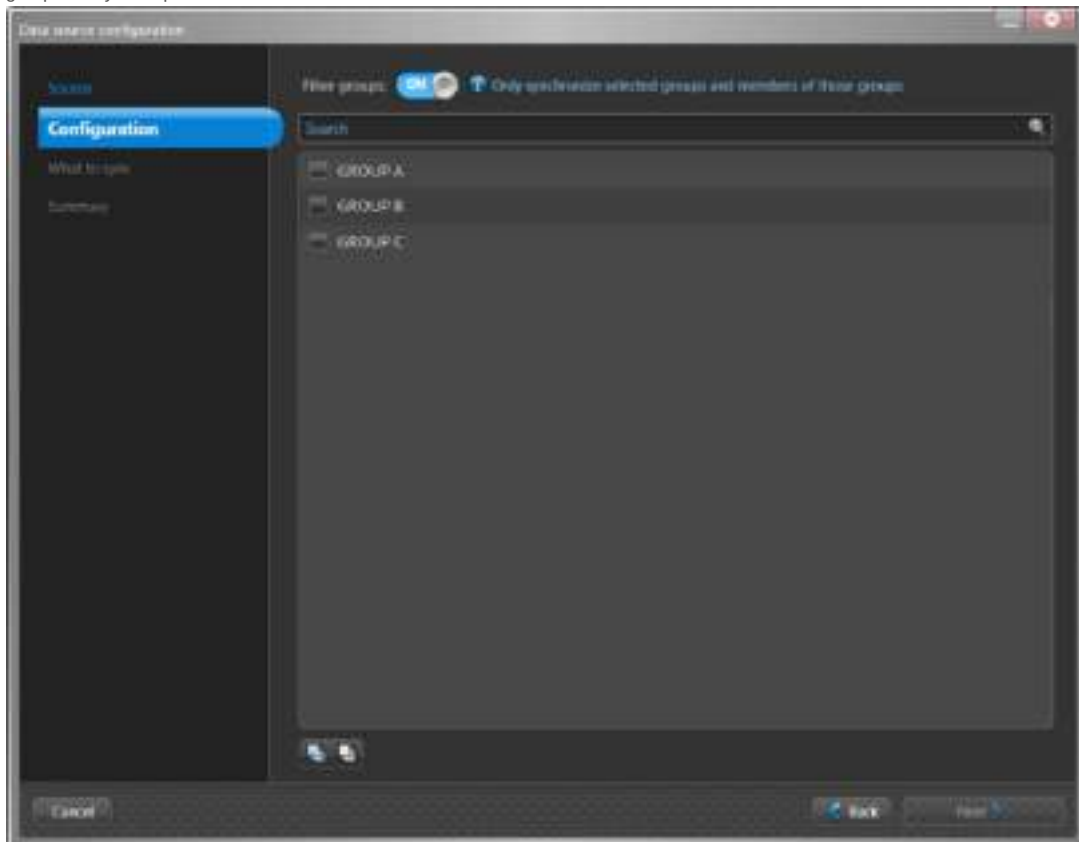
In the App key field, enter your App key. The App key is used to authenticate communications with ClearID. The App key format is an alpha-numeric format as follows: nXnxxxxXxxXnxxxxXXxXnxxxxXXnxxxxXnXXXXXxxx= .

- Tip: The Tenant name, Client ID, and App key can be obtained from your Azure Active Directory application registration.
- Click Next.



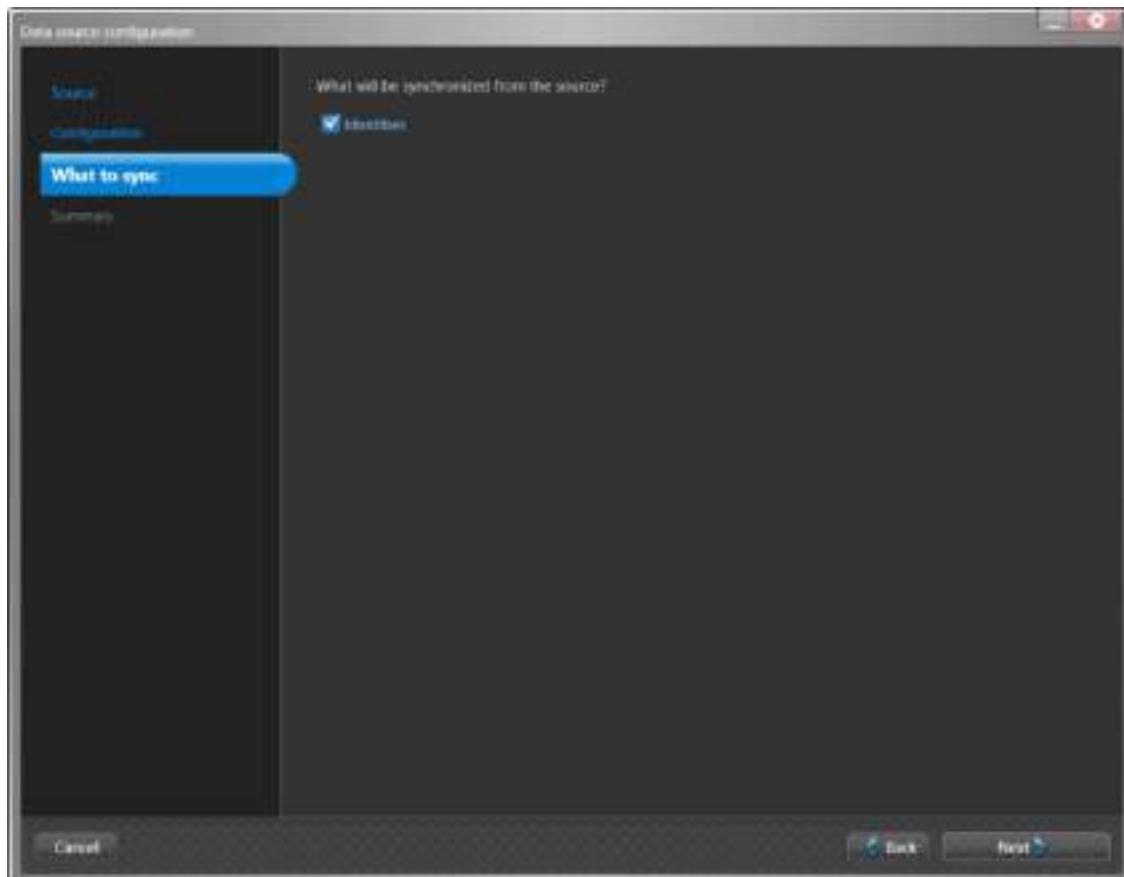
NOTE: Fetching information required for the data source configuration can take a long time and varies depending on the number of groups and users fetched.

- b. (Optional) Use the Filter groups option to only synchronize a subset of selected Azure AD groups and group members. Search for or select the groups that you require and click Next.



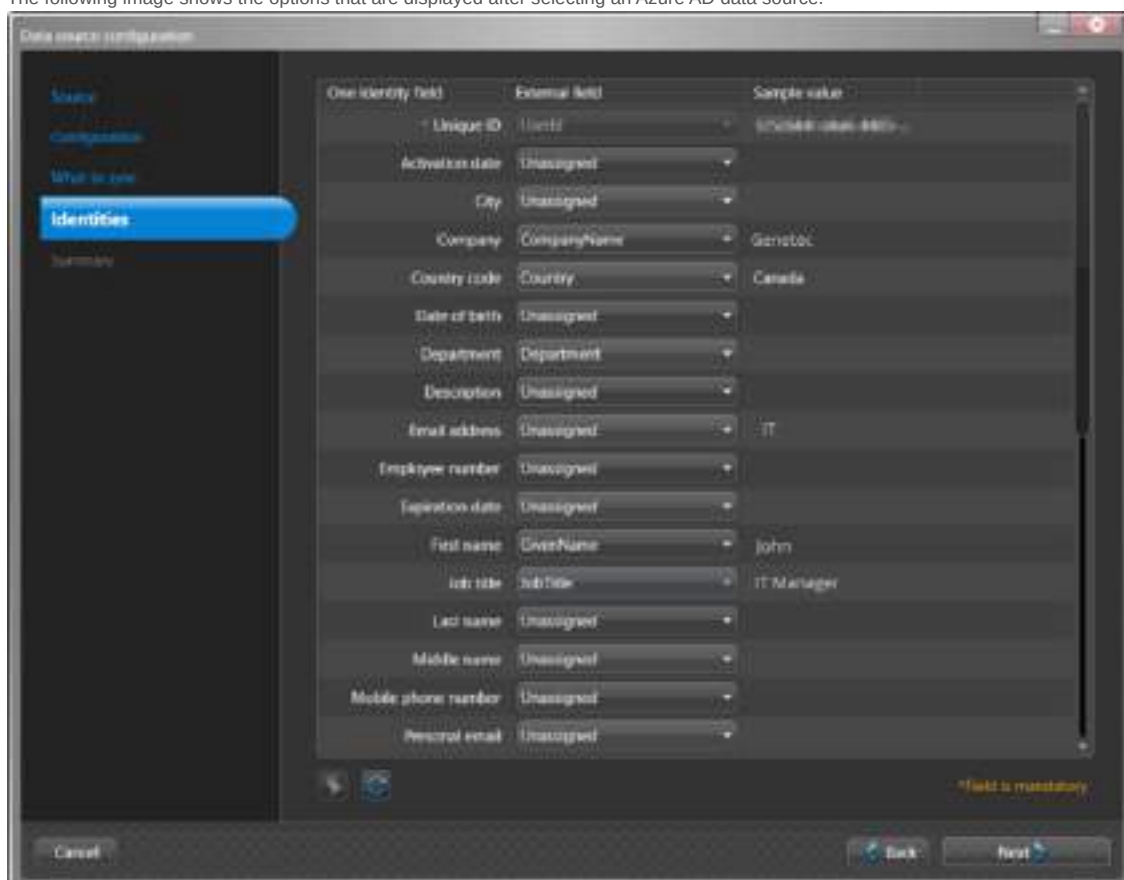
NOTE: If your Azure AD list is long, you can also use the Check all or Uncheck all icon to help you during your selection process.

4. In the What to sync section of the Data source configuration dialog, select Identities to synchronize from the external system data source.



5. If you selected Identities as a data source, in the What to sync section, configure the identity attributes settings.

NOTE: The fields that are displayed in the Identities section vary depending on the data source you selected in the Source section. The following image shows the options that are displayed after selecting an Azure AD data source.



a. Configure your External field attribute mappings.

One Identity field

Displays the ClearID identity attributes. Mandatory fields are highlighted using an asterisk (*).

External Field

Select system attributes in the External field columns that you want to map from the external system to the ClearID identity attributes shown in the One Identity field column.

CAUTION:

When using Azure AD as your data source, the One Identity Unique ID field must be mapped to the Azure AD User ID external field to ensure that the identity attributes are correctly mapped and synchronized.

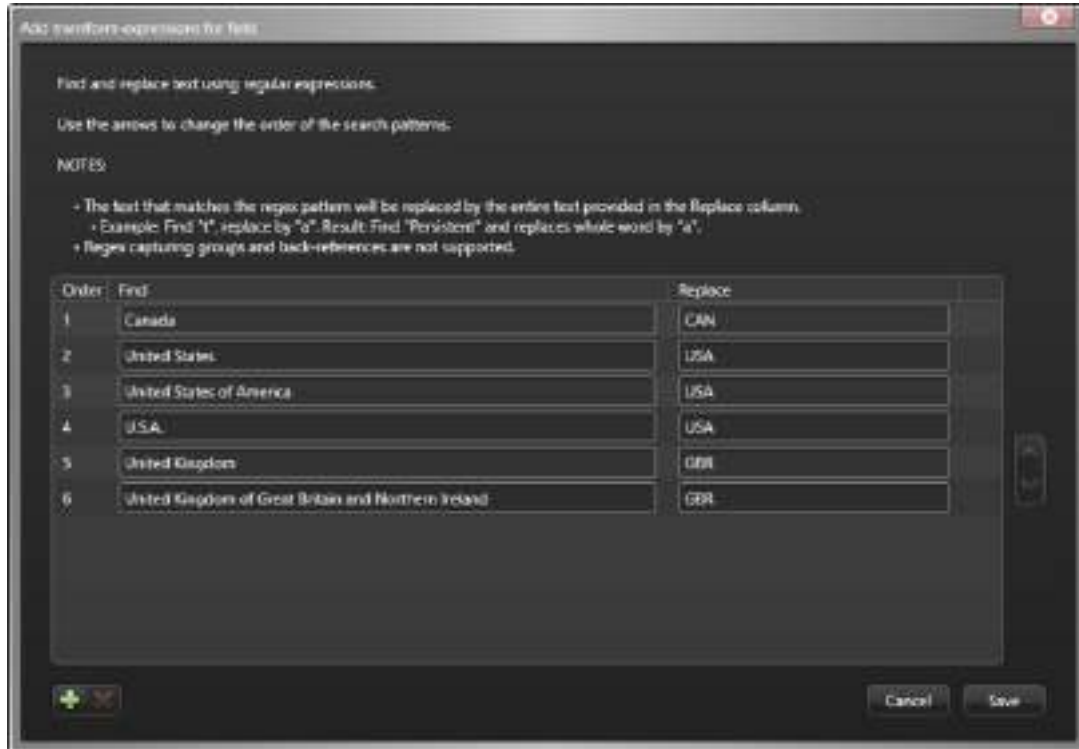
Sample value

If an External field is selected, an example of the selected external field data from your data source is displayed (if available) in the Sample value column next to the External field column.

Tip: Use the sample value column to check the format of the attributes data you are about to import from your external system fields into ClearID.

- b. (Optional) Click Script () to add a transform expression to find and replace external field text using regular expressions.

For example, you can look for variations of a country name to replace with the correct country code.



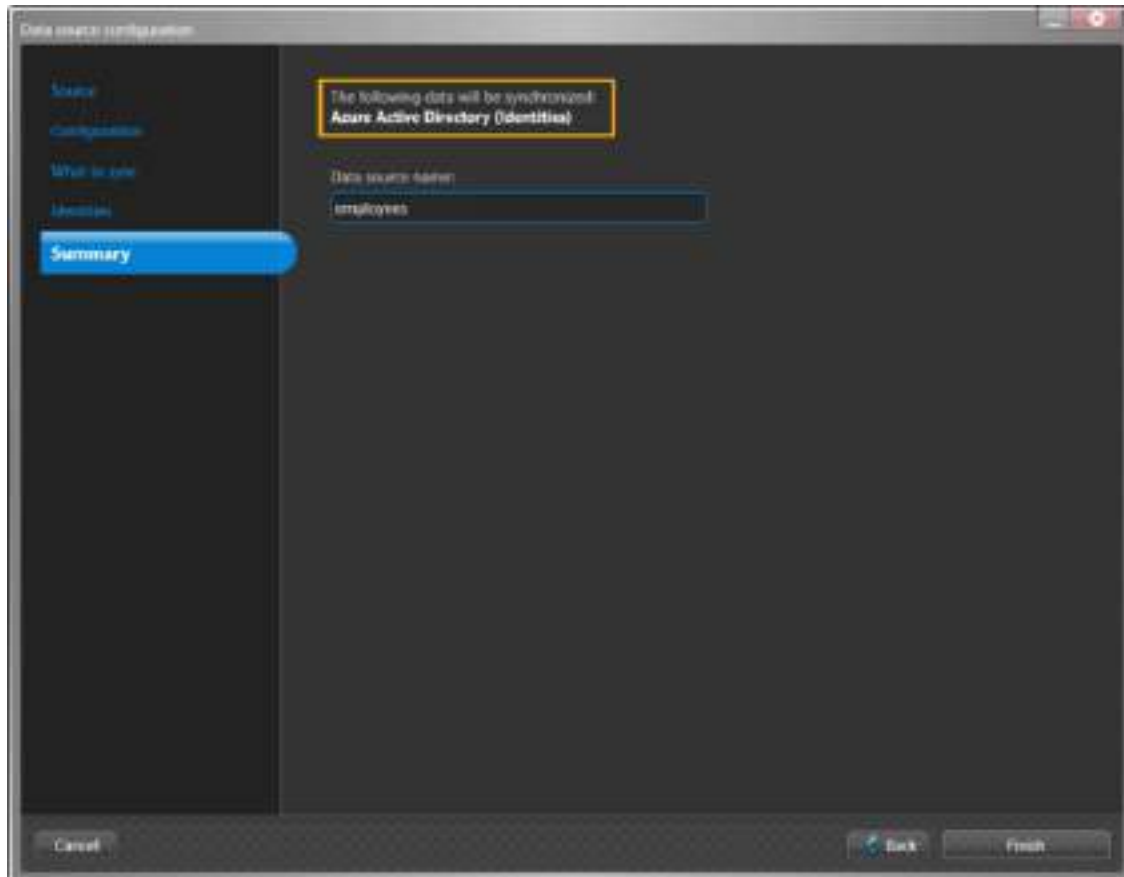
- A script icon () is shown in the Sample value column when the field text is being replaced with a regular expression.
- The transform expressions are processed in the order specified in the Add transform expressions for field dialog.

Tip: If required, you can select the row of any expressions that you no longer require, and click delete (.

- c. (Optional) Click Refresh () to update the external fields data from your data source. This refresh option is used in situations where the existing data has been modified, new data rows have been added, or new attribute columns have been added.

- d. Click Next.

6. In the Summary section, review the data that will be synchronized.



NOTE: If multiple data sources are selected, only the first data source file is displayed in the Summary section Data source name field. If you want each of the data files listed in the Data sources section, you must add them individually.

a. If the data synchronization details look correct, click Finish.

After you finish

Configure your synchronization settings.

Parent topic: [Configuring the ClearID One Identity Synchronization Tool](#)

Browse

- [About ClearID One Identity Synchronization Tool attribute fields](#)

12.5.5.3 | [Configuring the data source for Database synchronization in the ClearID One Identity Synchronization Tool](#)

[Synchronizing identities using One Identity Synchronization Tool in ClearID >](#)

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool data sources for database synchronization.

Before you begin

- [Familiarize yourself with the One Identity attribute fields.](#)
- Prepare a Database containing identities attributes that you want to import and synchronize.
- Check your license information: Part number CD-IDSYNC-SERVICE-1Y is required for One Identity Synchronization Tool import.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

This procedure describes how to configure the data source for a Database (Microsoft SQL Server, Oracle Database, ODBC).

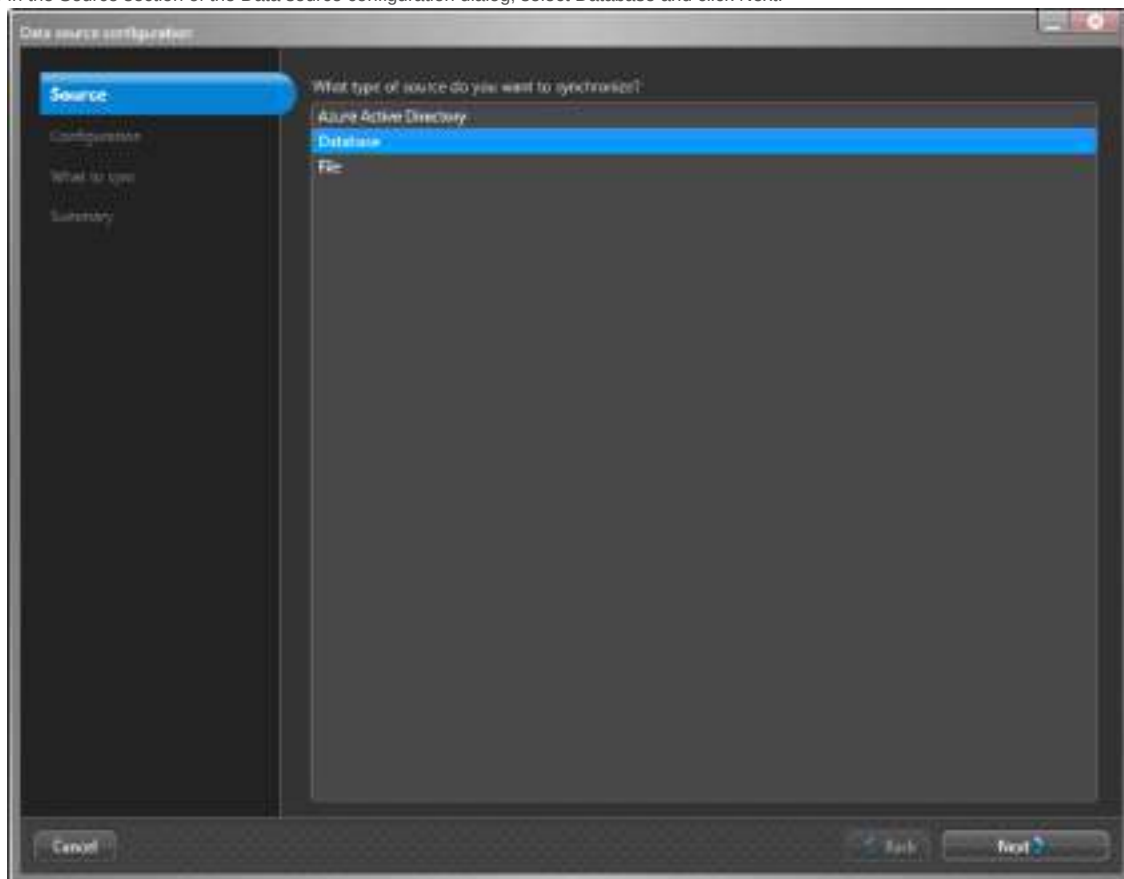
- The data source order is important because the first data source always overrides common fields.
- There is no limit to the number of data sources. However, the larger the data source, the memory requirements increase.

Procedure

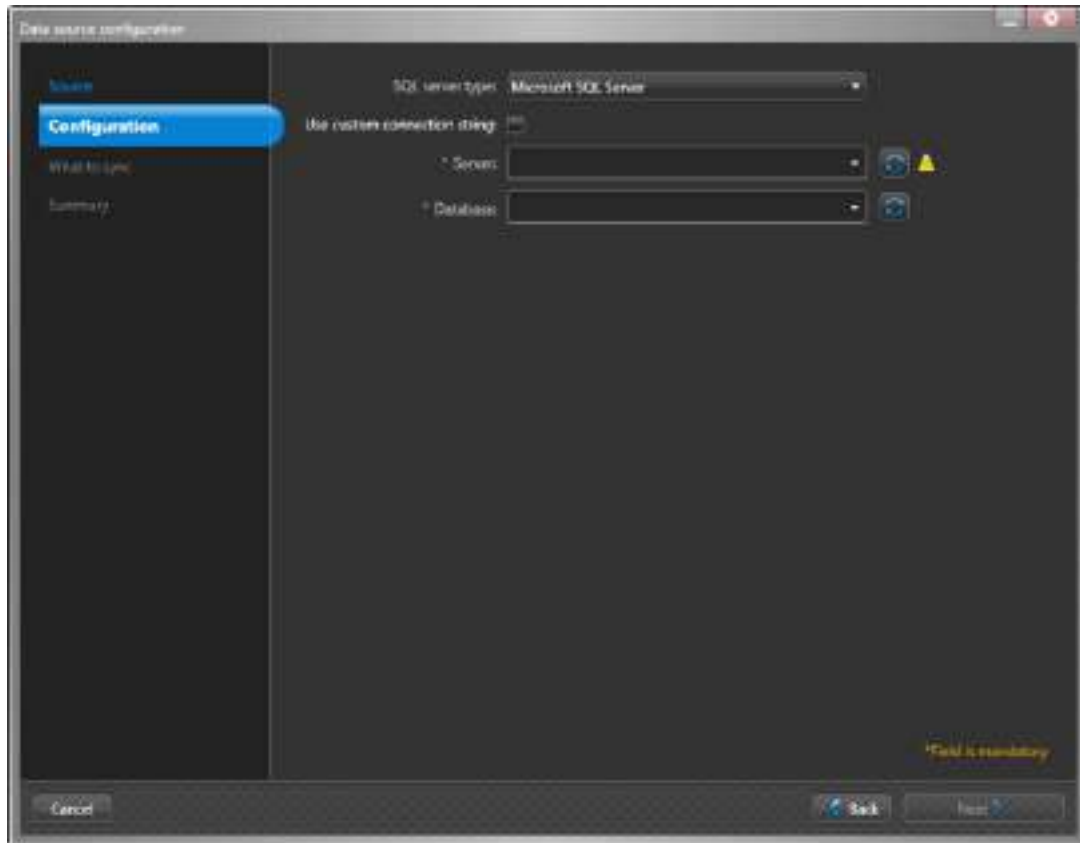
1. In the One Identity Synchronization Tool Data sources section, click Add data source ().



2. In the Source section of the Data source configuration dialog, select Database and click Next.



3. In the Configuration section of the Data source configuration dialog, configure the database settings.
- Select an SQL server type:
 - Microsoft SQL Server
 - Oracle Database (only views are currently supported)
 - ODBC
 - If you selected Microsoft SQL Server, configure the following:



Use custom connection string

Select the checkbox if you want to use a custom connection string.

NOTE: If you use the Use custom connection string option, the Server and Database fields are removed.

Connection string

Enter the connection string.

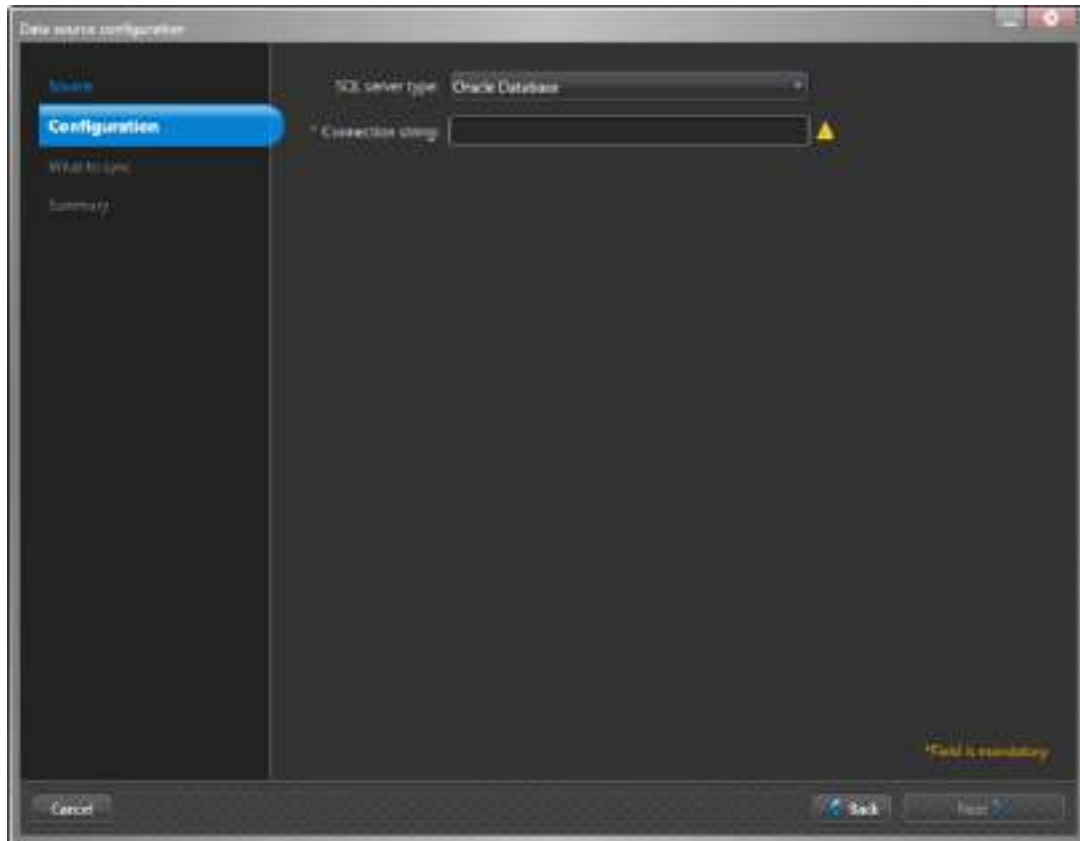
Server

Enter SQL server information or select a server from the list.

Database

Enter Database information or select a database from the list.

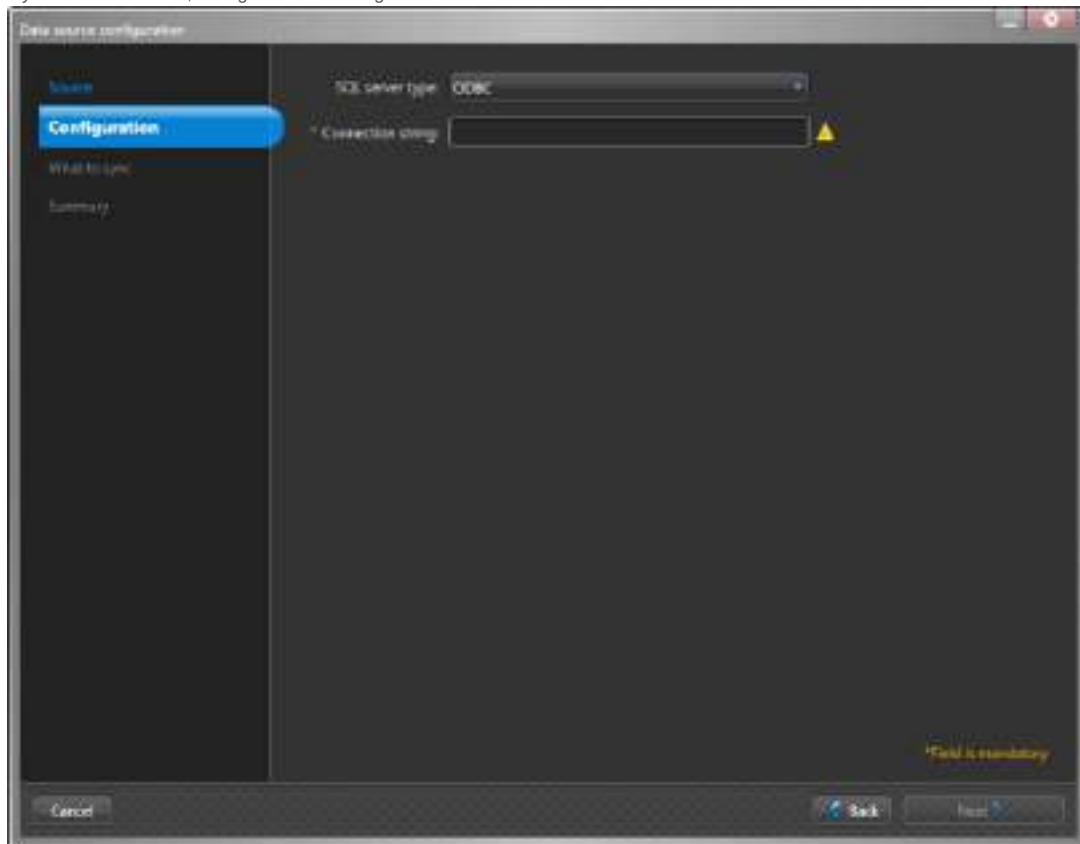
c. If you selected Oracle Database, configure the following:



Connection string

Enter the connection string.

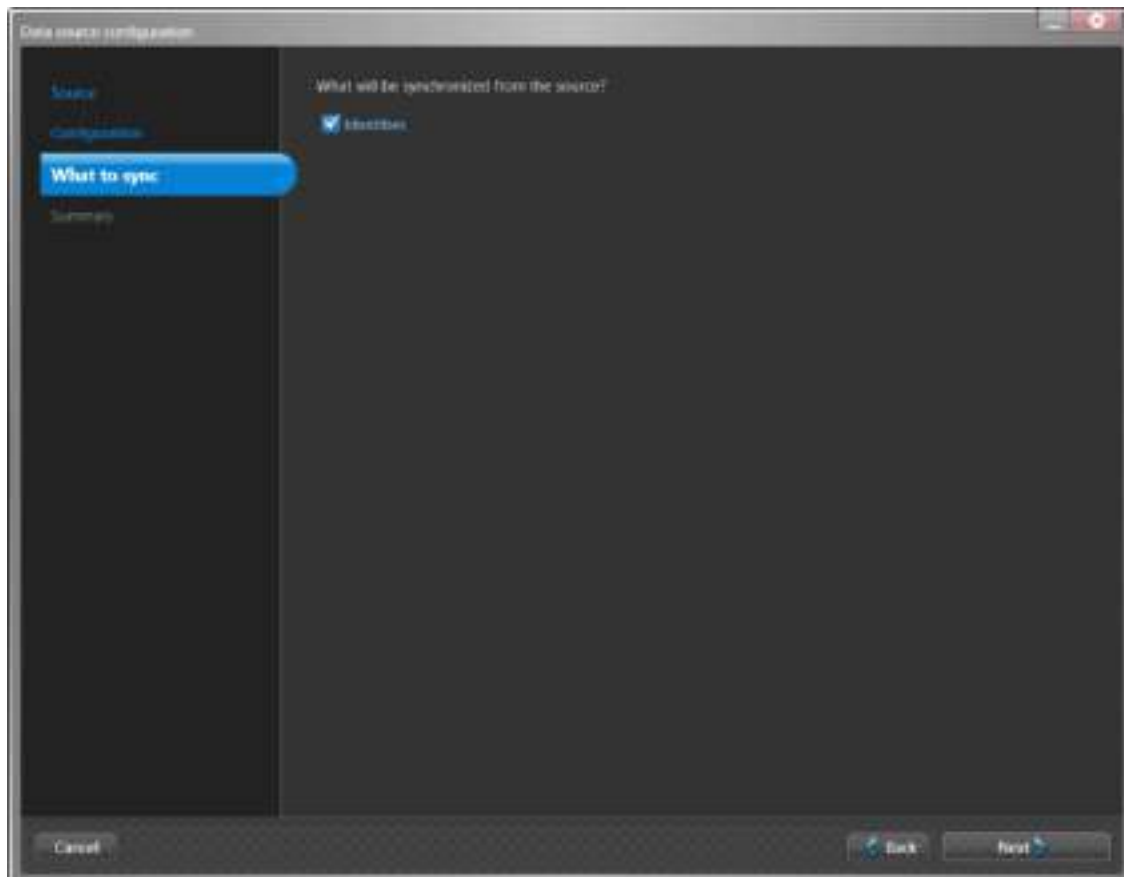
- d. If you selected ODBC, configure the following:



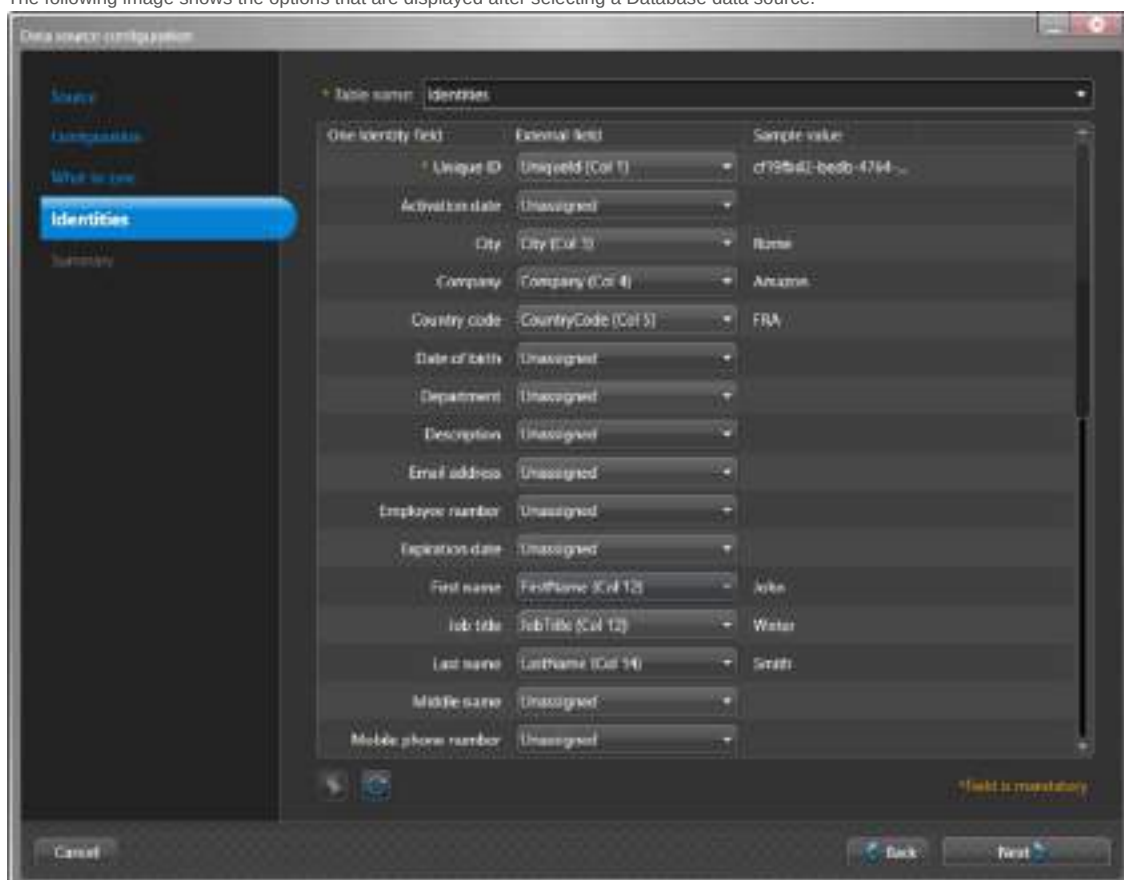
Connection string

Enter the connection string.

4. In the What to sync section of the Data source configuration dialog, select Identities to synchronize from the external system data source.



5. If you selected Identities as a data source, in the What to sync section, configure the identity attributes settings.
NOTE: The fields that are displayed vary depending on the data source you selected in the Source section.
The following image shows the options that are displayed after selecting a Database data source.



- a. Configure your External field attribute mappings.

One Identity field

Displays the ClearID identity attributes. Mandatory fields are highlighted using an asterisk (*).

Genetec ClearID®; User Guide

Displayed in the header

IMPORTANT: The Unique ID is used internally by One Identity as the primary key to identify what it is. For example, an employee number or email address could be used, as long as it is unique.

External Field

Select system attributes in the External field columns that you want to map from the external system to the ClearID identity attributes shown in the One Identity field column.

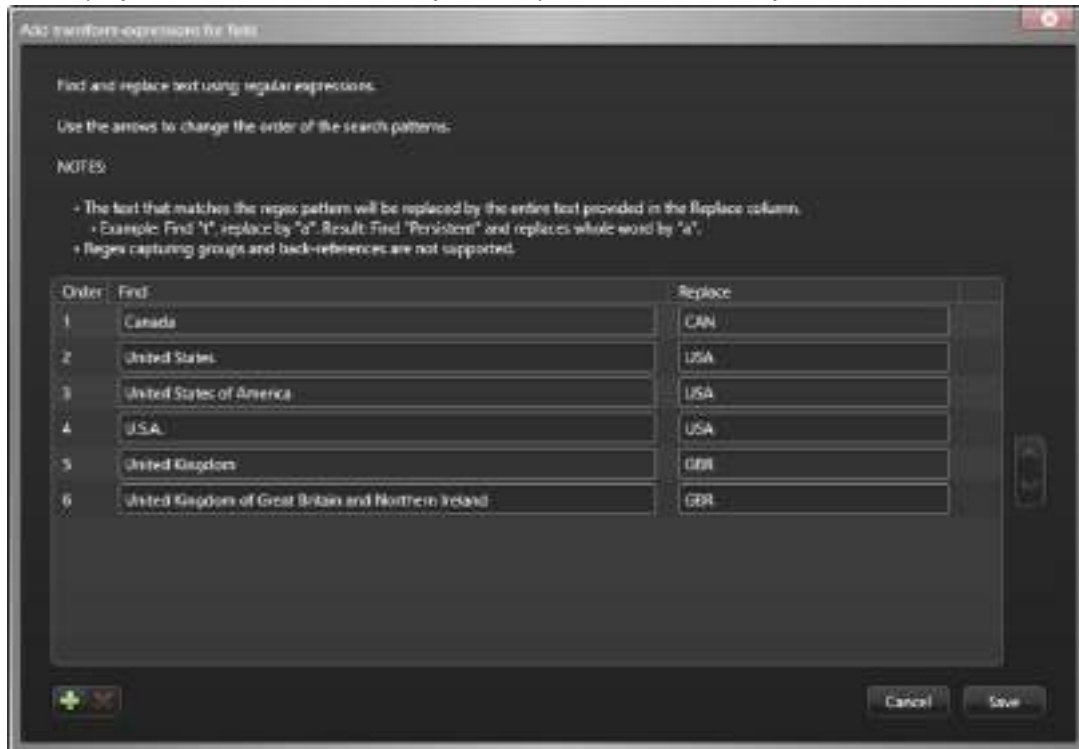
Sample value

If an External field is selected, an example of the selected external field data from your data source is displayed (if available) in the Sample value column next to the External field column.

Tip: Use the sample value column to check the format of the attributes data you are about to import from your external system fields into ClearID.

- b. (Optional) Click Script  to add a transform expression to find and replace external field text using regular expressions.

For example, you can look for variations of a country name to replace with the correct country code.



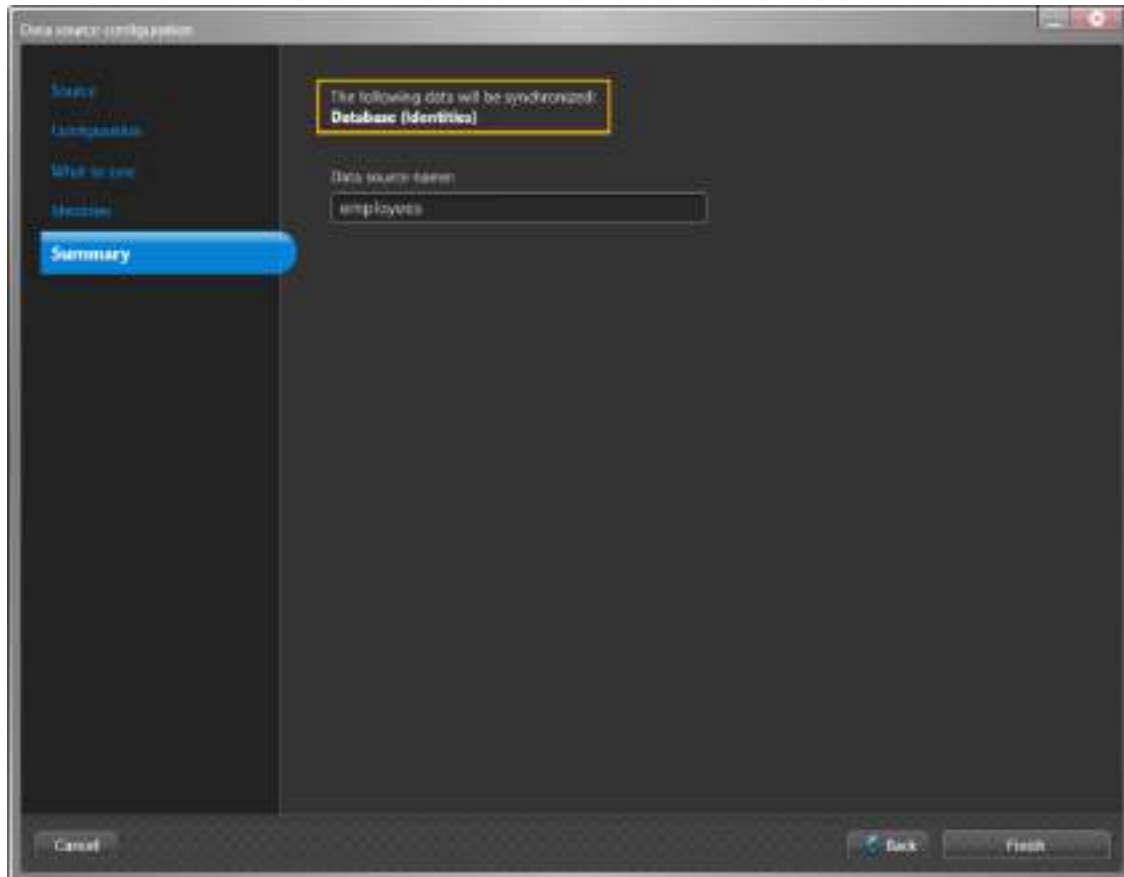
- A script icon  is shown in the Sample value column when the field text is being replaced with a regular expression.
- The transform expressions are processed in the order specified in the Add transform expressions for field dialog.

Tip: If required, you can select the row of any expressions that you no longer require, and click delete .

- c. (Optional) Click Refresh  to update the external fields data from your data source. This refresh option is used in situations where the existing data has been modified, new data rows have been added, or new attribute columns have been added.

- d. Click Next.

6. In the Summary section, review the data that will be synchronized.



NOTE: If multiple data sources are selected, only the first data source file is displayed in the Summary section Data source name field. If you want each of the data files listed in the Data sources section, you must add them individually.

- a. If the data synchronization details look correct, click Finish.

After you finish

Configure your synchronization settings.

Parent topic: [Configuring the ClearID One Identity Synchronization Tool](#)

Browse

- [About ClearID One Identity Synchronization Tool attribute fields](#)

12.5.5.4 | [Configuring the data source for File synchronization in the ClearID One Identity Synchronization Tool](#)

[Synchronizing identities using One Identity Synchronization Tool in ClearID](#) >

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool data sources for file (CSV) Synchronization.

Before you begin

- [Familiarize yourself with the One Identity attribute fields.](#)
- Prepare a CSV file containing the identities attributes that you want to import and synchronize.
- Check your license information: Part number CD-IDSYNC-SERVICE-1Y is required for One Identity Synchronization Tool import.

IMPORTANT: Make sure that your CSV files are not being edited and are closed, because the synchronization tool locks the files during the synchronization process.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

This procedure describes how to configure the data source for a File (CSV import).

- The data source order is important because the first data source always overrides common fields.
- One data source can include multiple CSV files containing identities.
- There is no limit to the number of data sources. However, the larger the data source (not only CSV files), the memory requirements increase.

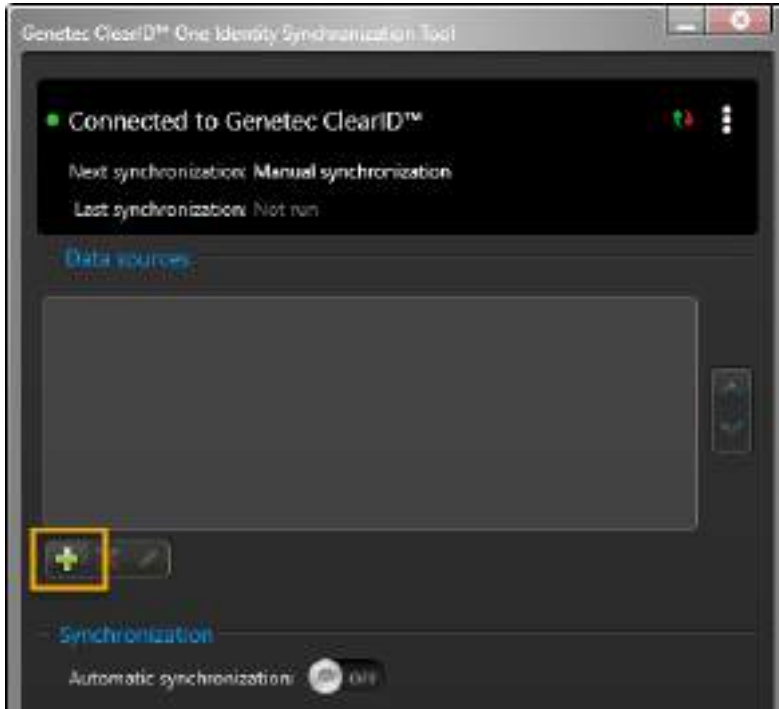
Genetec ClearID™ User Guide

Displayed in the header

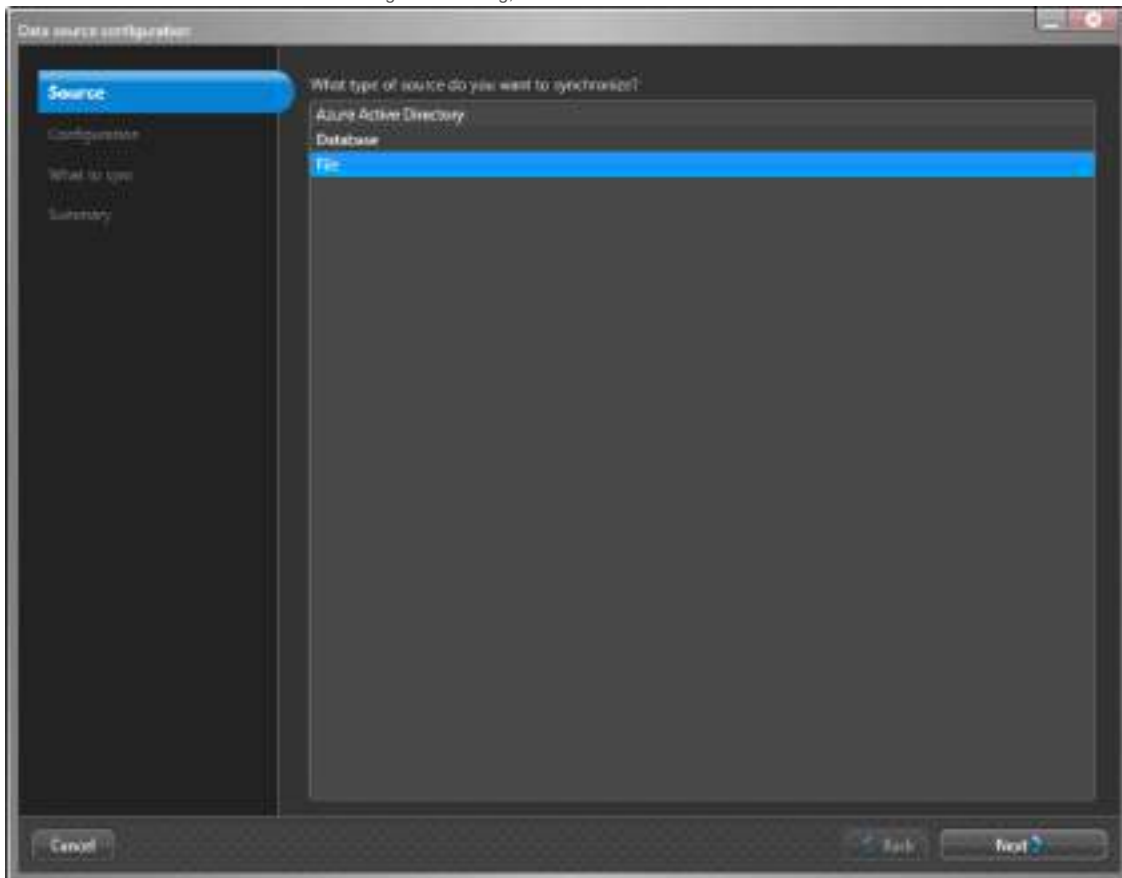
Best Practice: To avoid user permission issues when using CSV files with the ClearID One Identity Synchronization Tool, save them to a C: or C:\temp folder location. Do not save CSV files in a user-controlled file or folder locations (C:\Users folders or desktop folder location) or you might encounter File path is not valid user permissions issues.

Procedure

1. In the One Identity Synchronization Tool Data sources section, click Add data source .

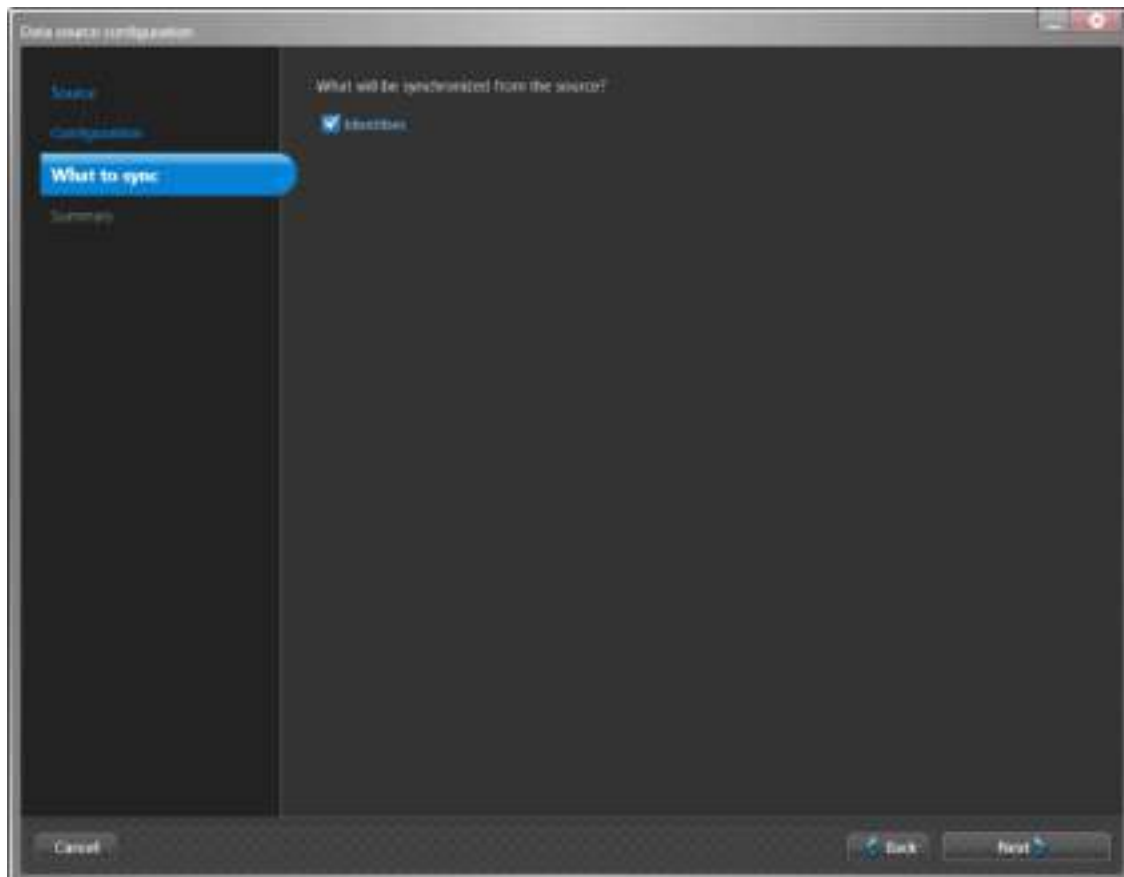


2. In the Source section of the Data source configuration dialog, select File and click Next.

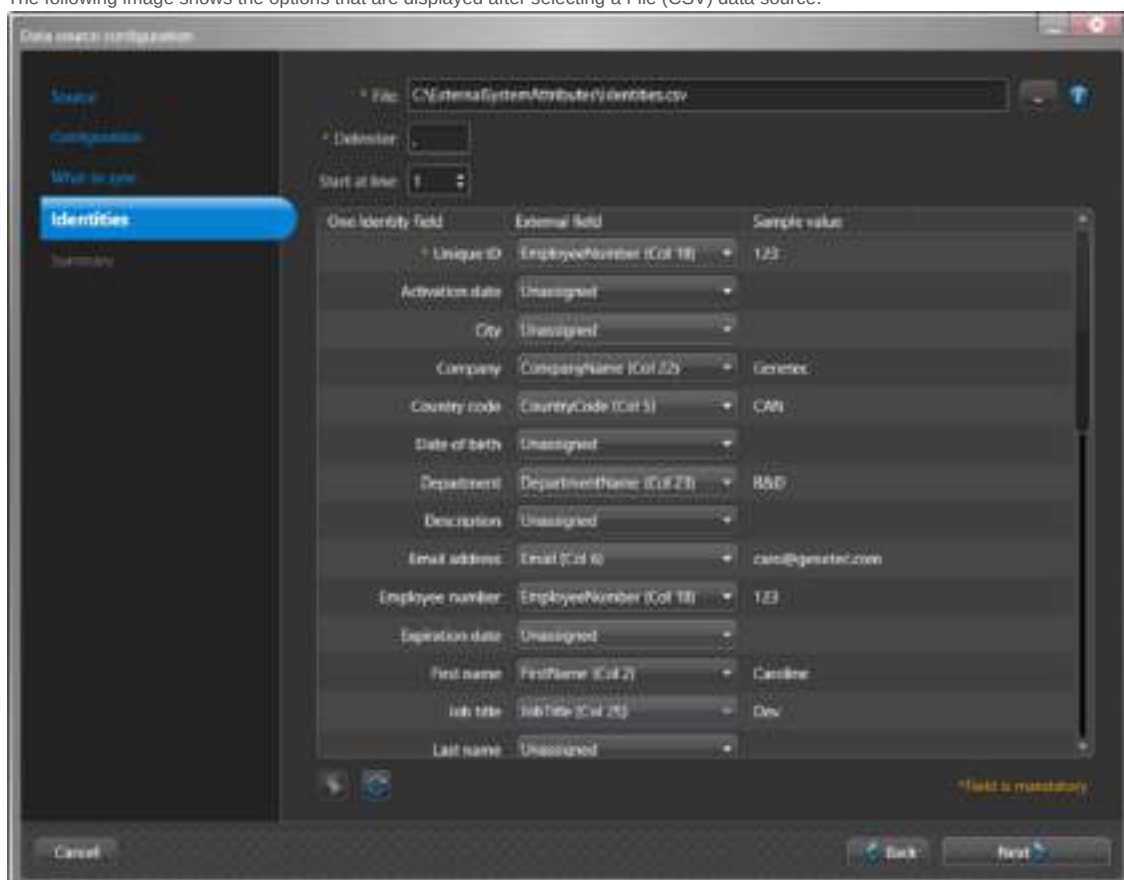


NOTE: If you selected File in the Source section, the Configuration section of the Data source configuration dialog is skipped because it is not required.

3. In the What to sync section of the Data source configuration dialog, select Identities to synchronize from the external system data source.



4. If you selected Identities as a data source, in the What to sync section, configure the identity attributes settings.
- NOTE: The fields that are displayed vary depending on the data source selected in the Source section (step 2) earlier. The following image shows the options that are displayed after selecting a File (CSV) data source.



- a. If you selected File as your data source, configure the file settings.

File

Click More (⋮) to select the CSV file containing your attributes.

NOTE: The file path must exist on the server where the One Identity Configuration Tool is installed.

Delimiter

Enter a Delimiter value.

For example, for a CSV file it is a comma-separated value (CSV).

Start at line

Select a Start at line.

For example, the data in a table with no headings might start at line 0, whereas the data in a table with headings might start at line 1.

b. Configure your External field attribute mappings.

One Identity field

Displays the ClearID identity attributes. Mandatory fields are highlighted using an asterisk (*).

IMPORTANT: The Unique ID is used internally by One Identity as the primary key to identify what it is. For example, an employee number or email address could be used, as long as it is unique.

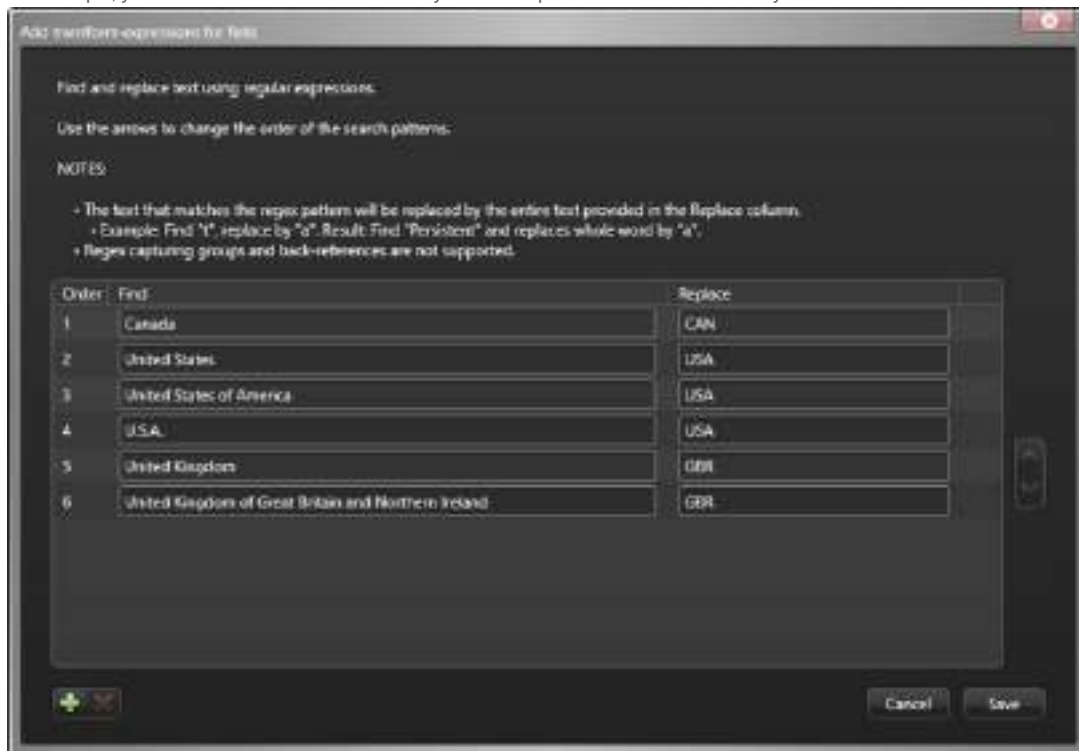
External Field

Select system attributes in the External field columns that you want to map from the external system to the ClearID identity attributes shown in the One Identity field column.

- If your CSV file contains column titles, the names are displayed.
- If your CSV file does not contain column titles, the column number is displayed.

c. (Optional) Click Script  to add a transform expression to find and replace external field text using regular expressions.

For example, you can look for variations of a country name to replace with the correct country code.



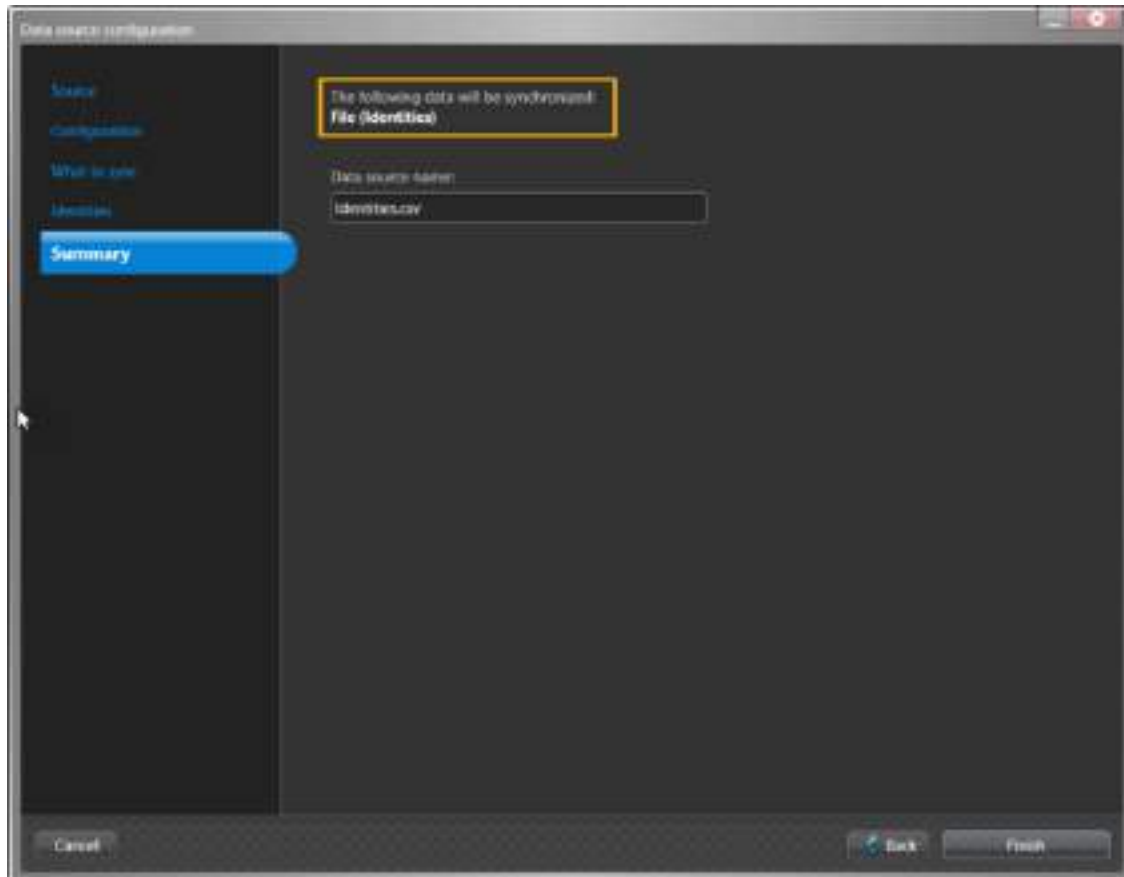
- A script icon  is shown in the Sample value column when the field text is being replaced with a regular expression.
- The transform expressions are processed in the order specified in the Add transform expressions for field dialog.

Tip: If required, you can select the row of any expressions that you no longer require, and click delete .

d. (Optional) Click Refresh  to update the external fields data from your data source. This refresh option is used in situations where the existing data has been modified, new data rows have been added, or new attribute columns have been added.

e. Click Next.

5. In the Summary section, review the data that will be synchronized.



NOTE: If multiple data sources are selected, only the first data source file is displayed in the Summary section Data source name field. If you want each of the data files listed in the Data sources section, you must add them individually.

- If the data synchronization details look correct, click Finish.

After you finish

Configure your synchronization settings.

Parent topic: [Configuring the ClearID One Identity Synchronization Tool](#)

Browse

- [About ClearID One Identity Synchronization Tool attribute fields](#)

12.5.5.5 | Configuring synchronization settings in the ClearID One Identity Synchronization Tool

[Synchronizing identities using One Identity Synchronization Tool in ClearID >](#)

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool synchronization settings.

Before you begin

- Check your license information: Part number CD-IDSYNC-SERVICE-1Y is required for One Identity Synchronization Tool import.

IMPORTANT: Make sure that your files are not being edited and are closed, because the synchronization tool locks the file during the synchronization process.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

Synchronization can be performed manually using the Synchronize now () option, or automatically at the Automatic synchronization intervals specified in the One Identity Synchronization Tool.

Synchronization of external system attributes into ClearID identity attributes is INBOUND only.

CAUTION:

Any changes only made to identities in ClearID can be overwritten during the next synchronization from the external system.

Procedure

1. In the One Identity Synchronization Tool Synchronization section, configure your synchronization settings.



Automatic synchronization

Enable automatic synchronization if you want attributes synchronized at a specified interval.

Interval

If automatic synchronization is enabled, choose a synchronization interval:

Fixed

Enter a Synchronization interval using the following format: 000d 01h 00m 00s.

For example, every 7 days would be 007d 00h 00m 00s, or every 12hrs 000d 12h 00m 00s.

Cron Schedule

Enter a synchronization interval using the Quartz Cron format. For example, 00***?*

For more information, see quartz-scheduler.org/documentation.

Tip: You can click Synchronize now () regardless of any scheduled settings to initiate an immediate synchronization.

Synchronize picture

Choose when to synchronize identity pictures from the external system.

Always

Identity pictures are synchronized every time a synchronization occurs.

Only if missing

Identity pictures are only synchronized when a synchronization occurs, if they are missing.

NOTE: Including pictures increases the amount of time that it takes to import attributes.

Stop Synchronization on error

Enable this option to stop synchronization if an error is encountered during the synchronization process.

Default web portal access

Specifies web portal access for synchronized users.

Grant access

ClearID web portal access for synchronized users is enabled by default.

NOTE: The username field must be mapped to give web portal access to a ClearID identity.

- There are only two possible values for the User type mapping: Admin and User. Any other value entered defaults to User.
- If the mapping for web portal access is not set, or the value is empty, the Default web portal access global setting is used.

No access

Web portal access for synchronized users is disabled by default.

Default country

Choose one of the following:

No default country

If a synchronized identity does not include a country attribute, the country attribute is ignored.

Default country

Select a default country. If a synchronized identity does not include a country attribute, the synchronized identity uses the default country specified here.

2. Click Save.

Results

The ClearID One Identity Synchronization Tool is now configured to synchronize attributes from the external system using the Data sources and Synchronization settings specified in the tool.

After you finish

After the synchronization has occurred, verify that the new attributes from the external system have been synchronized and contain the correct attributes.

Parent topic: [Configuring the ClearID One Identity Synchronization Tool](#)

12.5.6 | Reviewing synchronization status for the ClearID One Identity Synchronization Tool

To check that your identity attributes were synchronized into Genetec ClearID™ correctly, you can review the synchronization status in the Genetec ClearID™ One Identity Synchronization Tool or the ClearID web portal.

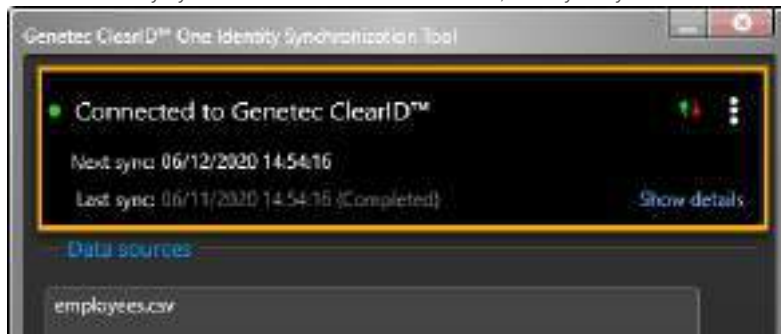
Before you begin

- [Configure the One Identity Synchronization Tool](#).
- Perform a manual or automatic synchronization using the One Identity Synchronization Tool.

Procedure

To review your attribute synchronization status in the One Identity Configuration Tool:

1. In the One Identity Synchronization Tool connection section, check your synchronization status.



Next sync

Displays information about the next synchronization.

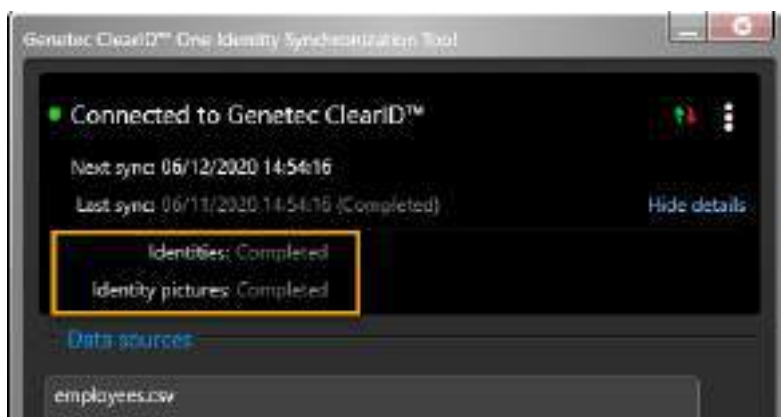
- If a date is displayed 06/16/2020 23:00:00, this date indicates the Fixed or Cron schedule interval when the next synchronization is scheduled to occur.
- If Manual synchronization is displayed, the synchronization must be performed manually.

Last sync

Displays information about the last synchronization.

Show details

Click Show details, to check the status of synchronization for Identities and Identity pictures.



NOTE: If there is an issue with any of the synchronizations, a Failed message is displayed next to the failing synchronization.

2. (Optional) Review summary logs.

- a. Click  then click Open logs folder.
- b. Review CSV-formatted Summary logs to identify any issues that might occur during synchronization.
- c. Read the overview Recap.txt file for a quick synchronization overview.

NOTE: The summary log files are saved in C:\ProgramData\Genetec\OneIdentity\Logs\Summary.

To review your attributes synchronization status in the ClearID web portal:

1. In the ClearID web portal, check to verify that the new attributes from the external system have been synchronized and contain the correct attributes.

- a. Click Organization > Identities and verify that your synchronized identity data is correct.

Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.7 | About ClearID One Identity Synchronization Tool logs

The Genetec ClearID™ One Identity Synchronization Tool includes logs that can be used for troubleshooting. The logs can be used to check the status of the configuration tool, the windows service, or review synchronization activities.

The ClearID One Identity Synchronization Tool uses the industry-standard Apache log4net™ framework for logging.

The logging configuration can be changed for both the synchronization service and the synchronization tool.

- To change the Genetec.ClearID.OneIdentity.SynchronizationService (OneIdentityService.exe) logging configuration, you can modify the `log4net.service.config` file.
- To change the Genetec.ClearID.OneIdentity.SynchronizationTool (OneIdentityConfigurationTool.exe) logging configuration, you can modify the `log4net.ct.config` file.

These log configuration files are found in the installation folder `C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service .`

The default settings are as follows:

- Log level is WARN.
- File size before rolling is 10Mb.
- Max rolling backups is 10.

For more information about the supported values and how to change them, see the [Apache log4net](#) documentation.

Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.8 | Viewing the ClearID One Identity Synchronization Tool logs

You can use the Genetec ClearID™ One Identity Synchronization Tool logs to check the status of the configuration tool, the windows service, or review synchronization activities.

Before you begin

- [Configuring the ClearID One Identity Synchronization Tool](#)
- [Configuring synchronization settings in the ClearID One Identity Synchronization Tool](#)

What you should know

Logs are subdivided into three separate folders as follows:

Configuration

Logs related to the *Genetec ClearID™ One Identity Synchronization Tool (OneIdentityConfigurationTool.exe)*.

Service

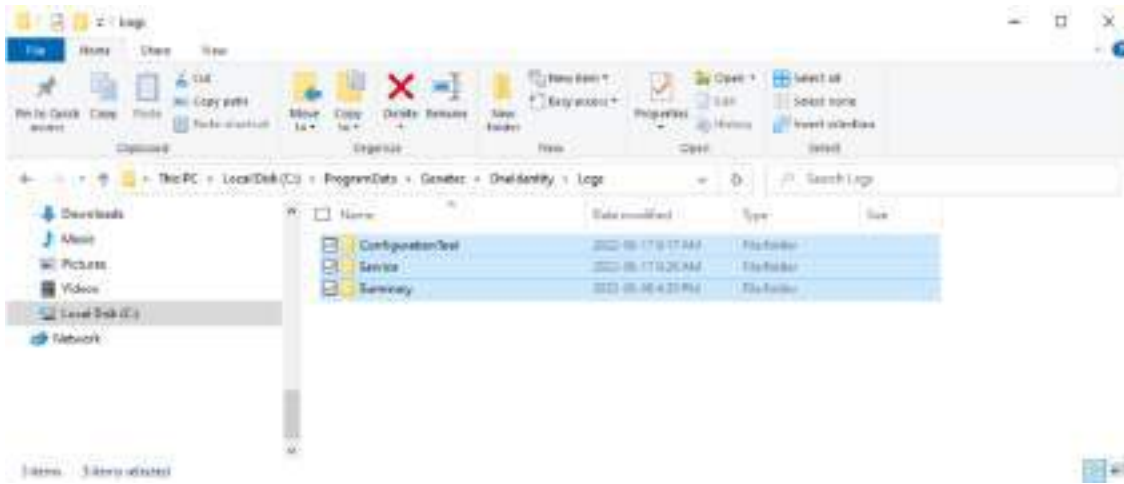
Logs related to the *Genetec.ClearID.OneIdentity.SynchronizationService (OneIdentityService.exe)*.

Summary

Logs related to synchronization summaries.

Procedure

1. Click  then click Open logs folder.



2. Review the ConfigurationTool logs if you are having connectivity issues. For example, if the synchronization tool is unable to connect to ClearID or unable to connect to Azure AD.
3. Review the Service logs if you are having data synchronization issues. For example, missing data fields, missing name fields, or missing email addresses.
4. Review the Summary logs to see a summary of synchronization activities. For example, when a synchronization started or ended and what occurred during the synchronization.
 - a. Read the Recap.txt file for a quick synchronization overview.

NOTE: The summary log files are CSV-formatted files to facilitate sorting information in Microsoft® Excel if required. They are automatically generated at the end of the synchronization.

- o If the synchronization completely fails, the summary log files are not generated.
- o If there is nothing to import, the summary log files are not created.

Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.9 | Updating existing identities from an external data source using ClearID One Identity Synchronization Tool

When users that have already been created have the same external ID as existing users, you can use Genetec ClearID™ One Identity Synchronization Tool to update the existing identities information from an external data source.

What you should know

This procedure is relevant for newly installed ClearID One Identity Synchronization Tool service when the Genetec ClearID™ environment already contains identities that are also present in the external system data source.

- When an external ID already exists in ClearID, that identity is updated with the values provided in the data sources.
- When an identity from the data source does not exist in One Identity (for example, on the first synchronization), the service tries to create the identity in ClearID.
- When the creation fails because the identity already exists, that identity is then fetched and updated.

Procedure

1. To reproduce a newly installed service, delete the file mappings under %ProgramData%\Genetec\OneIdentity\Configuration.
2. Configure a data source that already contains one or more identities that are present in ClearID.

The identities in the data source should have the same external ID and email as the identities in ClearID.
3. Start the synchronization and wait for completion.

Results

The identities in ClearID are updated with the mappings from the data source.

Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.6 | Synchronizing identities using LDAP in ClearID

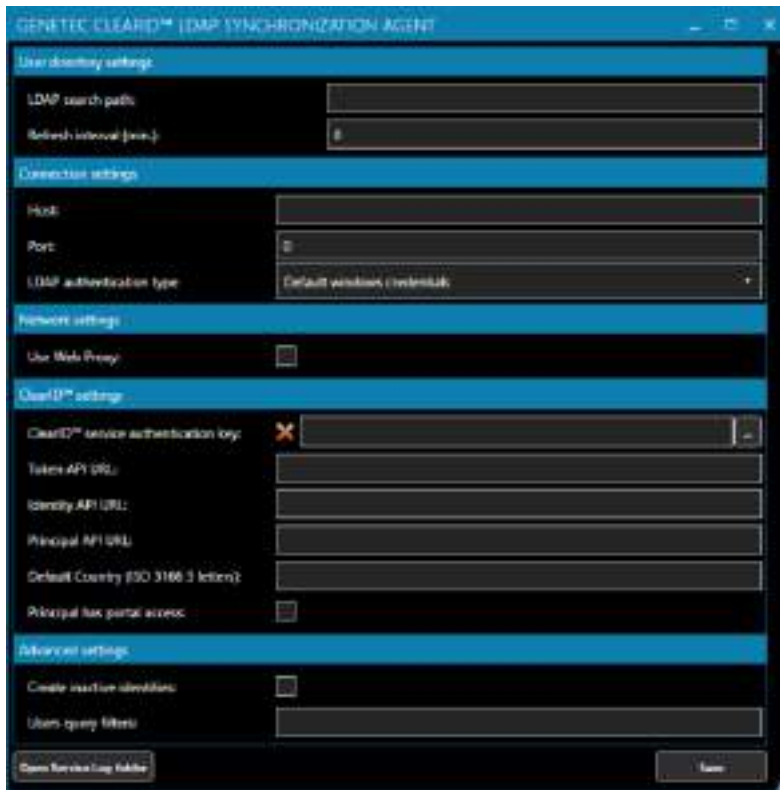
Use the Genetec ClearID™ LDAP Synchronization Agent to synchronize Active Directory (AD) Lightweight Directory Access Protocol (LDAP) attributes into Genetec ClearID™ identity attributes. These identity attributes in ClearID can then be used to assign people to roles and automate role-based access control.

Procedure

1. [Learn about the Genetec ClearID™ LDAP Synchronization Agent.](#)
2. [Learn about LDAP attributes to ClearID attribute mappings.](#)
3. [Configure the Genetec ClearID™ LDAP Synchronization Agent.](#)

12.6.1 | About ClearID LDAP Synchronization Agent

The Genetec ClearID™ LDAP Synchronization Agent is a Windows application that is used to synchronize Active Directory (AD) Lightweight Directory Access Protocol (LDAP) attributes into Genetec ClearID™ identity attributes.



The ClearID LDAP Synchronization Agent application includes the following components:

- Konfigurator (Genetec.ClearID.LdapSyncAgentConfiguration.exe) is the user interface component of the windows application that is used to configure the synchronization agent.
- Genetec ClearID LDAP Synchronizer (Genetec.ClearID.LdapSyncAgent.Service.exe) is the Windows service component of the application that performs Active Directory LDAP attributes to Genetec ClearID™ identity attributes synchronization automatically in the background at intervals specified in the Synchronization Agent.

The ClearID LDAP Synchronization Agent application is intended for use by IT or security personnel responsible for Active Directory (AD) administration.

Synchronization

Identities in ClearID can come from a variety of data sources (Databases, HR, External Sources) and can be synchronized using various tools (Genetec ClearID™ LDAP Synchronization Agent, Genetec ClearID™ API, or Genetec ClearID™ One Identity Synchronization Tool).

The following information describes Active Directory LDAP synchronization:

- Synchronization of LDAP attributes into ClearID identity attributes is INBOUND only.
CAUTION:
Any changes only made to identities in ClearID can be overwritten by the next synchronization from the Active Directory.
- Synchronization occurs automatically at the intervals specified in the ClearID LDAP Synchronization Agent.
 - The *whenChanged* attribute indicates the last time that a synchronization occurred. This attribute is then used to query Active Directory users that have changed since the last synchronization so that only changed users are updated when the next synchronization occurs.
 - The first time a synchronization occurs, all Active Directory user attributes are synchronized.
 - The next time a synchronization occurs, only Active Directory user attributes that have changed since the last time the agent ran are synchronized.

Parent topic: Synchronizing identities using LDAP in ClearID

12.6.2 | LDAP attributes to ClearID attribute mappings

When you synchronize an Active Directory (AD) with Genetec ClearID™ using the ClearID LDAP Agent Configurator, Lightweight Directory Access Protocol (LDAP) attributes are mapped to ClearID identity attributes.

LDAP attributes to ClearID attribute mappings

LDAP attributes	ClearID identity attributes
whenChanged IMPORTANT: The <i>whenChanged</i> attribute indicates the last time a synchronization with the ClearID LDAP Synchronization Agent occurred. This attribute is then used to query Active Directory users that have changed since the last synchronization so that only changed users are updated when the next synchronization occurs.	Not applicable
userAccountControl	Status NOTE: The ClearID <i>Status</i> attribute is set to inactive if the Active Directory attribute <i>userAccountControl</i> is set to disabled.
givenName	FirstName
sn	LastName
displayName	DisplayName
jpegPhoto	NOTE: <i>jpegPhoto</i> is used to upload a picture into the ClearID identity.
thumbnailPhoto (fallback if jpegPhoto is empty)	NOTE: <i>thumbnailPhoto</i> is used as a fallback (if jpegPhoto is empty) to upload a picture into the ClearID identity.
countryCode	CountryCode
employeeID	EmployeeNumber
employeeNumber (fallback if employeeID is empty)	EmployeeNumber
title	JobTitle
telephoneNumber	PhoneNumberPrimary
phone	PhoneNumberSecondary
Mobile (fallback if phone is empty)	PhoneNumberSecondary
department	DepartmentName
company	CompanyName
userPrincipalName NOTE: The <i>userPrincipalName</i> attribute is used as the link between the AD user and the ClearID identity.	Email, ExternalId
manager	SupervisorName
mail	Email

Parent topic: [Synchronizing identities using LDAP in ClearID](#)

12.6.3 | Configuring the ClearID LDAP Synchronization Agent

Before you can synchronize an Active Directory (AD) with Genetec ClearID™, you must first configure the Genetec ClearID™ LDAP Synchronization Agent.

Before you begin

- Download a service authentication key.
- Install the ClearID LDAP Synchronization Agent on its own dedicated server. It does not require a Security Center server.
NOTE: The ClearID LDAP Synchronization Agent is not generally available as a public download. The synchronizer download is supplied by your Deployment contact when needed.
- Part number: CD-IDSYNC-SERVICE-1Y is required for LDAP import.

What you should know

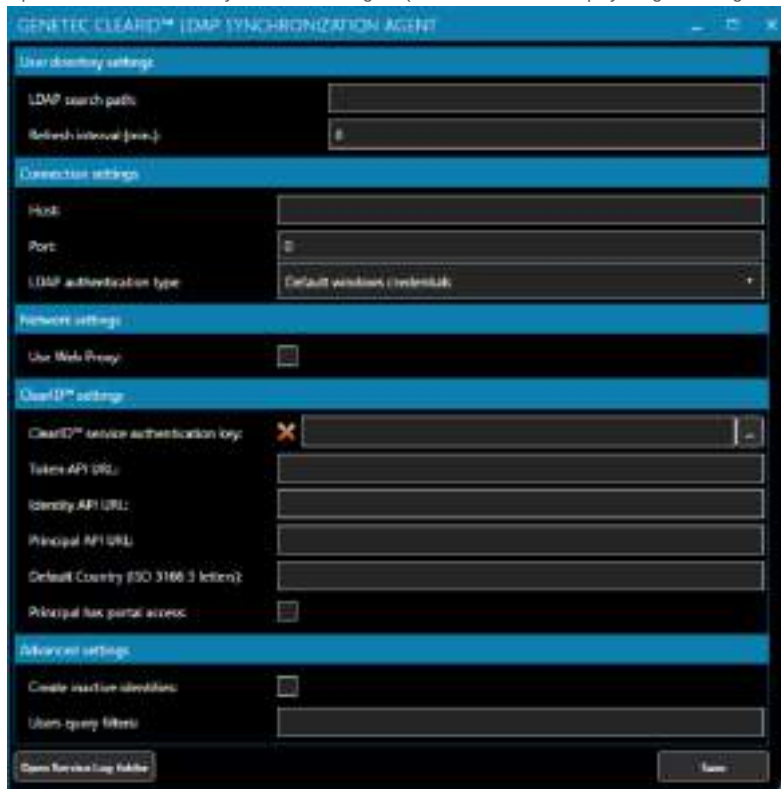
This procedure is for IT or security personnel responsible for Active Directory (AD) administration.
Synchronization of LDAP attributes into ClearID identity attributes is INBOUND only.

CAUTION:

Any changes only made to identities in ClearID can be overwritten by the next synchronization from the Active Directory.

Procedure

1. Open the ClearID LDAP Synchronization Agent (Genetec.ClearID.LdapSyncAgentConfiguration.exe) and configure your settings.



2. In the User directory settings section, enter your user directory details:

The User directory settings section is used to connect to the LDAP directory containing user attributes.

LDAP search path

Enter your organizational unit. For example, OU=Genetec. This search path specifies the location, root folder, or group containing Active Directory user attributes.

NOTE: The distinguishedName of the AD group is required for the LDAP search path field.

Refresh interval (min.)

Enter a refresh interval in minutes. For example, 60 to synchronize attributes every hour.

NOTE: Depending on the size of your organization and the number of attributes, *12hr.* or *24hr.* synchronizations (720 or 1440 mins) might be more appropriate.

3. In the Connection settings section, configure the host connection settings:

The Connection settings section is used to connect to the server where the User Directory settings are stored.

Host

Enter the address of your Active Directory. For example, Genetec.com.

Port

Enter the default port for your Active Directory. For example, 389.

LDAP authentication type

Select an authentication type from the following:

Genetec ClearID®; User Guide

Displayed in the header

Default windows credentials

For a client-side application, this option uses the Windows credentials (*username* and *password*) of the user running the application.

Simple bind

With the Simple bind option, the credentials (*username* and *password*) used to bind the LDAP client to the LDAP server are passed over the network unencrypted.

CAUTION:

Simple bind authentication type is not recommended in production LDAP servers.

Simple bind over SSL

Best Practice: With the Simple bind over SSL option, the credentials (*username* and *password*) used to bind the LDAP client to the LDAP server are passed over the network encrypted.

Username

If Simple bind or Simple bind over SSL was selected, enter the *username* supplied by your organization.

Password

If Simple bind or Simple bind over SSL was selected, click Set password and enter a password, then click OK.

NOTE: Use industry best practices for creating strong passwords. All passwords stored in the configuration file are encrypted.

4. (Optional) In the Network settings section, configure the Web proxy settings:

The Network settings section is used to configure proxy settings.

Use Web Proxy

Select the Use Web Proxy checkbox to specify that a proxy server is required to access the internet.

This option is typically used by customers behind a firewall or where network access to the internet is restricted.

A proxy server is a server that verifies and forwards incoming client requests to other servers for further communication. For example, when a client is unable to meet the security authentication requirements of the server but should be permitted access to some services.

Proxy URL

If Use Web Proxy is enabled, enter the proxy URL supplied by your organization.

For example, https://proxy:8080/outgoing. This information is typically supplied by the network administration team.

Proxy Authentication

Proxy authentication is the process of validating user credentials for access to a proxy server. This authentication typically includes a *username* and can also include a *password*.

Click to select either Default Credentials or Specific Credentials:

Default Credentials

Specifies that proxy authentication is not required.

Specific Credentials

Specifies that proxy authentication is required.

Proxy Username

If proxy authentication Specific Credentials was enabled, enter the proxy username supplied by your organization.

Proxy Password

Click Set password and enter a password, then click OK.

NOTE: Use industry best practices for creating strong passwords.

Proxy Domain

Enter the domain name supplied by your organization.

Proxy connection status

Status icons indicate a valid () or invalid () proxy connection. The status is only displayed after the Verify button has been clicked.

Verify

Click Verify to test that the connection settings for your proxy server are valid.

5. In the ClearID settings section, configure the settings:

The ClearID settings section is used to connect to ClearID services and synchronize data.

ClearID service authentication key

Click more () to navigate to and select the authentication key for your API integration. This key is used to authenticate the synchronization agent communications when making requests to your ClearID account.

-  Indicates that the synchronization agent is not connected to ClearID and a private key is needed.
-  Indicates that the synchronization agent is connected to ClearID and that the private key has been provided.

The following API URL settings are automatically completed after the ClearID service authentication key has been selected:

Token API URL (read-only)

The Token service provides the authentication token to contact the identity and principal service.

Identity API URL (read-only)

The Identity service is used to access all ClearID identity information.

Principal API URL (read-only)

The Principal service is used to give web portal access to users.

Default Country (ISO 3166 3 letters)

Enter your three-letter country code. For example, the USA or CAN.

NOTE: The three-letter country codes are based on the Alpha-3 codes in the ISO 3166-1 country codes standard.

Principal has portal access

Select the checkbox to enable ClearID web portal access for synchronized users.

6. (Optional) In the Advanced settings section, leave these fields blank.

The Advanced settings section is used to customize the synchronization agent behavior.

Create inactive identities

Select the checkbox to create inactive ClearID identities for any inactive users found in the Active Directory during synchronization.

Best Practice: This checkbox is typically cleared to prevent the creation of inactive users.

Users query filters

(Optional) Enter custom user query filters as specified by your deployment contact.

IMPORTANT: Only use this option when you are advised to by your deployment contact.

7. Click Save.

GENETEC CLEARID™ LDAP SYNCHRONIZATION AGENT

User directory settings

LDAP search path:

Refresh interval (min.):

Connection settings

Host:

Port:

LDAP authentication type:

Network settings

Use Web Proxy: ☒

Proxy URL:

Proxy Authentication: ☒ Default Credentials ☐ Specific Credentials

Proxy connection status:

ClearID™ settings

ClearID™ service authentication key:

Token API URL:

Identity API URL:

Principal API URL:

Default Country (ISO 3166 3 letters):

Principal has portal access: ☒

Advanced settings

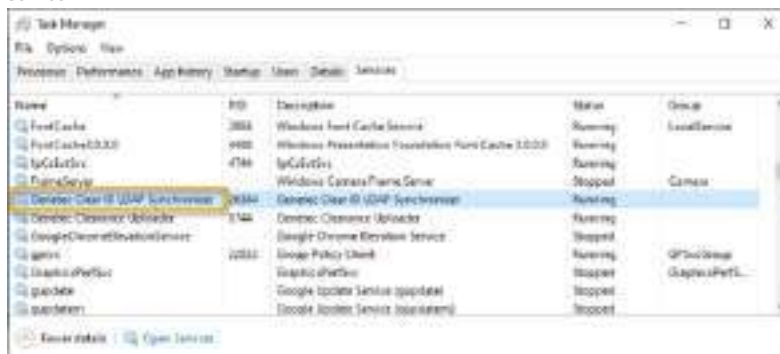
Create inactive identities: ☐

Users query filters:

The Synchronization Agent config file is saved to C:\ProgramData\Genetec ClearID LDAP Synchronizer\config.json

Tip: You can delete this file if you want to remove all your settings and configure the synchronization agent again.

8. Open the Windows Task Manager, and right-click the Genetec ClearID LDAP Synchronizer (Genetec.ClearID.LdapSyncAgent.Service.exe) windows service.



- a. If it is the first time you configure the agent, click Start to start your service so that your configuration settings are activated.
- b. If the agent is already running, click Restart to restart your service so that your configuration changes are activated.

Results

Your ClearID Synchronization Agent is now configured to automatically synchronize Active Directory LDAP attributes into ClearID identity attributes.

After you finish

1. Check the ClearID web portal to verify that the new identities for Active Directory users have been synchronized and contain the correct attributes.
2. (Optional) You can click Open Service Log folder to view the ErrorLog.txt or Eventlog.txt log files.
NOTE: The information in the *Service Log* folder is typically used when you raise a support call or if advised by your deployment contact to send Service logs to Genetec Inc..

Parent topic: [Synchronizing identities using LDAP in ClearID](#)

Browse

- [Authenticating your connection with ClearID](#)

13 | Visitor management devices

13.1 | About ClearID Self-Service Kiosk

Genetec ClearID™ Self-Service Kiosk is a mobile app that simplifies the management of visitors enrolled using the Genetec ClearID™ self-service portal. The self-service kiosk is intended for visitor centers or gated facilities where guests check-in by themselves.



Visitors can check in at the ClearID Self-Service Kiosk using several methods:

- Find a visitor associated with a visit by scanning their invitation QR code.
- Find a visitor associated with a visit by scanning their drivers license.
- Find a visitor associated with a visit by scanning their passport or citizen card (MRZ data).
- Find a visitor associated with a visit by scanning their Identity Document (various ID types from more than 200 countries).
- Find a visitor associated with a visit by their email.

NOTE: After visitors are checked-in from the ClearID Self-Service Kiosk, the host is notified by email and SMS message (if enabled).

With the ClearID Self-Service Kiosk, you can also do the following:

- Screen visitors during a self-service check-in or a self-registration.
- Take a photo of the visitor¹.
- Print a visitor badge using a wireless label printer (Bluetooth or Wi-Fi). The badge includes a photo and identifies the visitor and the event they are attending.
- Visitor self-registration.
- Company logos on the ClearID Self-Service Kiosk and visitor badges.
- Customer-specific welcome and assistance messages on the ClearID Self-Service Kiosk.

NOTE: ¹This photo is only used on the printed badge. The photo is not saved or stored for later use to ensure that visitor information is protected.

Visitor badges

The following examples show visitor badges in *portrait* and *landscape* orientation.



Badge dimensions: 10 x 6.1 cm's or 3.94 x 2.56 inches.

To download the Genetec ClearID™ Self-Service Kiosk mobile app, visit the App Store.

Browse

- Supported devices for ClearID
- Identity document types in ClearID

Browse

- ClearID Self-Service Kiosk Datasheet (2 pages)

13.1.1 | About ClearID Self-Service Kiosk check-in

Use this information to help you understand how visitors check in at a Genetec ClearID™ Self-Service Kiosk.



NOTE: Visitors can check in up to 1 hour before a visit event.

Scenario 1: Self-Service Kiosk check-in (paper badge)

Visitors can easily check in at a ClearID Self-Service Kiosk. Using their emailed QR code, visitors scan the code, take a picture, and print a visitor badge that identifies the visitor and the event they are attending.

Scenario 2: Self-Service Kiosk check-in (cardholder credential)

Using Security Center, a receptionist can assign a credential to Genetec ClearID™ visitors, the visitor can then use their card to access specified areas in the building when accompanied by their host.

Self-service check-in

The self-service check-in is intended for visitors who have been invited or pre-registered.



You can use the ClearID Self-Service Kiosk to check in yourself using QR code, ID, or email up to 1 hour before a visit event:

- If duplicate names are found, you select your unique email from list.
- If you scan a QR code that is not found, the Self-Service Kiosk switches to looking for visitor by email.
- If an ID or email is not found the Self-Service Kiosk switches to the self-registration process.

NOTE: The check-in choices displayed on the ClearID Self-Service Kiosk Welcome page can be customized to hide any options that are not relevant to your site or your visitor experience.

For more information, see the Kiosks tab section in Enabling visitor management for sites in ClearID.

Parent topic: [About ClearID Self-Service Kiosk](#)

Browse

- [Enabling visitor management for sites in ClearID](#)

13.1.2 | About ClearID Self-Service Kiosk Self registration

The Genetec ClearID™ Self-Service Kiosk self-registration process is designed to manage unplanned visits or visitors who have not been invited or pre-registered.

The self-registration workflow is triggered (if enabled for your account) when a visitor arrives on site with no invite and they are not found in the system during the self-service check-in process.

NOTE: Any pre-filled entries cannot be modified.



The self-registration process is linked to a site. Visitors are accepted automatically with default entry-level visitor access to the site. For example, Front door, reception, or check-in area to ensure a smooth check-in experience.

IMPORTANT: Any visitors on a block list will be denied access if the *watchlist* function is enabled for your account, and the *watchlist manager* is notified. In this situation, the visitor should talk to security or reception staff.

Parent topic: [About ClearID Self-Service Kiosk](#)

13.2 | Configuring the ClearID Self-Service Kiosk iPad

Before visitors can use the self-service kiosk to check in or check out, you must add the Genetec ClearID™ Self-Service Kiosk iPad device to Genetec ClearID™. Then you can register and activate the device in the ClearID Self-Service Kiosk mobile app.

Before you begin

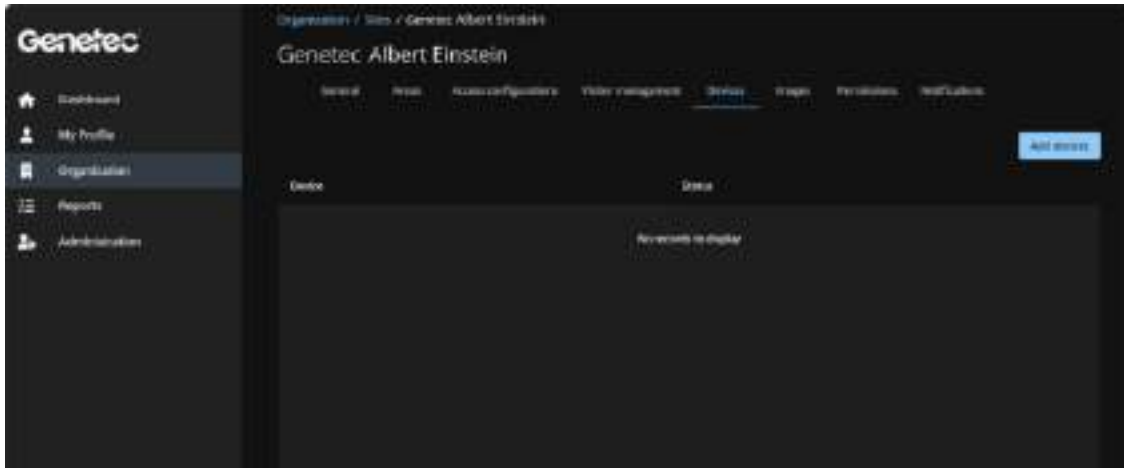
- Wi-Fi must be enabled on the self-service kiosk device before activating the device.
- Your device must be running iOS 16.6 or later.

What you should know

- Only an *administrator* or a *Site owner* can generate a device activation code in ClearID.
- You can only activate and associate a ClearID Self-Service Kiosk with one site at a time.
- The ClearID Self-Service Kiosk iPad must be on the same Wi-Fi network as the label printer.

Procedure

1. In ClearID, click Organization and select your site.
2. On the Site page, click Devices.



- a. Click Add devices to configure your ClearID Self-Service Kiosk in ClearID.
 - b. In the Add devices dialog, enter a name for the device.
Tip: Consider including the associated site or area in the name to help you easily identify your device in the future.
 - c. Enter the number of devices that you want to add, and click Add.
NOTE: You can configure up to 50 devices with a single activation code.
3. Download the ClearID Self Service Kiosk app on the iOS devices that you want to register,
 4. Activate your kiosk in ClearID:
 - a. Select your iPhone from the devices list.
 - b. In the Status field, click Generate activation code.



c. Make a note of the activation code for later use.

d. (Optional) Copy to clipboard.

Tip: Use Copy to clipboard when the person who registers the ClearID mobile operator check-in device in the ClearID portal is different to the person who activates the device. Once the code is in the clipboard, it can be emailed to the person who activates the device.

e. Click OK.

5. In the ClearID Self-Service Kiosk mobile app, enter your device activation code and tap Activate.



Results

Your self-service kiosk is now activated in ClearID and ready for use.



Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.



After you finish

- Configure your kiosk label printer
- (Optional) Customize your banner image for email notifications
- (Optional) Customize your Self-Service Kiosk configuration
- (Optional) Customize your Self-Service Kiosk badge logo

Browse

- Supported devices for ClearID
- Firewall ports used in ClearID

13.2.1 | Customizing the ClearID Self-Service Kiosk configuration

Configure your site images and kiosk options to customize the choices that are displayed to visitors using your Genetec ClearID™ Self-Service Kiosk during the check-in or check-out process. Customization can include company logos, kiosk themes, and customer-specific welcome and assistance messages.

Before you begin

Configuring the ClearID Self-Service Kiosk iPad

Tip: Ensure that your welcome screen images meet the requirements described in the  tooltip on the Visitor management > Kiosks page of the Genetec ClearID™ web portal.

What you should know

Only a site owner or account administrator can customize the kiosk configuration options.

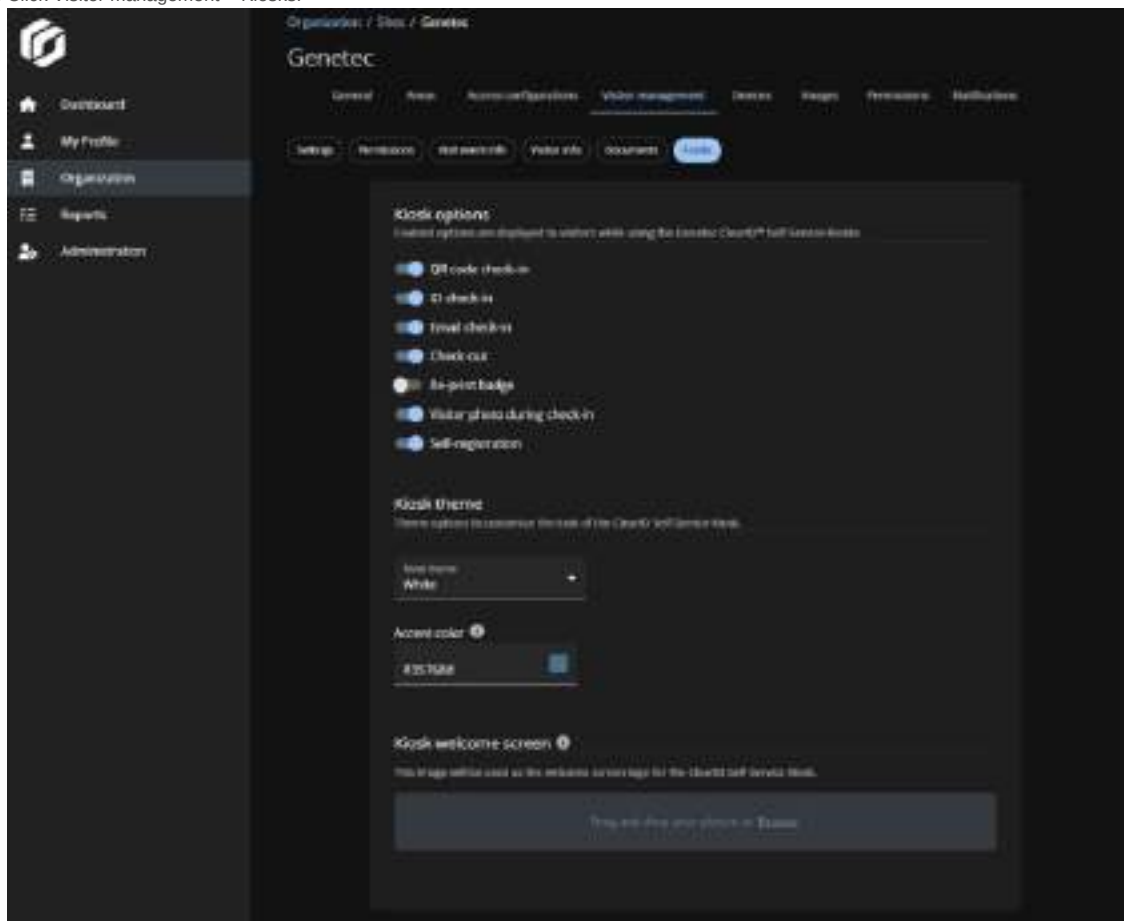
- Customized kiosk options changes are synchronized with your kiosk every 60 seconds.

Best Practice: For optimum results, use transparent .PNG images when customizing your welcome screen image.

Procedure

1. In the ClearID web portal, click Organization and select your site.

2. Click Visitor management > Kiosks.



3. In the Kiosk tab, customize your kiosk configuration options as required:
 - a. (Optional) In the Kiosk theme section, choose a theme to customize the look of the kiosk.
For example, select the White theme and choose an Accent color that aligns with your corporate branding.
 - b. (Optional) In the Kiosk welcome screen section, upload an image to use as the welcome screen logo.
For example, a *company name* or *logo* that aligns with your corporate branding.
For more detailed information and to see examples of these kiosk customizations, see [Enabling visitor management for sites in ClearID](#).
4. Click Save.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

Parent topic: [Configuring the ClearID Self-Service Kiosk iPad](#)

13.2.2 | Customizing the ClearID Self-Service Kiosk visitor badge logo

You can customize the visitor badge logo image that is used on temporary badges or visitor badges printed by the kiosk.

Before you begin

Configuring the ClearID Self-Service Kiosk iPad

Tip: Ensure that your badge logo images meet the requirements described in the  tooltip on the Images page of the Genetec ClearID™ web portal.

What you should know

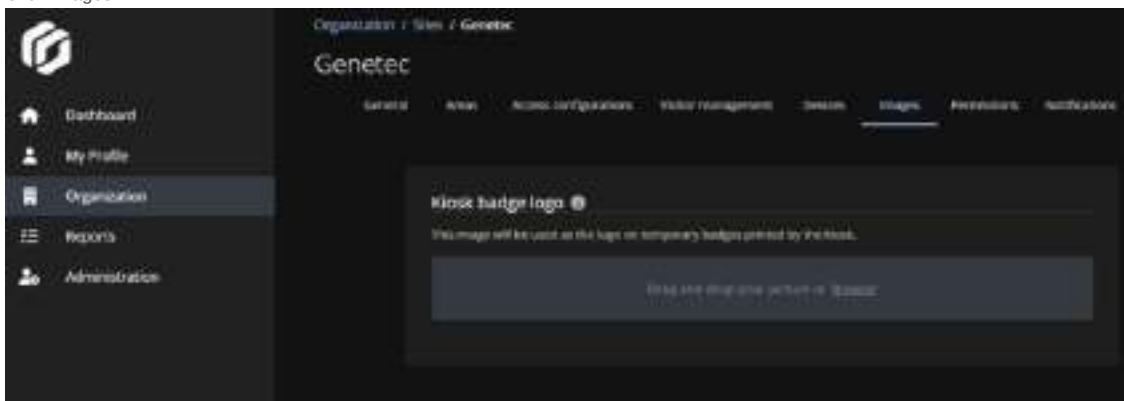
Only a site owner or account administrator can customize the visitor badge logo.

- Customized Kiosk options changes are synchronized with your kiosk every 60 seconds.

Best Practice: For optimum results, use transparent .PNG images when customizing your visitor badge logo.

Procedure

1. In the ClearID web portal, click Organization > Sites.
2. Search for and select a site.
3. Click Images.



- a. In the Kiosk badge logo section, drag and drop your picture or browse to select a Kiosk badge logo.
This image is used as the logo on temporary badges printed by the kiosk.
- b. Click Save.

The following example shows a custom badge logo for the kiosk.



Parent topic: Configuring the ClearID Self-Service Kiosk iPad

13.2.3 | Adding visitor compliance documents to the ClearID Self-Service Kiosk

For sites with special requirements, *Account administrators* and *Site owners* can upload documents like non-disclosure agreements, waivers, and more for visitors to sign when checking in using the Self-Service Kiosk.

Before you begin

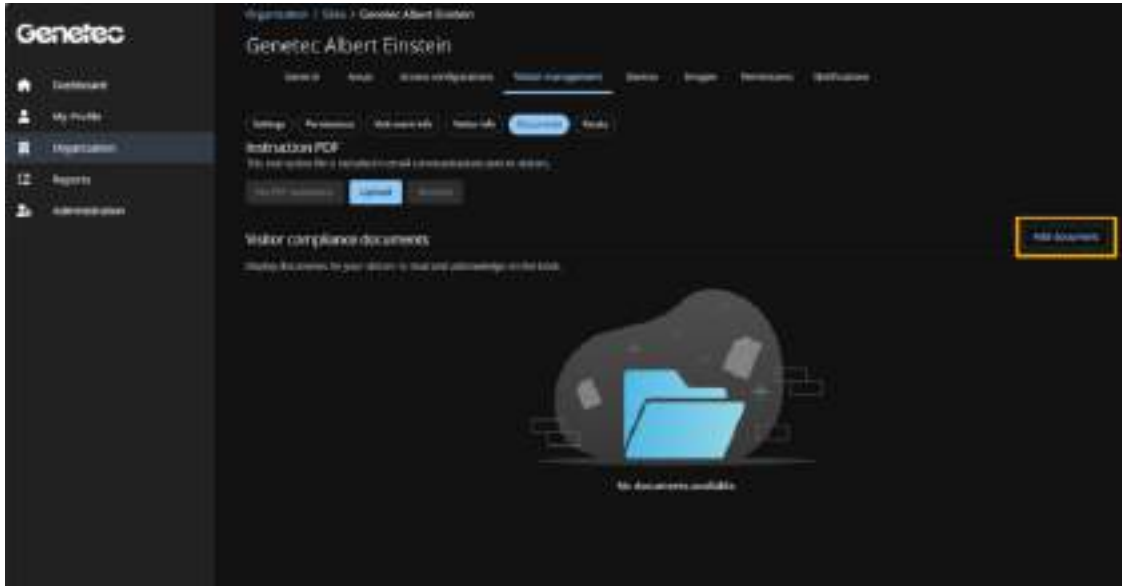
Enable visitor management for sites.

What you should know

- You must be an *Account administrator* or *Site owner* to add documents for visitors to acknowledge to the Self-Service Kiosk.
- You can display up to five documents on the kiosk during check-in.

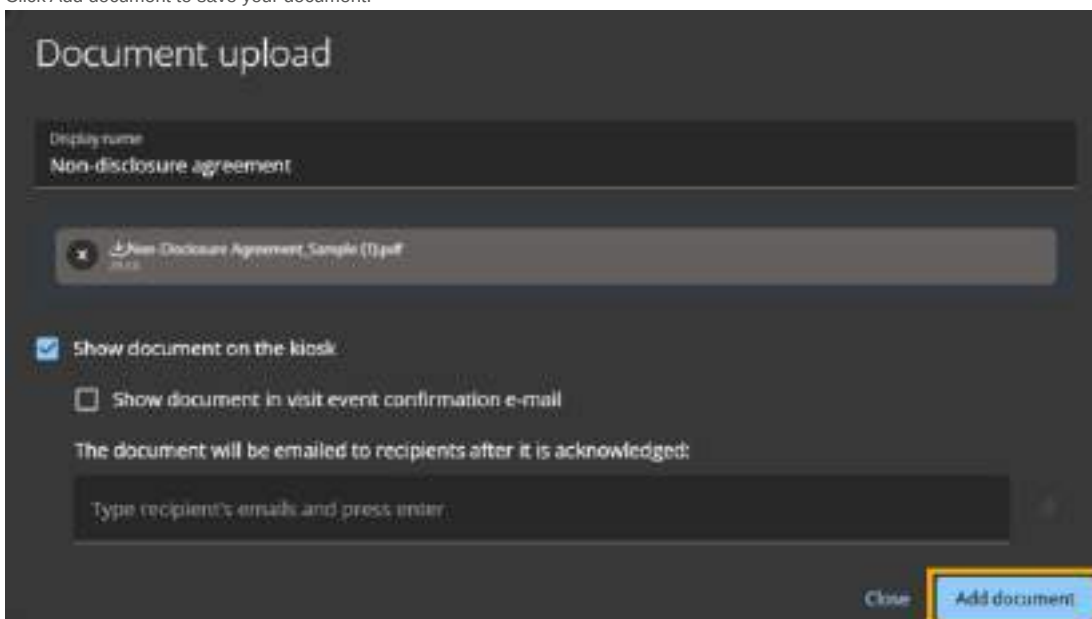
Procedure

1. In the Genetec ClearID™ web portal, click Organization > Site > Visitor management > Documents.
2. Click Add document.



IMPORTANT: These documents must be in PDF format.

- a. In the Display name field, enter a name for the document.
 - b. Drag and drop a file into the field, or click Browse to search for a file.
3. Configure your sharing preferences for the document as needed:
 - a. Select the Show document on the kiosk checkbox to show the document on the Kiosk during visitor check-in.
Tip: When the checkbox is not selected, the document remains available in draft mode.
 - b. Select the Show document in visit event confirmation e-mail checkbox to attach a copy of the document to visitor confirmation emails so that visitors can review the documents before they arrive.
 - c. Add a list of recipients who should receive a copy of the document once visitors acknowledge it.
NOTE: You can click  to copy the complete list of recipients, for example, to add the same recipients to other compliance documents.
 4. Click Add document to save your document.

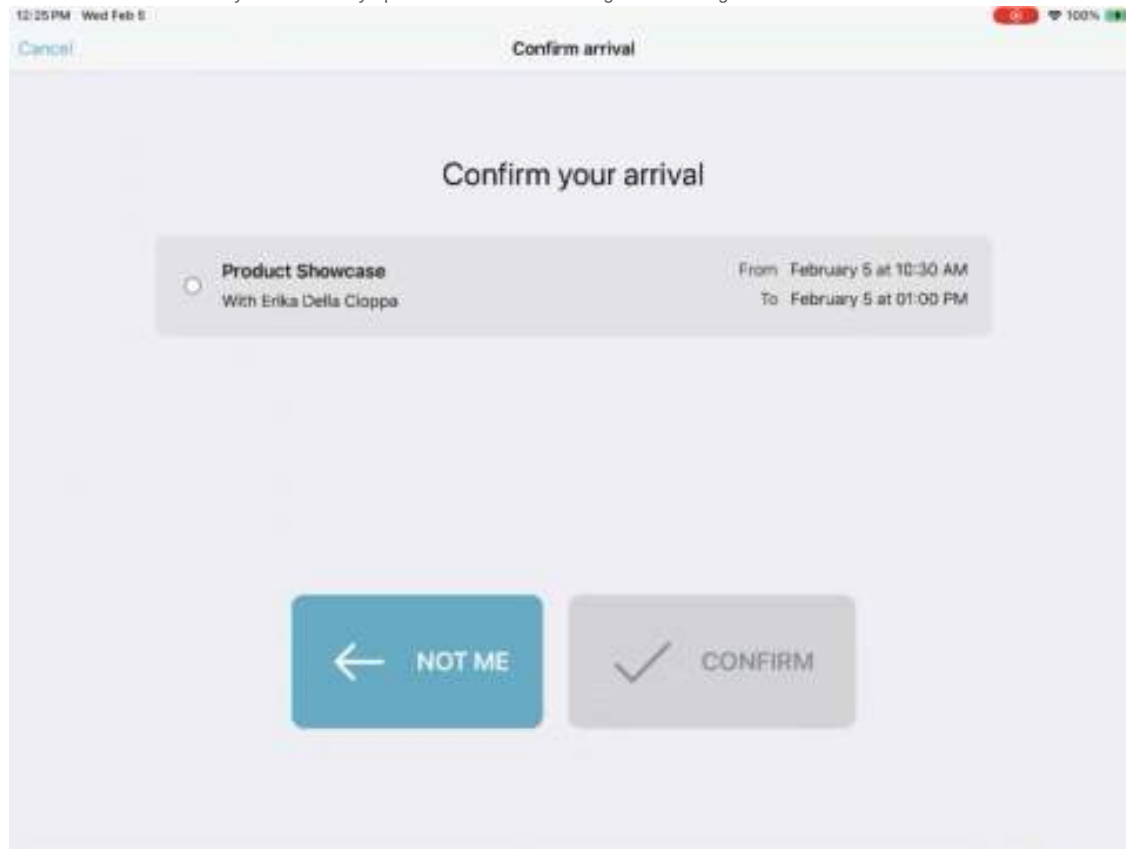


5. Use the icons to manage each uploaded document:
 - a. Click  to modify an existing document.

- b. Click  to download a local copy of the document.
- c. Click  to remove a document.

Results

Visitors have to confirm they have read any uploaded documents and sign them during check-in at the Self-Service Kiosk.



Parent topic: [Configuring the ClearID Self-Service Kiosk iPad](#)

13.2.4 | Activating badge reprinting for the ClearID Self-Service Kiosk

As a *Site owner*, you can activate badge reprinting so that visitors can reprint lost or damaged temporary badges from the ClearID Self-Service Kiosk.

Before you begin

[Configure the Self-Service Kiosk iPad.](#)

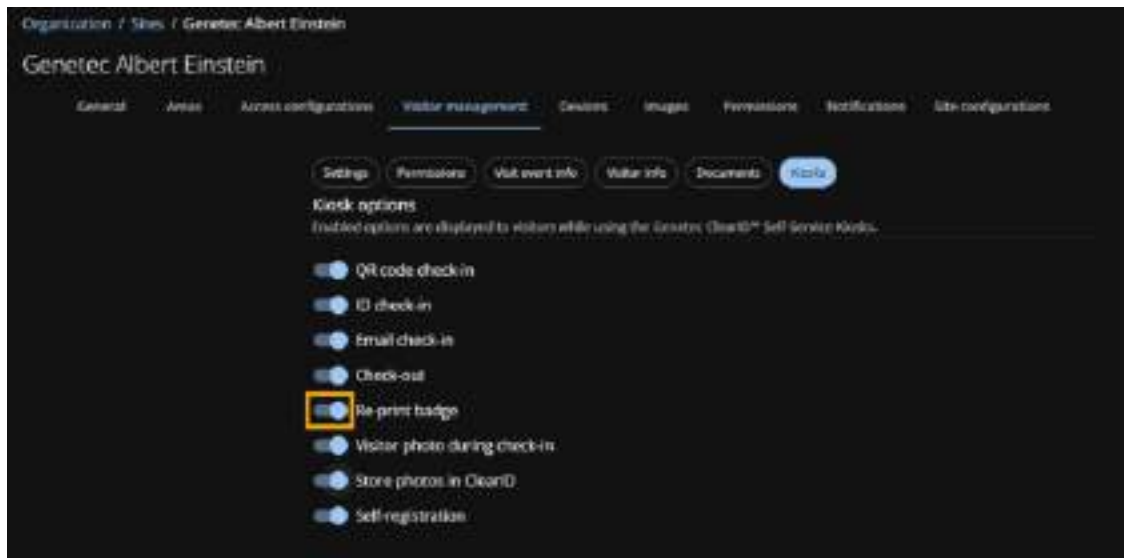
What you should know

You must be a *Site owner* to activate badge reprinting with the ClearID Self-Service Kiosk.

Best Practice: Visitor QR codes configured as credentials should only give access to non-secure areas.

Procedure

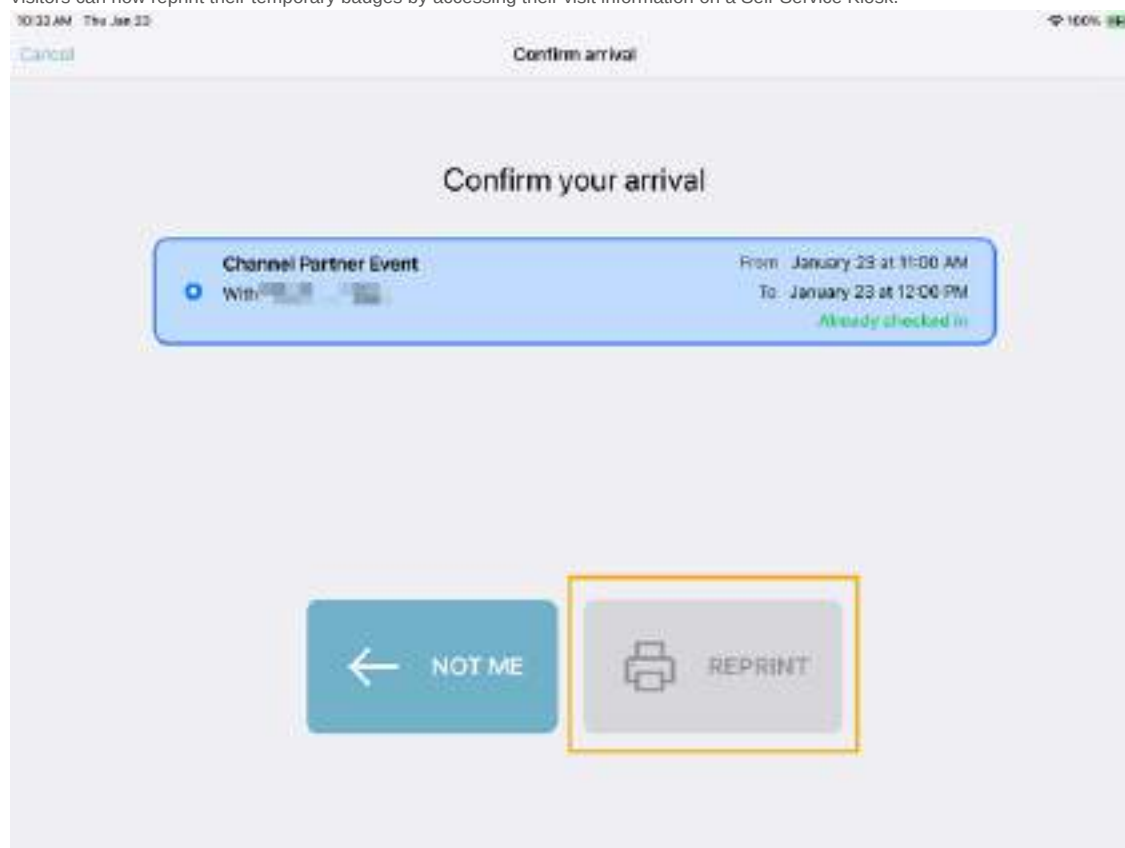
1. In the Genetec ClearID™ web portal, click Organization > Site > Visitor management > Kiosks.
2. In the Kiosk options section, turn on the Re-print badge option.



3. Click Save.

Results

Visitors can now reprint their temporary badges by accessing their visit information on a Self-Service Kiosk.



Parent topic: Configuring the ClearID Self-Service Kiosk iPad

13.2.5 | Disabling visitor photo during ClearID Self-Service Kiosk check-in

For sites where visitor privacy is crucial, *Site owners* can disable photo-taking during visitors check-in at the ClearID Self-Service Kiosk.

Before you begin

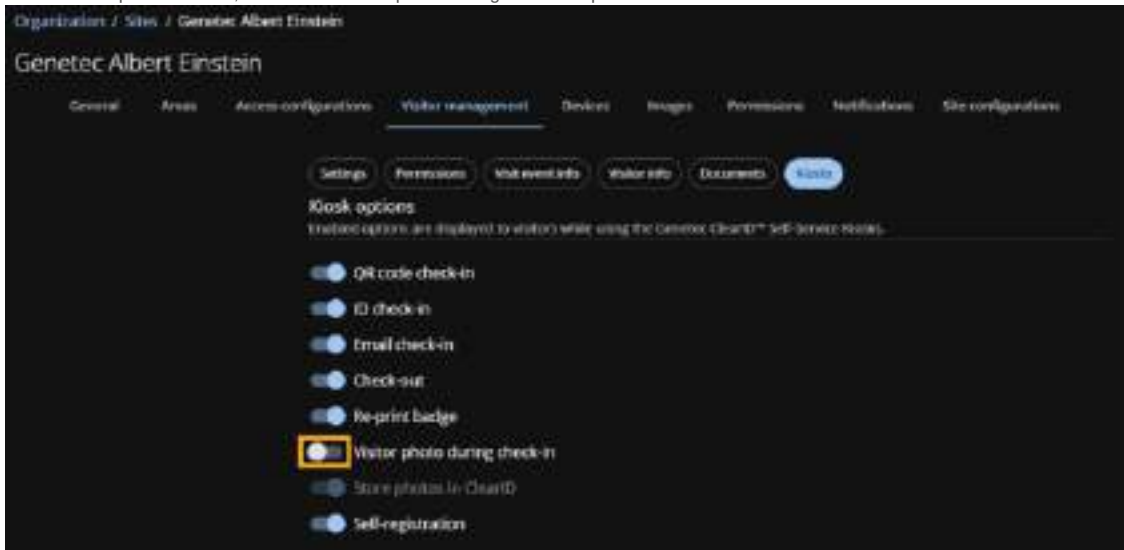
Configure the Self-Service Kiosk iPad.

What you should know

You must be a *Site owner* to disable visitor photos during check-in with the ClearID Self-Service Kiosk.

Procedure

1. In the Genetec ClearID™ web portal, click Organization > Site > Visitor management > Kiosks.
2. In the Kiosk options section, turn off the Visitor photo during check-in option.



NOTE: Visitor photo during check-in is turned on by default.

3. Click Save.

Results

Visitors can now check in at a Self-Service Kiosk without having to take a photo.

Parent topic: [Configuring the ClearID Self-Service Kiosk iPad](#)

13.2.6 | Activating visitor photo retention in ClearID

As a *Site owner* you can activate visitor photo retention to save photos of visitors taken during check-in to the Genetec ClearID™ web portal. You can access saved visitor photos for incident management and auditing purposes.

Before you begin

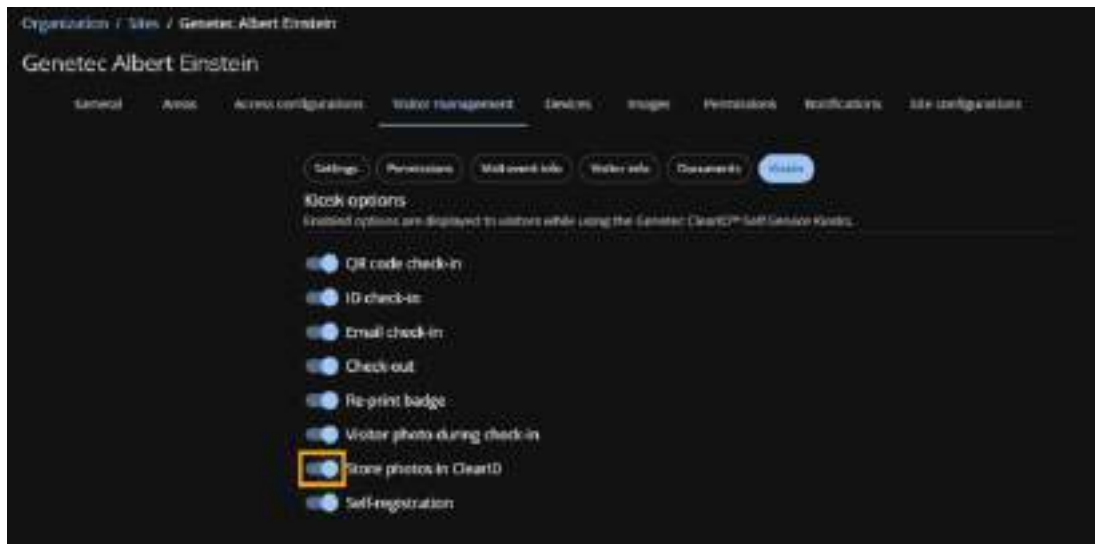
Configure the Self-Service Kiosk iPad and enable visitor photos during check-in.

What you should know

- You must be a *Site owner* to turn on visitor photo retention.
- Visitor photo during check-in must be turned on to store visitor photos in ClearID.

Procedure

1. In the ClearID web portal, click Organization > Site > Visitor management > Kiosks.
2. In the Kiosk options section, turn on the Store photos in ClearID option.



NOTE: Visitor photo during check-in is turned on by default.

3. Click Save.

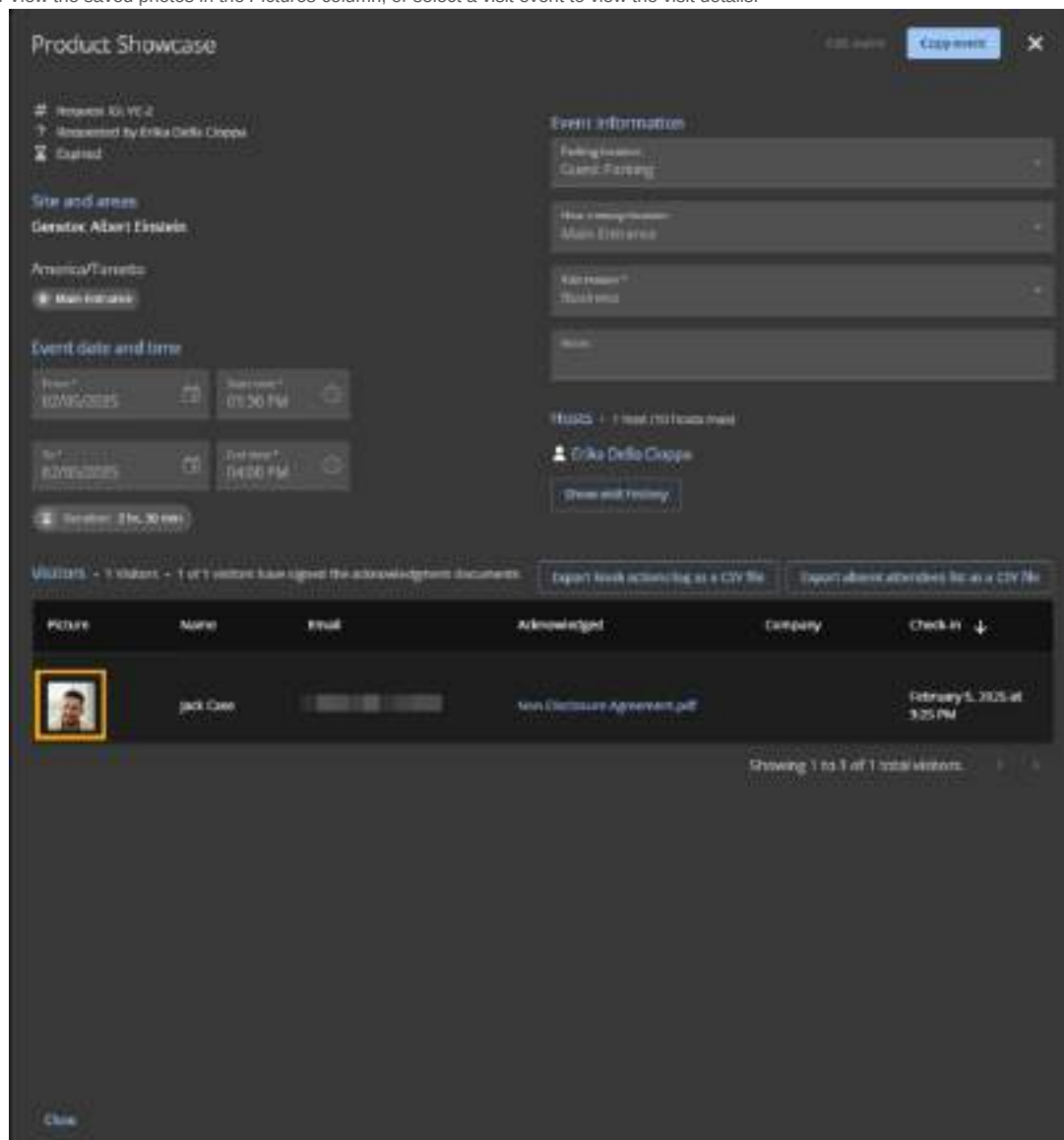
Visitor photos are stored in ClearID.

4. (Optional) View saved visitor photos.

a. In the ClearID web portal, click Reports > Visitors.

b. Filter the report as needed.

c. View the saved photos in the *Pictures* column, or select a visit event to view the visit details.



NOTE: Visitor photos are stored in ClearID for one year by default.

Parent topic: Configuring the ClearID Self-Service Kiosk iPad

13.3 | About ClearID mobile operator check-in

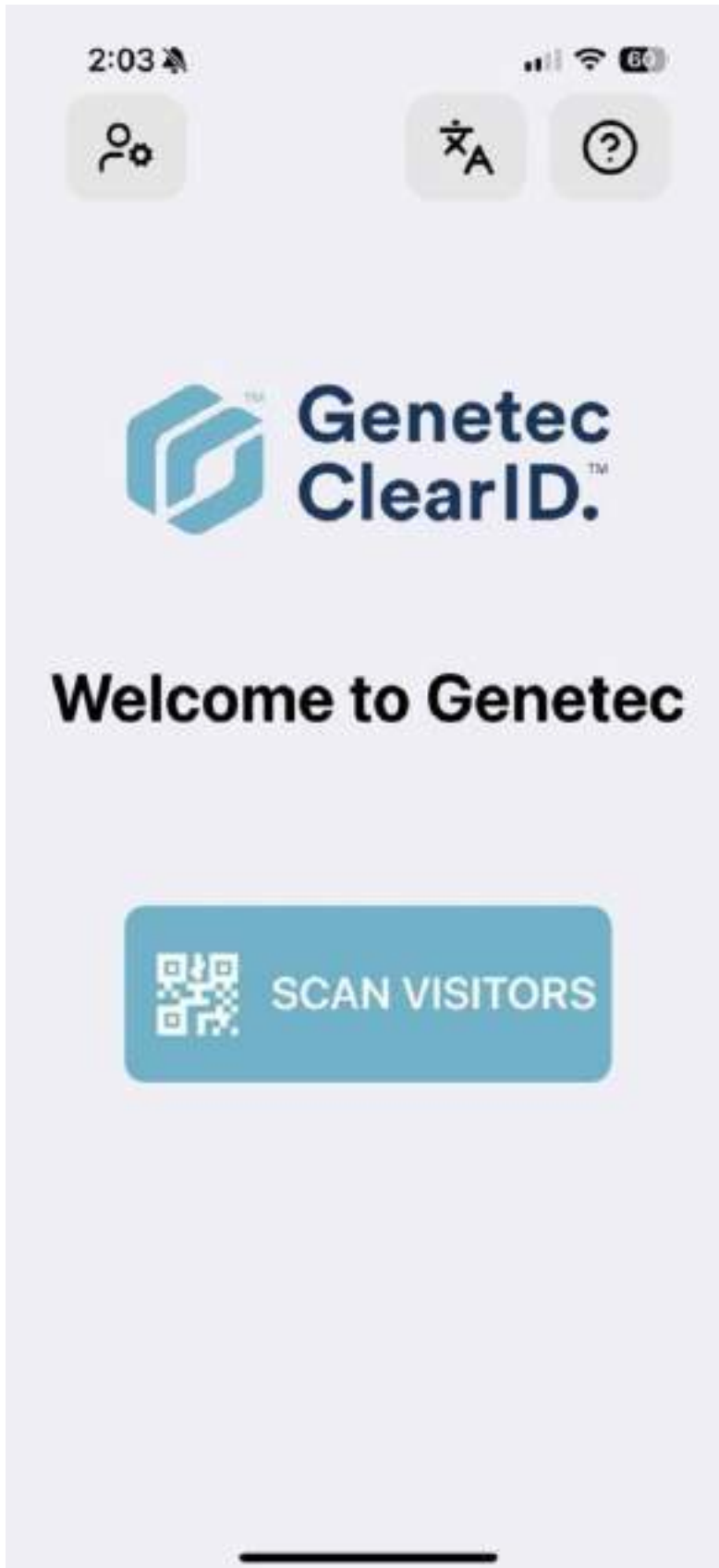
Use this information to help you understand how operators check visitors in and out of events using mobile operator check-in.



NOTE: Visitors can check in up to 1 hour before a visit event.

Mobile operator check-in

Mobile operator check-in is intended for operators in charge of checking in visitors who have been invited or pre-registered. Mobile operator check-in can be active on many iPhones at the same time, making checking into large events quicker by avoiding lineups at self-service kiosks.



Operators such as receptionists, security guards, and attendants can quickly check many visitors in at large events. Using the ClearID Self-Service Kiosk app on an iPhone, operators can scan QR codes or search for visitors by name or email.

- Visitors can't self-register when checked in by an operator.
- Mobile operator check-in doesn't scan IDs, take pictures, or print badges.

Check-in count

Once an operator scans a visitor's QR code, all visit information is displayed, including check-in and check-out options. Using these options, Genetec ClearID™ tracks the number of times visitors enter and leave your event.

13.4 | Configuring ClearID mobile operator check-in

Before you can use mobile operator check-in to check visitors into large events or look up visitor information, you must add an iPhone to Genetec ClearID™. Then you can register and activate the device in the ClearID Self-Service Kiosk mobile app.

Before you begin

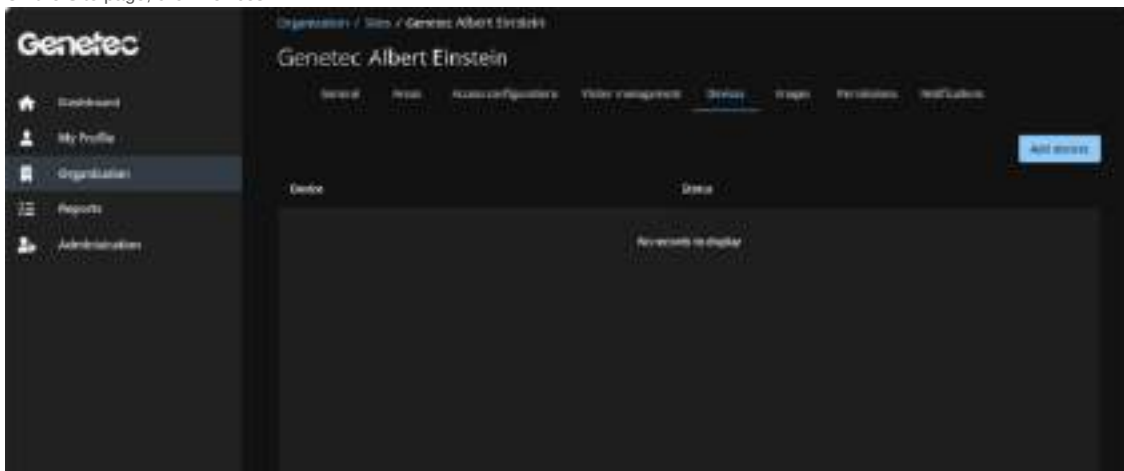
- Wi-Fi or cellular data must be enabled on the mobile operator check-in device before activating the device.
- Your device must be running iOS 16.6 or later.

What you should know

- Only an *administrator* or a *Site owner* can generate a device activation code in ClearID.
- You can only activate and associate a mobile operator check-in device with one site at a time.
- iPhones inherit the theme and settings of the self-service kiosk iPads associated with the same site.
- Check-ins using an iPhone don't require visitors to take a photo, print a badge, or acknowledge documents.

Procedure

1. In Genetec ClearID, click Organization and select your site.
2. On the Site page, click Devices.



- a. Click Add devices to configure your mobile operator check-in device in ClearID.
 - b. In the Add devices dialog, enter a name for the device.
Tip: Consider including the associated site or area in the name to help you easily identify your device in the future.
 - c. Enter the number of devices that you want to add, and click Add.
NOTE: You can configure up to 50 devices with a single activation code.
3. Download the ClearID Self Service Kiosk app on the iOS devices that you want to register.
 4. Activate your iPhone in ClearID:
 - a. Select your iPhone from the devices list.
 - b. In the Status field, click Generate activation code.



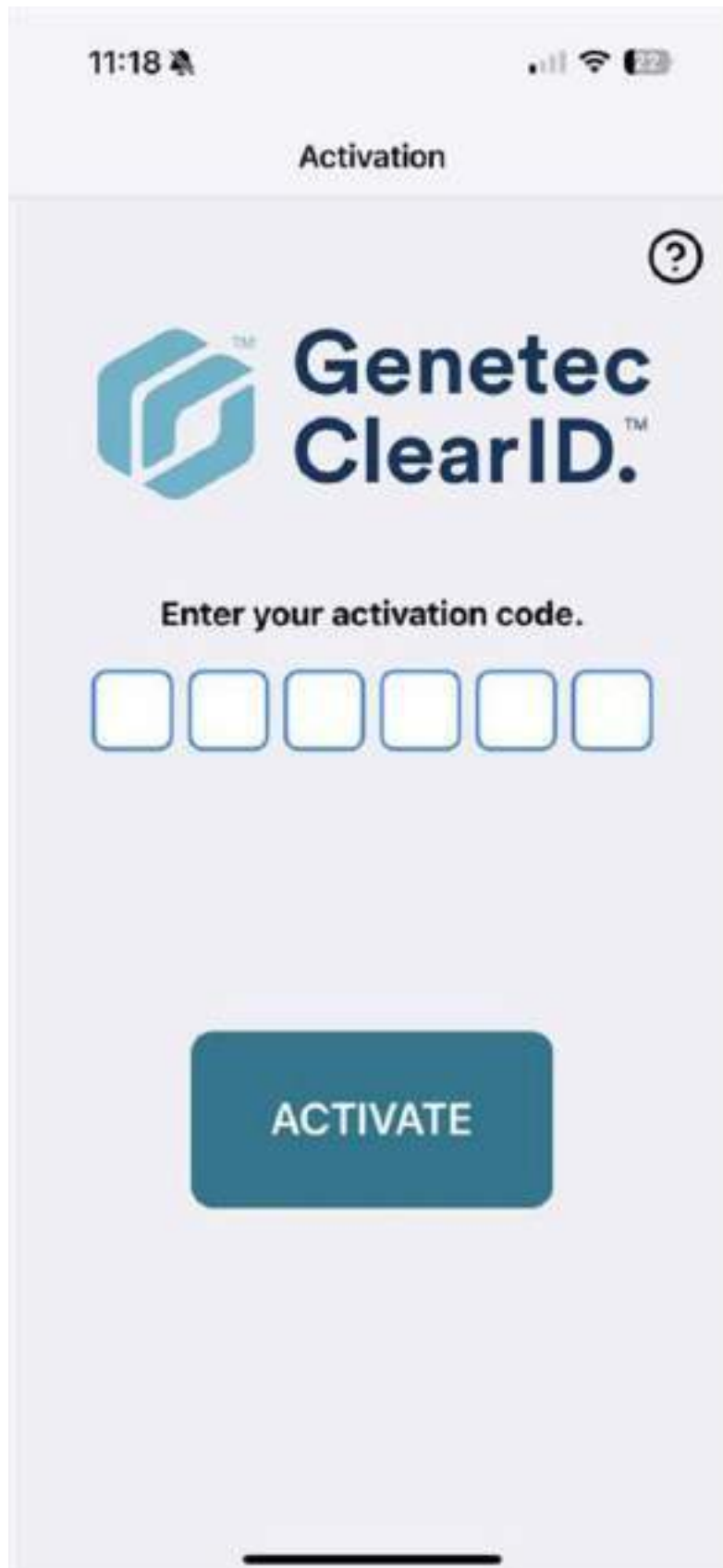
c. Make a note of the activation code for later use.

d. (Optional) Copy to clipboard.

Tip: Use Copy to clipboard when the person who registers the ClearID mobile operator check-in device in the ClearID portal is different to the person who activates the device. Once the code is in the clipboard, it can be emailed to the person who activates the device.

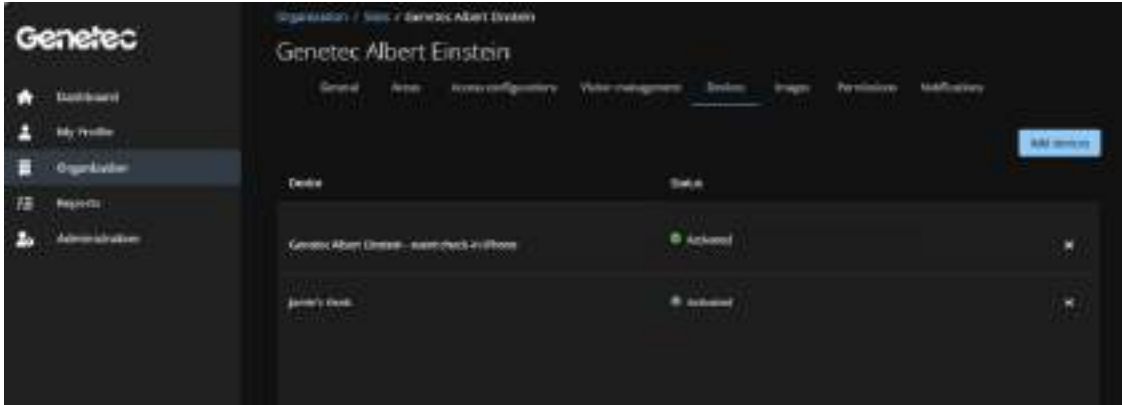
e. Click OK.

5. In the ClearID Self-Service Kiosk iPhone app, enter your device activation code and tap Activate.



Results

Your iPhone is now activated in ClearID and ready for use as a mobile operator check-in device.



13.5 | Configuring the ClearID Self-Service Kiosk label printer (Brother QL-820NWBc, QL-820NWB, or QL-810W)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother QL-810W/820NWB Quick Setup Guide \(English\)](#)
- [Brother QL-810W/QL-820NWB User Guide \(English\)](#)
- [Brother QL-820NWB LED Status indicators](#)

NOTE: The Brother QL-820NWBc replaced the Brother QL-820NWB printer (discontinued). For more information about the differences, see [Brother QL-820NWBc Specifications changes](#).

What you should know

Best Practice: Use only one label printer per kiosk and [pair the printer with the kiosk using Bluetooth](#).

If you require one label printer to be used with many kiosk devices, or you need the label printer far away from the kiosk devices use Wi-Fi or Ethernet. For example, two kiosks by the entrance and one label printer on the reception desk.

NOTE: A rechargeable Li-ion battery unit (power supply) can also be purchased and used in situations where mains power is unavailable.

Procedure

Choose one of the following:

- [Configuring Bluetooth mode \(Brother QL-820NWBc or QL-820NWB\)](#)
- [Configuring Wi-Fi mode \(Brother QL-820NWBc, QL-820NWB, or QL-810W\)](#)
- [Configuring Ethernet mode \(Brother QL-820NWBc or QL-820NWB\)](#)

After you finish

From time to time you might need to order supplies, replace the coin cell battery, recharge the optional battery unit (if used), or clean the label printer.

For more information, see *Brother QL-810W/QL-820NWB Quick Setup Guide* and *Brother QL810W/QL-820NWB User Guide*.

Browse

- [Brother QL-820NWB Label Printer FAQs](#)
- [Brother QL-820NWB printer supplies](#)

Browse

- [Supported devices for ClearID](#)
- [ClearID Self-Service Kiosk options](#)

13.5.1 | Configuring the ClearID Self-Service Kiosk label printer for Bluetooth mode (Brother QL-820NWBc or QL-820NWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother QL-810W/820NWB Quick Setup Guide \(English\)](#)
- [Brother QL-810W/QL-820NWB User Guide \(English\)](#)
- [Brother QL-820NWB LED Status indicators](#)

NOTE: The Brother QL-820NWBc replaced the Brother QL-820NWB printer (discontinued). For more information about the differences, see [Brother QL-820NWBc Specifications changes](#).

What you should know

When using the Brother QL-820NWBc or QL-820NWB label printer in Bluetooth printing mode, the following applies:

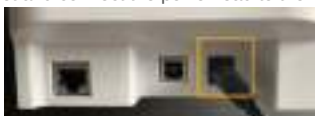
- One label printer can be paired with only one kiosk.
- The label printer must be within 30ft of the kiosk.

NOTE: A rechargeable Li-ion battery unit (power supply) can also be purchased and used in situations where mains power is unavailable.

Procedure

1. Plug printer AC adapter into a power outlet and connect the power lead to the label printer.

Brother QL-820NWBc label printer (rear)



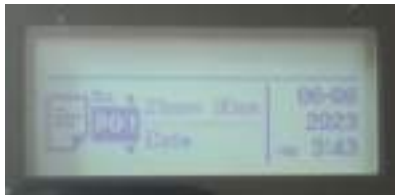
Brother QL-820NWB label printer (rear)



2. Press the Power button to turn the label printer on.

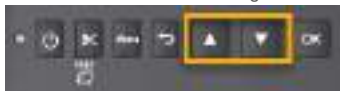


3. (Optional) If you see Template Mode menu and the incorrect label size displayed, disable it.



- a. Press Menu, navigate to Template Settings and turn off the Template Mode setting.

4. Use the arrow buttons to navigate the label printer menu.



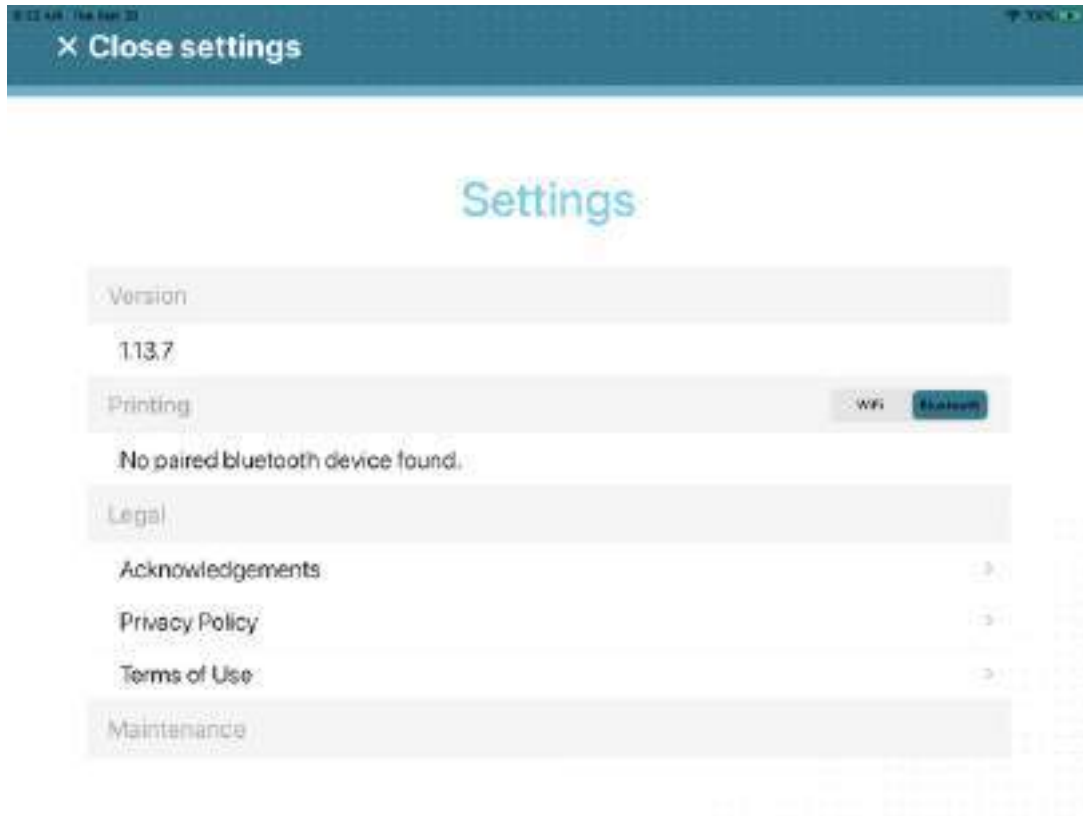
- a. Select Bluetooth > Bluetooth (On/Off) > On in the settings menu and press OK.

- b. Select Bluetooth > Automatic Reconnection (On/Off) > On in the settings menu and press OK.

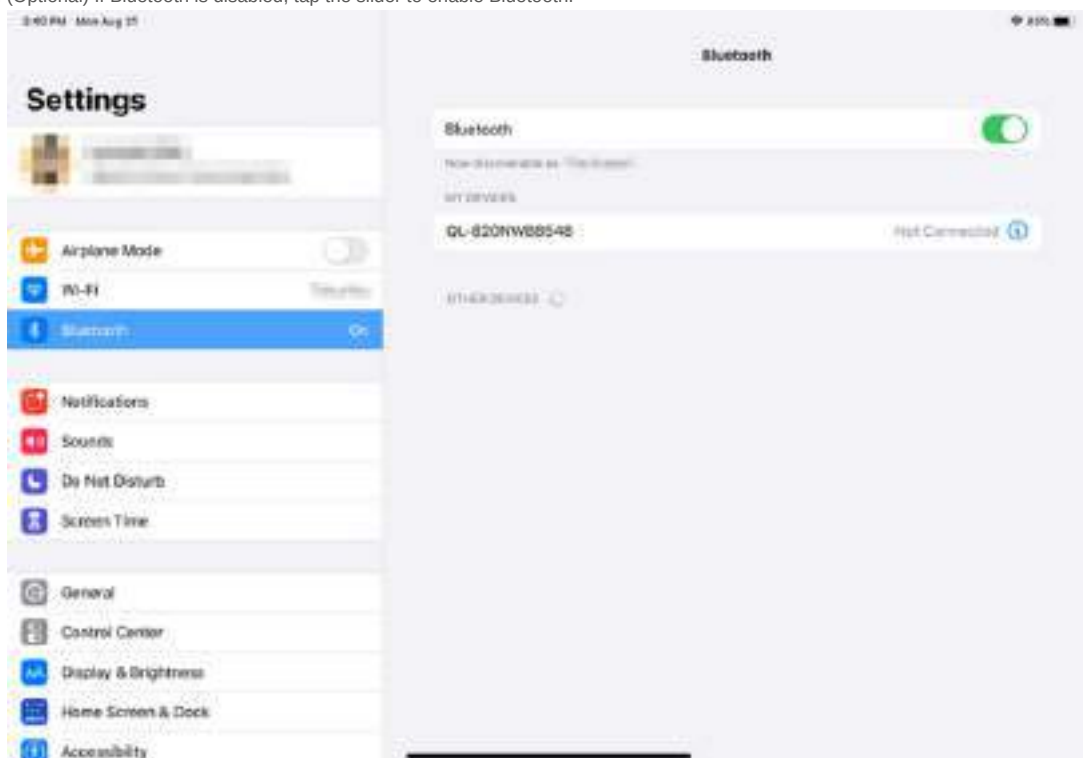
5. Pair your Bluetooth label printer with your ClearID Self-Service Kiosk iPad.

- a. In the Self-Service Kiosk mobile app, tap Settings (⚙️).

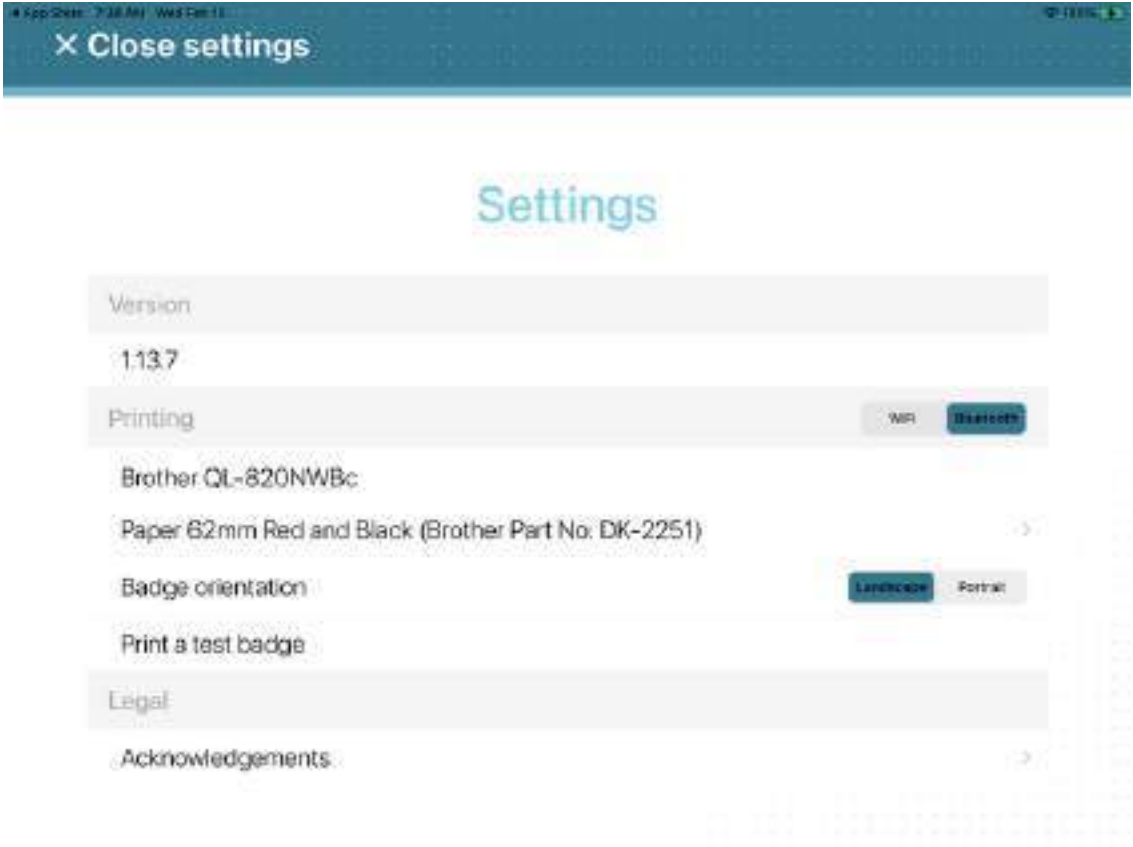
- b. In the Printing section, tap the slider control to select Bluetooth.



6. On your iPad, navigate to the Apple Settings icon, tap Settings > Bluetooth.
 - a. (Optional) If Bluetooth is disabled, tap the slider to enable Bluetooth.



- b. Click the correct printer to pair the ClearID Self-Service Kiosk iPad with your printer.
7. In the Self-Service Kiosk mobile app, tap Settings (👤).



- a. In the Printing section, check that your Brother QL-820NWBc or QL-820NWB printer is displayed.
Tip: If the printer is not displayed or bluetooth is not selected, tap WiFi then tap Bluetooth to trigger discovery again.

After you finish

(Optional) Print a test badge.
Parent topic: [Configuring the ClearID Self-Service Kiosk label printer \(Brother QL-820NWBc, QL-820NWB, or QL-810W\)](#)
[Browse](#)

- [Firewall ports used in ClearID](#)

13.5.2 | **Configuring the ClearID Self-Service Kiosk label printer for Wi-Fi mode (Brother QL-820NWBc, QL-820NWB, or QL-810W)**

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother QL-810W/820NWB Quick Setup Guide \(English\)](#)
- [Brother QL-810W/QL-820NWB User Guide \(English\)](#)
- [Brother QL-820NWB LED Status indicators](#)

NOTE: The Brother QL-820NWBc replaced the Brother QL-820NWB printer (discontinued). For more information about the differences, see [Brother QL-820NWBc Specifications changes](#).

What you should know

- One label printer can support up to five self-service kiosks
- The label printer must be on the same Wi-Fi network as the Genetec ClearID™ Self-Service Kiosk iPad.

The Wi-Fi network must be enabled for use and support the following:

- Bonjour - required for device search.
- SNMP - required to check printer status information.
- UDP or TCP Port 9100 - required to send print data.

NOTE: A rechargeable Li-ion battery unit (power supply) can also be purchased and used in situations where mains power is unavailable.

Procedure

1. Plug printer AC adapter into a power outlet and connect the power lead to the label printer.

Brother QL-820NWBc label printer (rear)



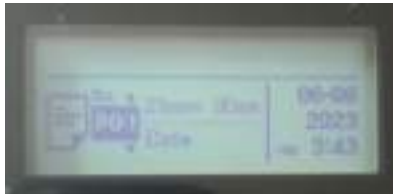
Brother QL-820NWB label printer (rear)



2. Press the Power button to turn the label printer on.

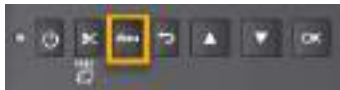


3. (Optional) If you see Template Mode menu and the incorrect label size displayed, disable it.

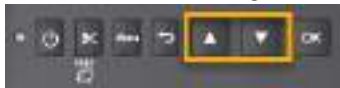


- a. Press Menu, navigate to Template Settings and turn off the Template Mode setting.

4. Press the Menu button.



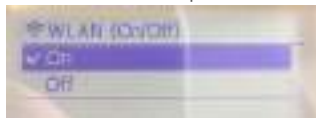
5. Use the arrow buttons to navigate the label printer menu.



6. Scroll down to the WLAN (5/7) settings and press OK.



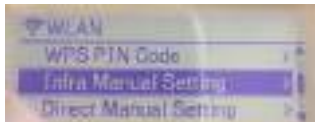
- a. Select WLAN On and press OK .



- b. In the Network Mode menu items, select Infrastructure Mode and press OK.



7. Scroll down to Infra Manual Setting and press OK.



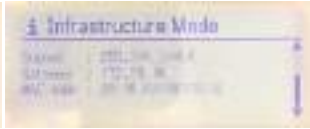
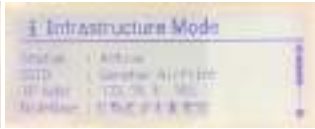
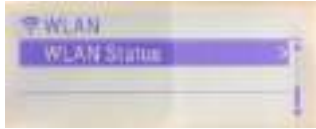
- a. After the search completes, scroll down and select your Wi-Fi network from the Service Set Identifier (SSID) list and press OK.



NOTE: Typically this network is a Wi-Fi network with AirPrint enabled.

b. When prompted enter the Wi-Fi password.

8. Navigate to WLAN Status and press OK to verify your Wi-Fi network status and IP address.



Tip: Make a note of the SSID (Wi-Fi network) and IP Addr (Label Printer IP) for later use.

- The SSID is used to verify that you are on the same Wi-Fi network as the ClearID Self-Service Kiosk iPad.
- The IP address is used later when selecting a label printer to verify you have the correct printer.

9. Select your Wi-Fi label printer.

After you finish

(Optional) Print a test badge.

Parent topic: Configuring the ClearID Self-Service Kiosk label printer (Brother QL-820NWBc, QL-820NWB, or QL-810W)

Browse

- Firewall ports used in ClearID

13.5.3 | Configuring the ClearID Self-Service Kiosk label printer for Ethernet mode (Brother QL-820NWBc or QL-820NWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- Brother QL-810W/820NWB Quick Setup Guide (English)
- Brother QL-810W/QL-820NWB User Guide (English)
- Brother QL-820NWB LED Status indicators

NOTE: The Brother QL-820NWBc replaced the Brother QL-820NWB printer (discontinued). For more information about the differences, see Brother QL-820NWBc Specifications changes.

What you should know

- One label printer can support up to five self-service kiosks

NOTE: A rechargeable Li-ion battery unit (power supply) can also be purchased and used in situations where mains power is unavailable.

Procedure

1. Plug printer AC adapter into a power outlet and connect the power lead to the label printer.



Brother QL-820NWBc label printer (rear)



Brother QL-820NWB label printer (rear)

2. Make sure that the printer is turned OFF before connecting the LAN cable.

Brother QL-820NWBc label printer (rear)



Brother QL-820NWB label printer (rear)



- a. Connect a LAN cable to the LAN port on the back of the printer.

Tip: Use a straight-through Category 5 (or greater) twisted-pair cable for 10BASE-T or 100BASE-TX Fast Ethernet Network.

3. Press the Power button to turn the label printer on.



4. (Optional) If you see Template Mode menu and the incorrect label size displayed, disable it.



- a. Press Menu, navigate to Template Settings and turn off the Template Mode setting.

5. Select your label printer (Ethernet).

After you finish

(Optional) Print a test badge.

Parent topic: [Configuring the ClearID Self-Service Kiosk label printer \(Brother QL-820NWBc, QL-820NWB, or QL-810W\)](#)

Browse

- [Firewall ports used in ClearID](#)

13.6 | Configuring the ClearID Self-Service Kiosk label printer (Brother TD-4550DNWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the Brother TD-4550DNWB label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother TD-4550DNWB Quick Setup Guide](#)
- [Brother TD-4550DNWB User Guide](#)
- [Brother TD-4550DNWB online User Guide \(HTML\)](#)
- [Brother TD-4550DNWB LED status indicators](#)

What you should know

Best Practice: Use only one label printer per kiosk and [pair the printer with the kiosk using Bluetooth](#).

If you require one label printer to be used with many kiosk devices, or you need the label printer far away from the kiosk devices use Wi-Fi or Ethernet. For example, two kiosks by the entrance and one label printer on the reception desk.

Procedure

Choose one of the following:

- [Configuring Bluetooth mode \(Brother TD-4550DNWB\)](#)
- [Configuring Wi-Fi mode \(Brother TD-4550DNWB\)](#)
- [Configuring Ethernet mode \(Brother TD-4550DNWB\)](#)

After you finish

From time to time you might need to order supplies, replace the coin cell battery, or clean the label printer.

For more information, see *Brother TD-4550DNWB Quick Setup Guide* and *Brother TD-4550DNWB User Guide*.

Browse

- [Brother TD-4550DNWB Label Printer FAQs](#)
- [Brother TD-4550DNWB printer supplies](#)

Browse

- [Supported devices for ClearID](#)

13.6.1 | Configuring the ClearID Self-Service Kiosk label printer for Bluetooth mode (Brother TD-4550DNWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother TD-4550DNWB Quick Setup Guide](#)
- [Brother TD-4550DNWB User Guide](#)
- [Brother TD-4550DNWB online User Guide \(HTML\)](#)
- [Brother TD-4550DNWB LED status indicators](#)

What you should know

When using the Brother TD-4550DNWB label printer in Bluetooth printing mode, the following applies:

- One label printer can be paired with only one kiosk.
- The label printer must be within 30ft of the kiosk.

Procedure

1. Plug printer AC adapter into a power outlet and connect the power lead to the label printer.



2. Press the Power button to turn the label printer on.



3. Press the Menu button.



4. Use the arrow buttons to navigate the label printer menu.



- a. Select BLUETOOTH > BLUETOOTH (On/Off) > On in the settings menu and press OK.



- b. Select BLUETOOTH > Automatic Reconnection (On/Off) > On in the settings menu and press OK.

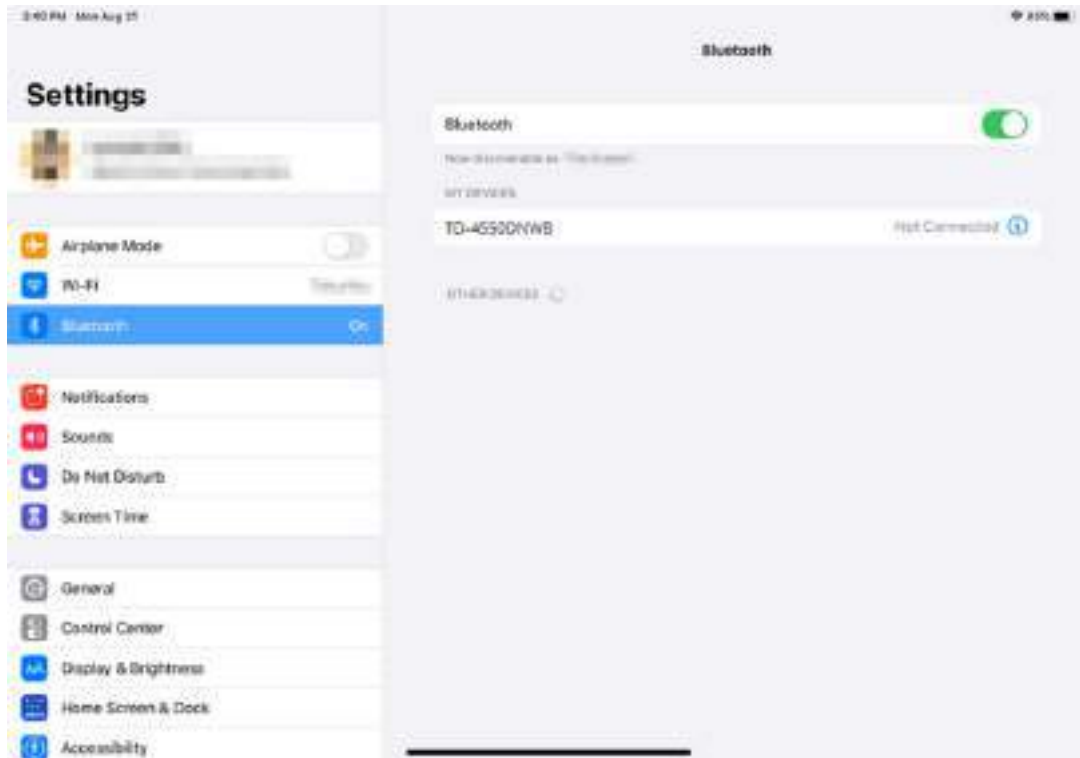


5. Pair your Bluetooth label printer with your ClearID Self-Service Kiosk iPad.

- a. In the Self-Service Kiosk mobile app, tap Settings (⚙️).
b. In the Printing section, tap the slider control to select Bluetooth.



6. On your iPad, navigate to the Apple Settings icon, tap Settings > Bluetooth.
a. (Optional) If Bluetooth is disabled, tap the slider to enable Bluetooth.



b. Click the correct printer to pair the ClearID Self-Service Kiosk iPad with your printer.

7. In the Self-Service Kiosk mobile app, tap Settings (⚙️).



a. In the Printing section, check that your Brother TD-4550DNWB printer is displayed.

Tip: If the printer is not displayed or bluetooth is not selected, tap WiFi then tap Bluetooth to trigger discovery again.

After you finish

(Optional) Print a test badge.

Parent topic: Configuring the ClearID Self-Service Kiosk label printer (Brother TD-4550DNWB)

Browse

- Firewall ports used in ClearID

13.6.2 | Configuring the ClearID Self-Service Kiosk label printer for Wi-Fi mode (Brother TD-4550DNWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- Brother TD-4550DNWB Quick Setup Guide
- Brother TD-4550DNWB User Guide
- Brother TD-4550DNWB online User Guide (HTML)
- Brother TD-4550DNWB LED status indicators

What you should know

- One label printer can support up to five self-service kiosks
- The label printer must be on the same Wi-Fi network as the Genetec ClearID™ Self-Service Kiosk iPad.
 - The Wi-Fi network must be enabled for use and support the following:
 - Bonjour - required for device search.
 - SNMP - required to check printer status information.
 - UDP or TCP Port 9100 - required to send print data.

Procedure

1. Plug printer AC adapter into a power outlet and connect the power lead to the label printer.



2. Press the Power button to turn the label printer on.



3. Press the Menu button.



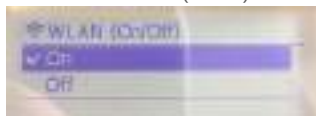
4. Use the arrow buttons to navigate the label printer menu.



5. Scroll down to the WLAN (6/8) settings and press OK.



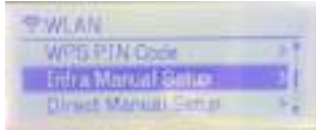
- a. Select WLAN WLAN (On/Off) > On and press OK .



- b. In the Network Mode menu items, select Infrastructure Mode and press OK.



6. Scroll down to Infra Manual Setup and press OK.



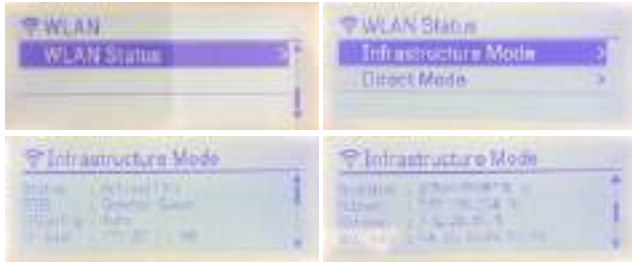
- a. After the search completes, scroll down and select your Wi-Fi network from the Service Set Identifier (SSID) list and press OK.



NOTE: Typically this network is a Wi-Fi network with AirPrint enabled.

- b. When prompted enter the Wi-Fi password.

7. Navigate to WLAN Status > Infrastructure Mode and press OK to verify your Wi-Fi network status and IP address.



Tip: Make a note of the SSID (Wi-Fi network) and IP Addr (Label Printer IP) for later use.

- The SSID is used to verify that you are on the same Wi-Fi network as the ClearID Self-Service Kiosk iPad.
- The IP address is used later when selecting a label printer to verify you have the correct printer.

8. Select your label printer (Wi-Fi).

After you finish

(Optional) Print a test badge.

Parent topic: [Configuring the ClearID Self-Service Kiosk label printer \(Brother TD-4550DNWB\)](#)

Browse

- [Firewall ports used in ClearID](#)

13.6.3 | Configuring the ClearID Self-Service Kiosk label printer for Ethernet mode (Brother TD-4550DNWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother TD-4550DNWB Quick Setup Guide](#)
- [Brother TD-4550DNWB User Guide](#)
- [Brother TD-4550DNWB online User Guide \(HTML\)](#)
- [Brother TD-4550DNWB LED status indicators](#)

What you should know

- One label printer can support up to five self-service kiosks

IMPORTANT: Do not connect this product to any LAN connection that is subject to overvoltages.

Procedure

1. Plug printer AC adapter into a power outlet and connect the power lead to the label printer.



2. Make sure that the printer is turned OFF before connecting the LAN cable.



- a. Connect a LAN cable to the LAN port on the back of the printer.

Tip: Use a straight-through Category 5 (or greater) twisted-pair cable for 10BASE-T or 100BASE-TX Fast Ethernet Network.

3. Press the Power button to turn the label printer on.



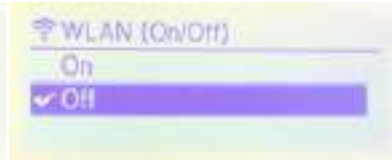
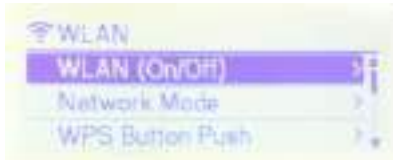
4. Press the Menu button.



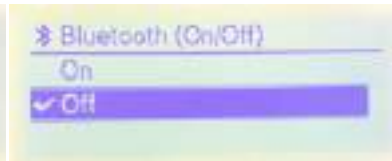
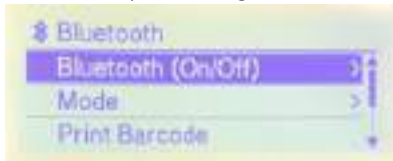
5. Use the arrow buttons to navigate the label printer menu.



6. From the label printer Settings menu, turn OFF WLAN (Wi-Fi).



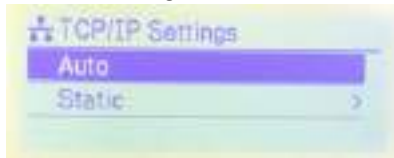
7. From the label printer Settings menu, turn OFF Bluetooth.



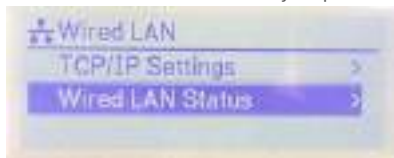
8. Scroll down to the Wired LAN (5/8) settings and press OK.



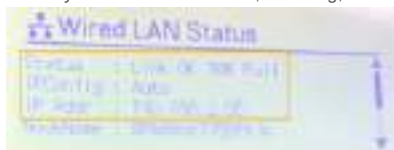
- a. Click TCP/IP Settings and select AUTO.



- b. Click Wired LAN Status to check your printer.



- c. Check your connection Status, IPConfig, and IP Addr.



Tip: Make a note of your IP address and other settings for later use when selecting your printer.

9. Select your label printer (Ethernet).

After you finish

(Optional) Print a test badge.

Parent topic: Configuring the ClearID Self-Service Kiosk label printer (Brother TD-4550DNWB)

Browse

- Firewall ports used in ClearID

13.7 | Selecting a ClearID Self-Service Kiosk label printer

Before you can print visitor badges from the Genetec ClearID™ Self-Service Kiosk, you must select a label printer.

Before you begin

Do one of the following:

- Configure the Brother QL-820NWBc or QL-820NWB Self-Service Kiosk Label Printer
- Configure the Brother TD-4550DNWB Self-Service Kiosk Label Printer

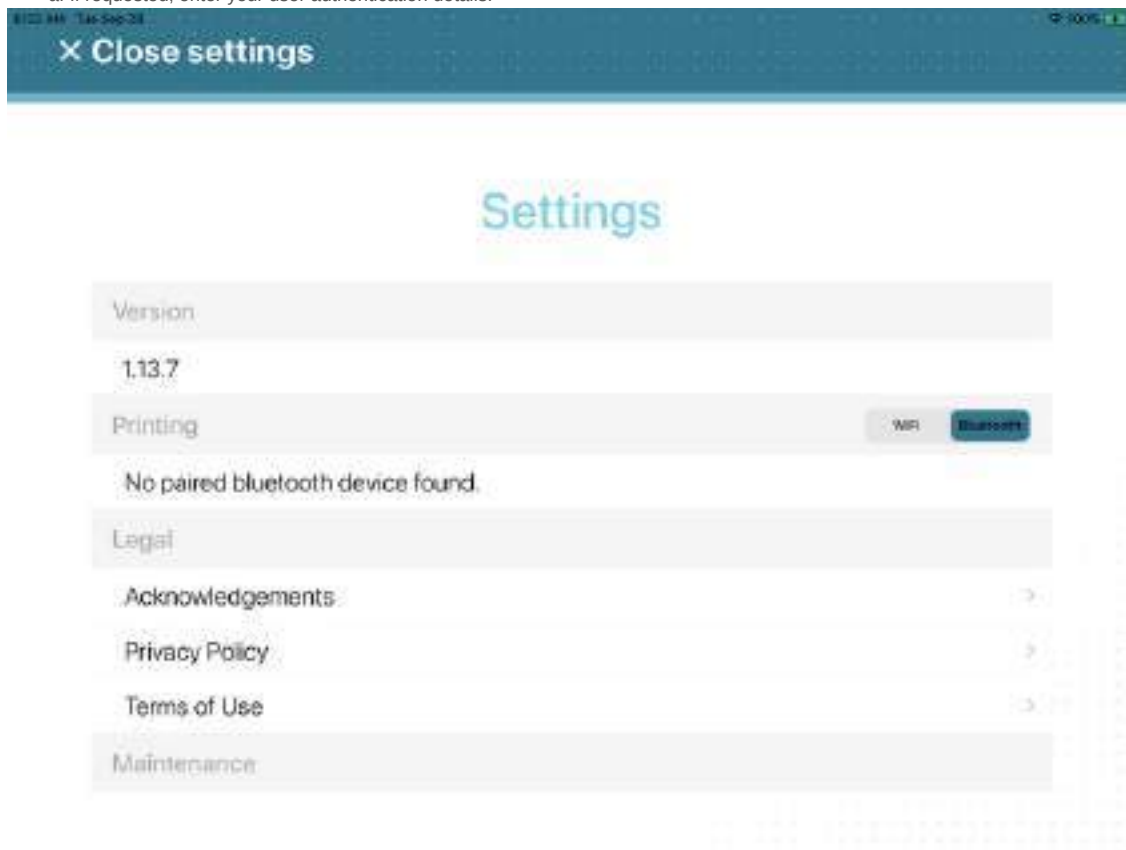
What you should know

Wi-Fi or Ethernet only: Make sure that you have the IP address of the label printer so that you can verify your selection.

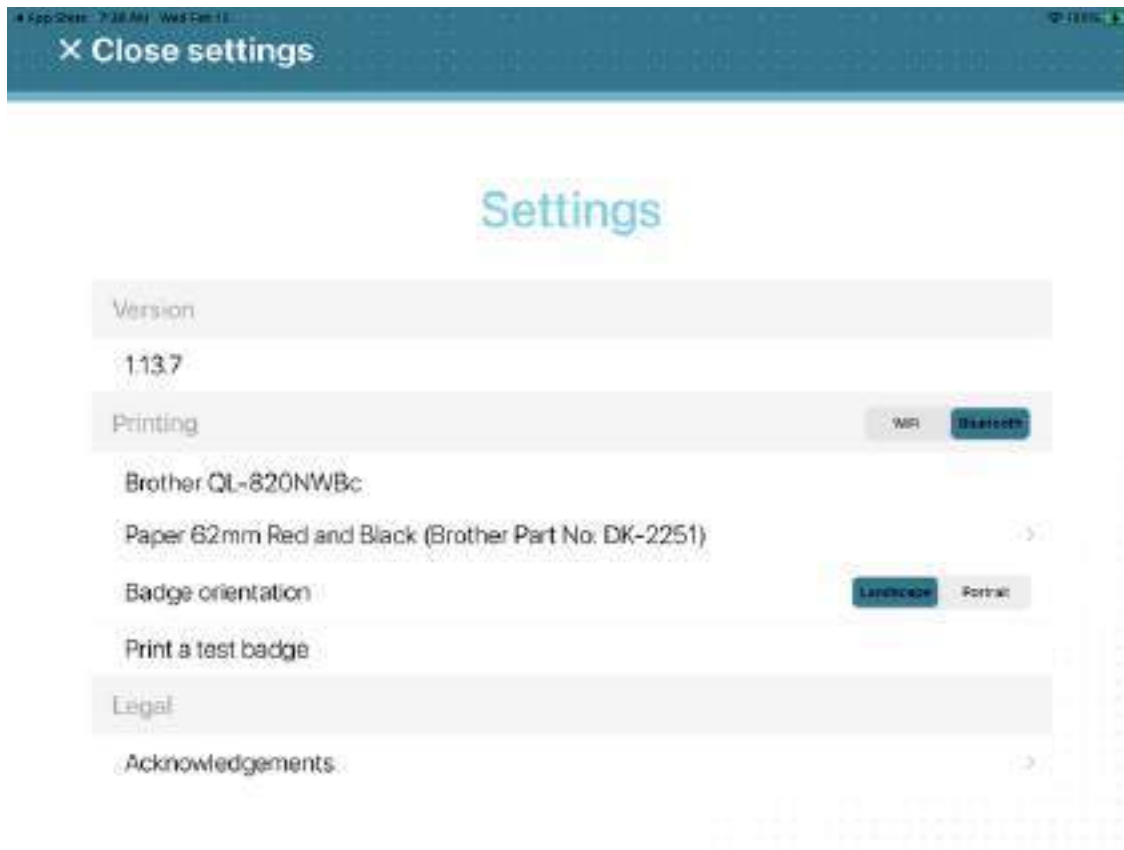
Procedure

To select a Bluetooth kiosk label printer:

1. In the Self-Service Kiosk mobile app, tap Settings (⚙️).
2. On the Settings page, tap Bluetooth to select the printing mode you require.
 - a. If requested, enter your user authentication details.



3. If you selected Bluetooth, in the Printing section, your selected printer should be displayed.

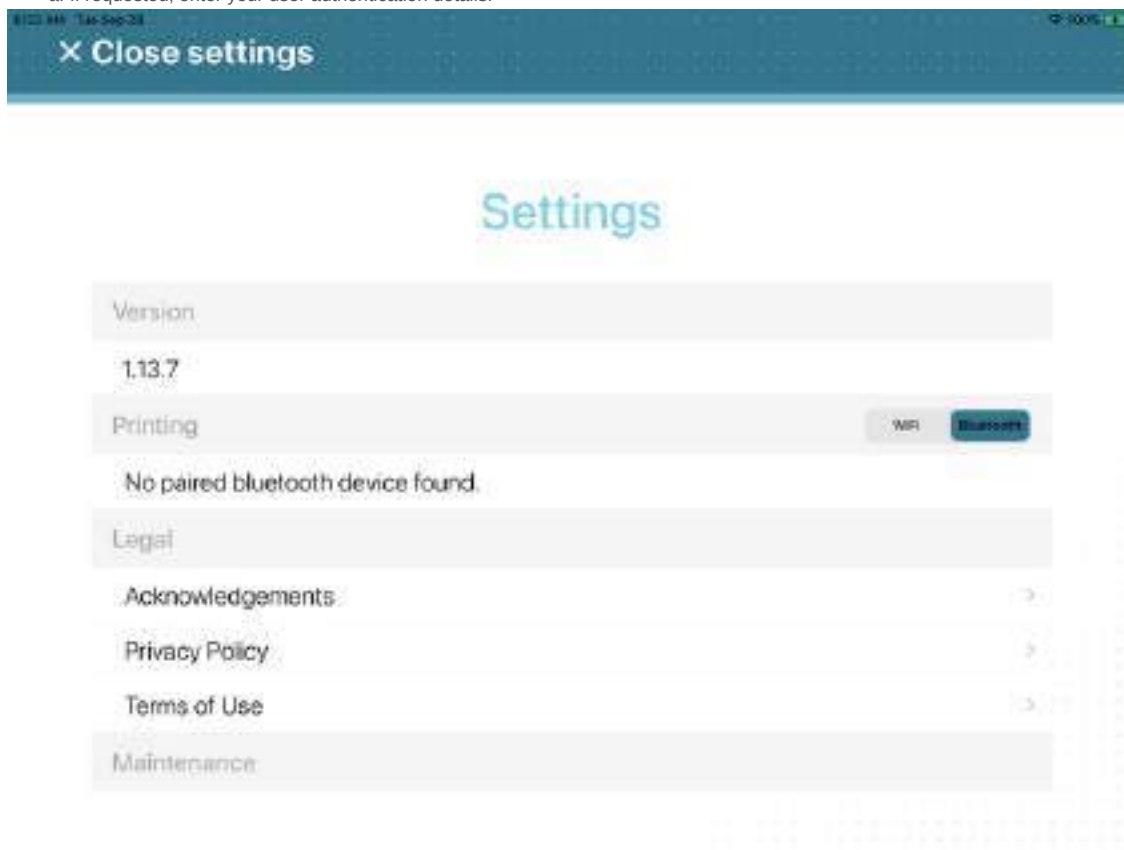


Tip: Bluetooth mode: If the printer is not displayed or bluetooth is not selected, tap WiFi then tap Bluetooth to trigger discovery again.

4. Tap Close settings to complete your printer selection setup.

To select a Wi-Fi kiosk label printer:

1. In the Self-Service Kiosk mobile app, tap Settings (👤).
2. On the Settings page, tap WiFi to select the printing mode you require.
 - a. If requested, enter your user authentication details.



3. Choose one of the following:
 - Discover WiFi printer
 - Set printer manually (IP address)

Genetec ClearID®; User Guide

Displayed in the header

- a. If you selected Discover WiFi printer, wait for the Printers list to be displayed then select your printer.
Verify that the IP address of the printer you are selecting matches the IP address seen during printer configuration.
Tip: Wi-Fi mode: If the printer is not displayed or Wi-Fi is not selected, tap Bluetooth then tap WiFi to trigger discovery again.
- b. If you selected Set printer manually (IP address), enter the IP address of the printer and tap Save.



4. Tap Close settings to complete your printer selection setup.

To select an Ethernet kiosk label printer:

1. In the Self-Service Kiosk mobile app, tap Settings (⚙️).
2. On the Settings page, tap WiFi to select the printing mode you require.
 - a. If requested, enter your user authentication details.



3. Choose one of the following:
 - Discover WiFi printer
 - Set printer manually (IP address)

- a. If you selected Discover WiFi printer, wait for the Printers list to be displayed then select your printer.
Verify that the IP address of the printer you are selecting matches the IP address seen during printer configuration.
Tip: Wi-Fi mode: If the printer is not displayed or Wi-Fi is not selected, tap Bluetooth then tap WiFi to trigger discovery again.
- b. If you selected Set printer manually (IP address), enter the IP address of the printer and tap Save.



4. Tap Close settings to complete your printer selection setup.

After you finish

Print a test badge.

13.8 | Printing a test badge from the ClearID Self-Service Kiosk

To help you understand if the printer is working as expected, you can print a test badge. This test print can be performed either after first initial setup or after replacing a label roll.

Before you begin

- Select a kiosk label printer.
- Make sure that labels are loaded in the printer.
- Make sure that labels are correctly aligned.

What you should know

The Brother QL-820NWBc, QL-820NWB, and QL-810W label printers can print either Black or Red and Black badges:

- 62mm Black (Brother Part No: DK-2205)
- 62mm Red and Black (Brother Part No: DK-2251)

The Brother TD-4550DNWB label printer can only print Black badges:

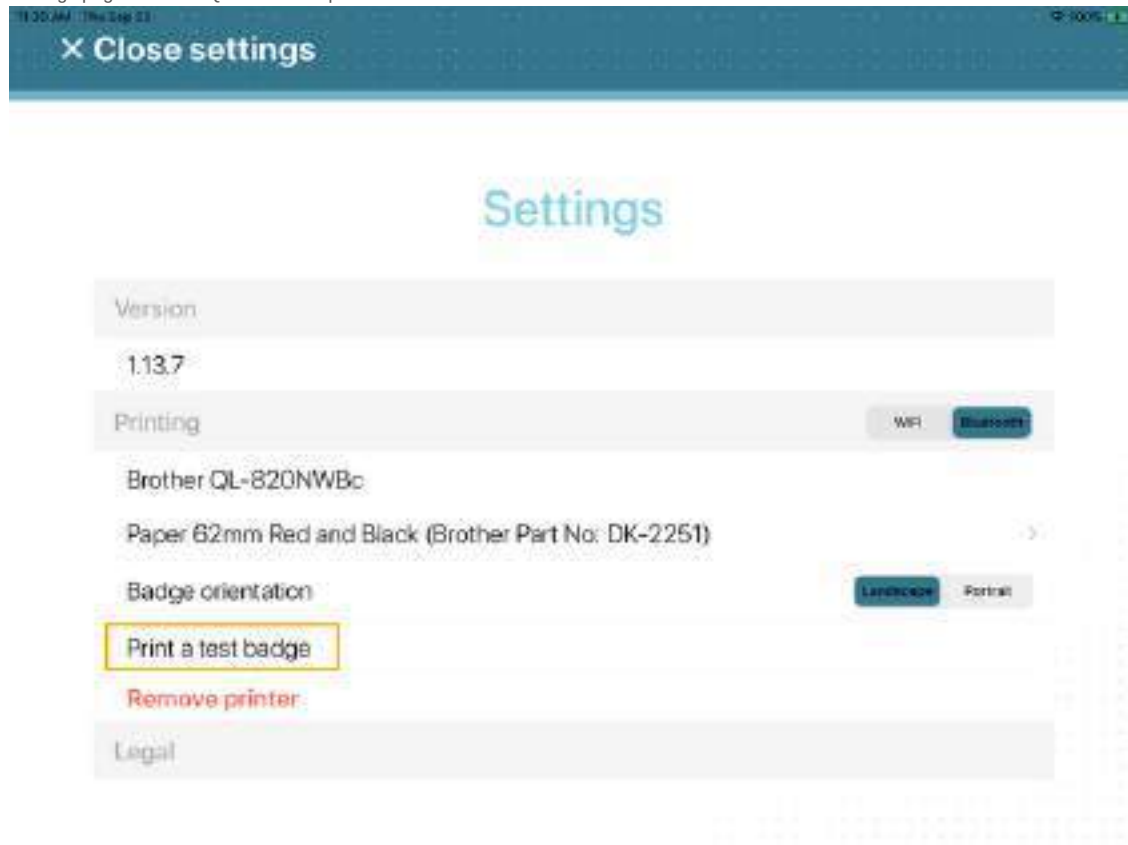
- 57mm Black (Brother Part No: RD001U1S)
- IMPORTANT: The labels for the Brother TD-4550DNWB printer MUST be orientated correctly otherwise badge printing issues can occur.

Badges can be printed in either *Portrait* or *Landscape* format.

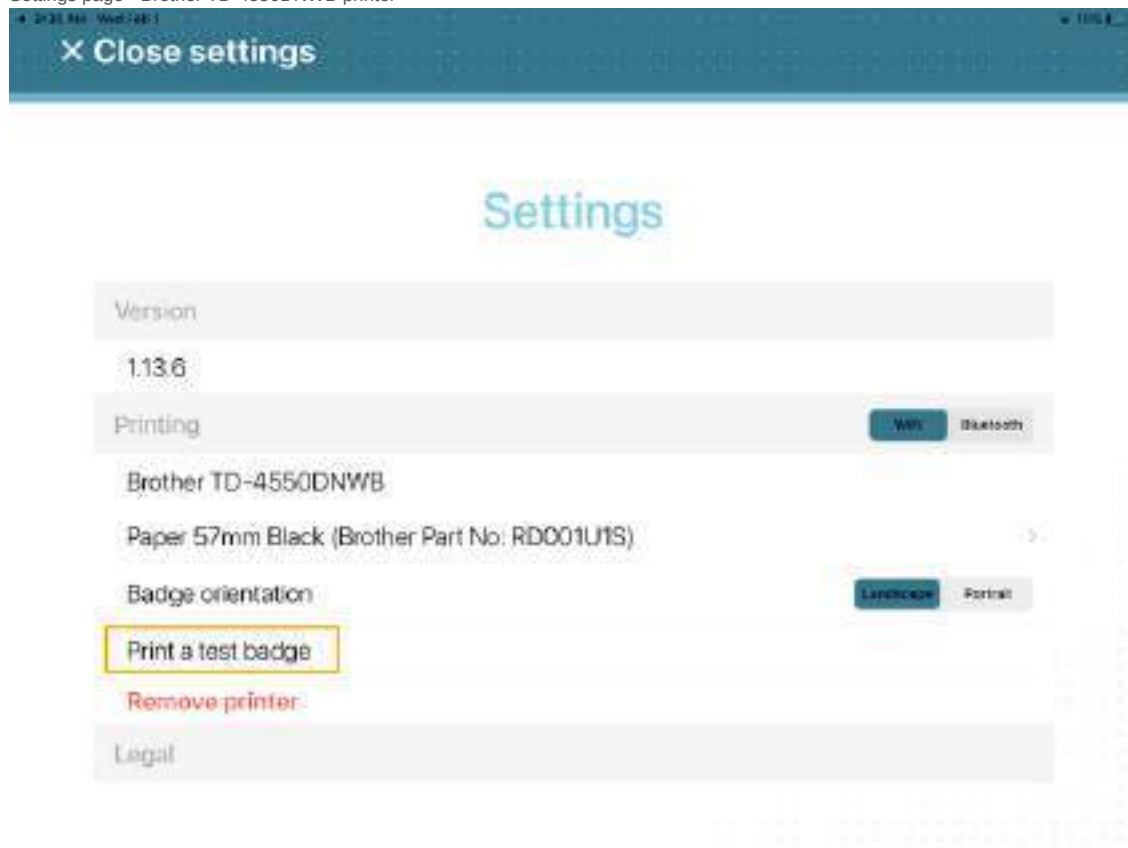
Procedure

1. In the Genetec ClearID™ Self-Service Kiosk mobile app, tap settings (⚙️).
2. In the Settings page, tap Print a test badge.

Settings page - Brother QL-820NWBc printer



Settings page - Brother TD-4550DNWB printer



3. Collect and examine your test badge.



Badge dimensions: 10 x 6.1 cm's or 3.94 x 2.56 inches.

NOTE: When printing to a Brother TD-4550DNWB label printer, your badges are printed in black and white.

Results

You are now ready for visitors to use the ClearID Self-Service Kiosk and print their own visitor badges during their check-in.

After you finish

From time to time you might need to order supplies, replace the coin cell battery, recharge the optional battery unit (Brother QL-820NWBc or QL-820NWB only), or clean the label printer.

For more information, see the third-party user guide documentation for your printer.

Browse

- [ClearID Self-Service Kiosk label printer issues](#)

13.9 | Resetting the ClearID Self-Service Kiosk mobile app

In some situations, you might need to perform a hard reset of the Genetec ClearID™ Self-Service Kiosk mobile app. For example, if you encounter issues with selecting the label printer, printing labels, listing people, or if you want to move the kiosk to another site.

Before you begin

- Make sure that you have your Apple ID information.
- Make sure that you have your Wi-Fi network information.

What you should know

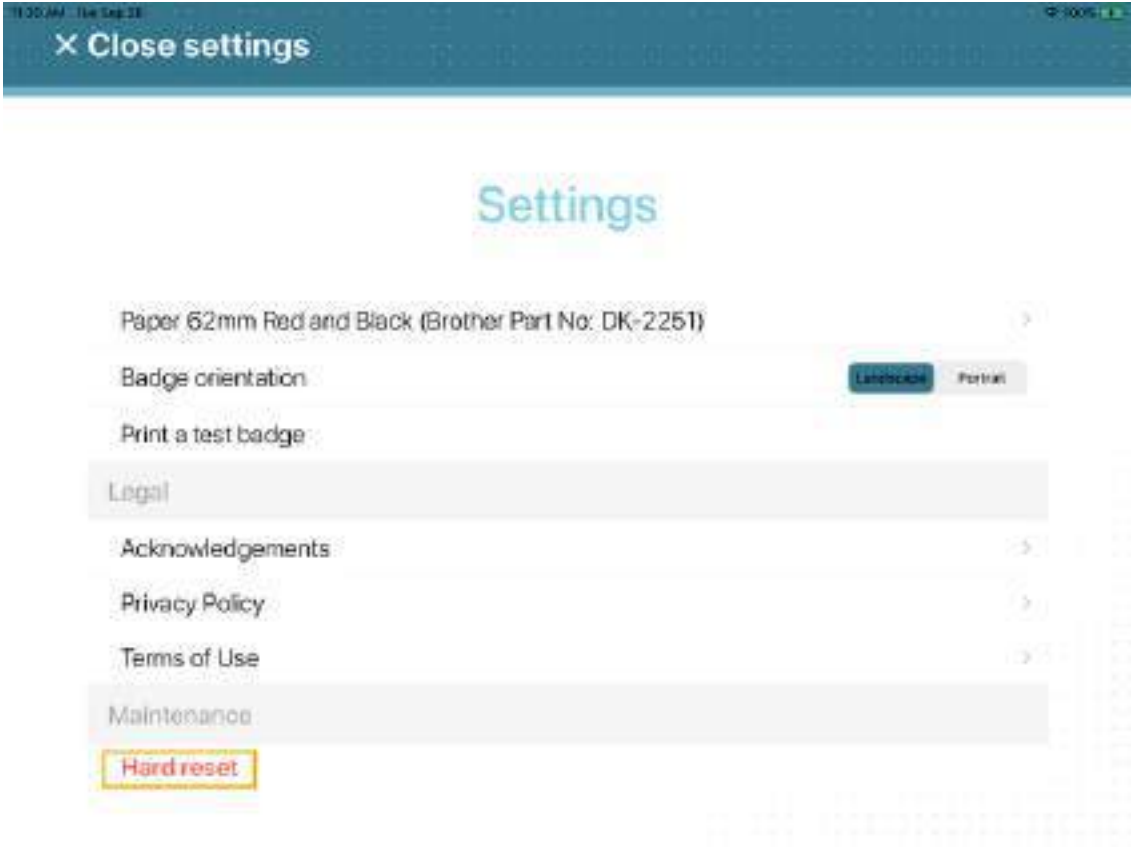
- Only an *administrator* or a *Site owner* can generate a device activation code in ClearID.

CAUTION:

The hard reset action erases all application data, user data, and visit, check-in, check-out information from the Kiosk device and performs a hard reset of the mobile app. If you proceed, you must register the kiosk device again.

Procedure

1. In the Self-Service Kiosk mobile app, tap Settings (👤).
2. In the Settings page, scroll to the bottom of the page and in the Maintenance section tap Hard reset.



3. Configure your Self-Service Kiosk iPad.
4. Configure your Self-Service Kiosk label printer.
5. Select your Self-Service Kiosk label printer.
6. Print a test badge.

Results

Your Self-Service Kiosk is now ready for use.
Browse

- ClearID Self-Service Kiosk label printer issues

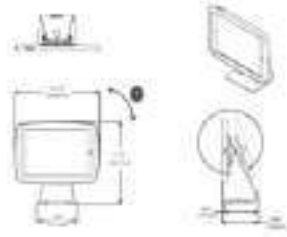
13.10 | ClearID Self-Service Kiosk options

Use the following information to help you understand the Genetec ClearID™ Self-Service Kiosk license, kiosk, and accessory options that are available.

ClearID Self-Service Kiosk license options

Item description	Part	Item
Kiosk license subscription One Genetec ClearID™ kiosk license for one, three, or five years NOTE: The ClearID Self-Service Kiosk app on an iPhone doesn't need to be licensed.	• CID-KIOSK-LIC-1Y • CID-KIOSK-LIC-3Y • CID-KIOSK-LIC-5Y	Kiosk subscription license

ClearID Self-Service Kiosk options

Item description	Part	Item
Kiosk tabletop stand Apple iPad (Wi-Fi) with one year of Apple Care Table top kiosk kit with iPad enclosure, tabletop stand, and one iPad charging cable. (Printer <u>not included</u>) NOTE: Depending on your check-in requirements, the kiosk iPad housing on this tabletop stand can be configured for use in either <i>Portrait</i> or <i>Landscape</i> mode.	VM-KIOSK-TABLETOP-KIT¹	
Tabletop kit Table top kiosk kit with iPad enclosure, tabletop stand, and one iPad charging cable. (iPad and Printer <u>not included</u>) NOTE: Depending on your check-in requirements, the kiosk iPad housing on this tabletop stand can be configured for use in either <i>Portrait</i> or <i>Landscape</i> mode.	VM-TABLETOP-KIT¹	
Kiosk floor stand kit Apple iPad (Wi-Fi) with one year of Apple Care Floor stand kit with iPad enclosure, floor stand, one iPad charging cable, and a printer shelf (Printer <u>not included</u>) NOTE: Depending on your check-in requirements, the kiosk iPad housing on this floor stand can be configured for use in either <i>Portrait</i> or <i>Landscape</i> mode.	VM-KIOSK-FLOORSTAND-KIT¹	
Floor stand kit Floor stand kit with iPad enclosure, floor stand, one iPad charging cable, and a printer shelf (iPad and Printer <u>not included</u>) NOTE: Depending on your check-in requirements, the kiosk iPad housing on this floor stand can be configured for use in either <i>Portrait</i> or <i>Landscape</i> mode.	VM-FLOORSTAND-KIT¹	

IMPORTANT: ¹ For EMEA, APAC, and some LATCAR regions, an adapter kit (VM-KIOSK-WORLD-ADAPTER-KIT) is added to your order once you've specified your region.

The VM-KIOSK-WORLD-ADAPTER-KIT part number includes a World Travel Adapter kit and power adapter plugs to fit different electrical outlets around the world. These include North America, Japan, China, United Kingdom, Continental Europe, Korea, Australia, Hong Kong, and Brazil. Without this kit, the plug isn't compatible with the electrical outlets in your region.

ClearID Self-Service Kiosk accessories

Item description	Part	Item
World travel adapter kit Adapter plug kit that includes plugs with prongs that fit different electrical outlets around the world	VM-KIOSK-WORLD-ADAPTER-KIT	International adapter plug kit for the kiosk iPad
Visitor label printer Brother QL-820NWBc thermal printer - Network (Ethernet), Wi-Fi, and Bluetooth - Prints black and red labels NOTE: Only the Brother DK Roll - 62mm Black (Brother Part No: DK-2205) or 62mm Red and Black (Brother Part No: DK-2251) labels are supported.	Brother QL-820NWBc Kit part numbers: - VM-KIOSK-PRINTER-NA-KIT - VM-KIOSK-PRINTER-AU-KIT - VM-KIOSK-PRINTER-BRA-KIT - VM-KIOSK-PRINTER-EU-KIT - VM-KIOSK-PRINTER-IN-KIT - VM-KIOSK-PRINTER-UK-KIT	

For more information or to order kiosk parts, see [Genetec Parts Manager](#).
Browse

- License options for ClearID system integration
- Supported devices for ClearID

Browse

- [ClearID Self-Service Kiosk Datasheet \(2 pages\)](#)

13.10.1 | ClearID Self-Service Kiosk floor stand

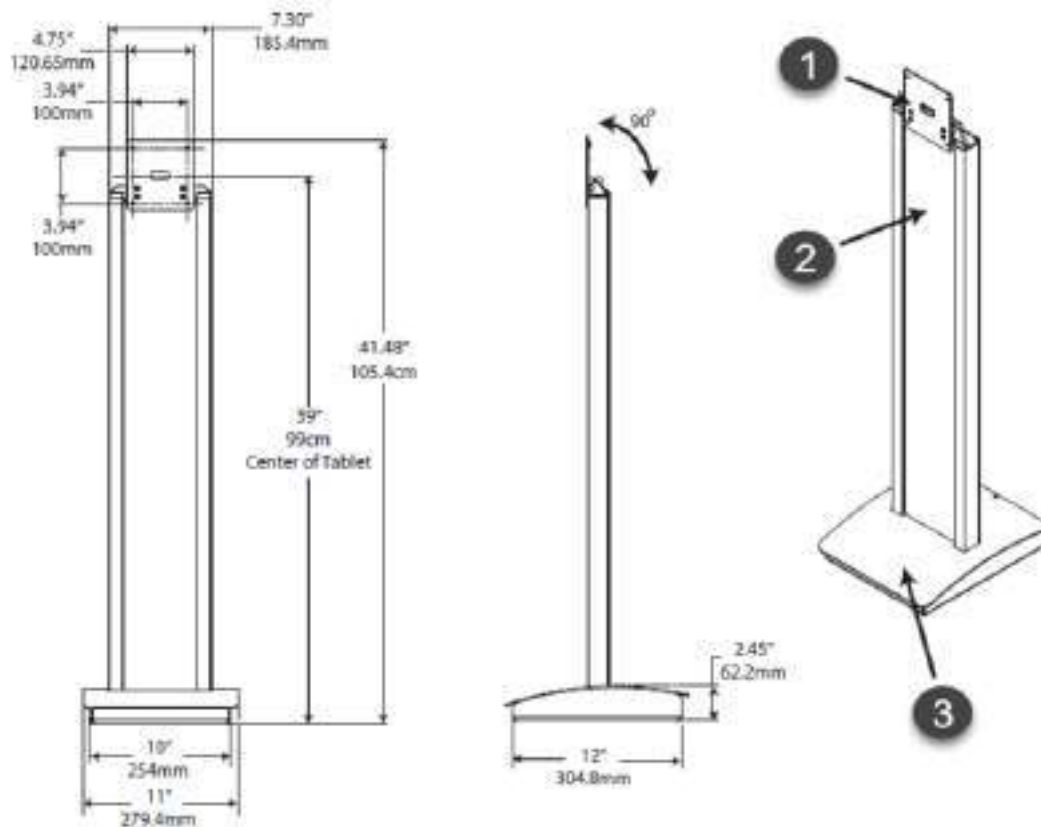
Use the following information to help you understand the Genetec ClearID™ Self-Service Kiosk floor stand dimensions, mounting, and features.



NOTE: Depending on your check-in requirements, the ClearID Self-Service Kiosk iPad housing can be configured on this floor stand for use in either *Portrait* or *Landscape* mode.

Floor stand dimensions

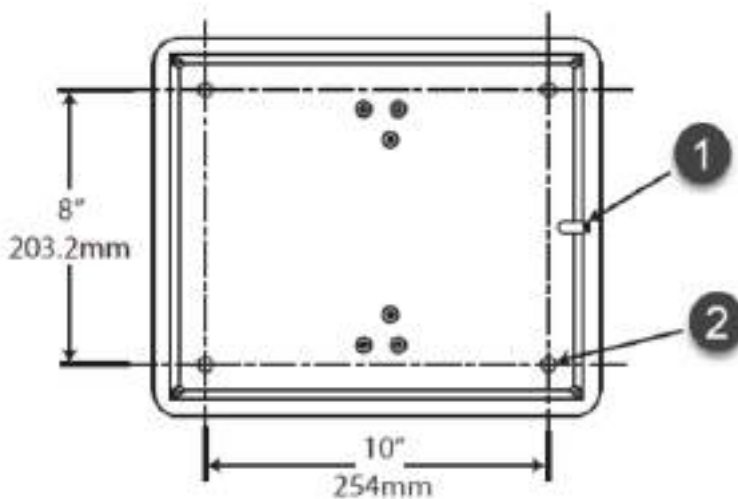
The following diagram illustrates the floor stand dimensions including the height and footprint of the stand.



- ¹ Mount supports any tablet enclosure with a standard VESA mount (100mm x 100mm) or a 90° degree rotation adapter.
- ² Removable signage panel (included).
- ³ Removable cover provides access to the storage area for the power supply.

Floor mount

The following diagram illustrates the floor mount dimensions and underside view of the kiosk floor stand.



- ¹ Opening for power supply cable.
- ² 4x floor mounting holes for 0.25inch or 6mm screw hardware (not included) used to secure the floor stand to the floor surface.

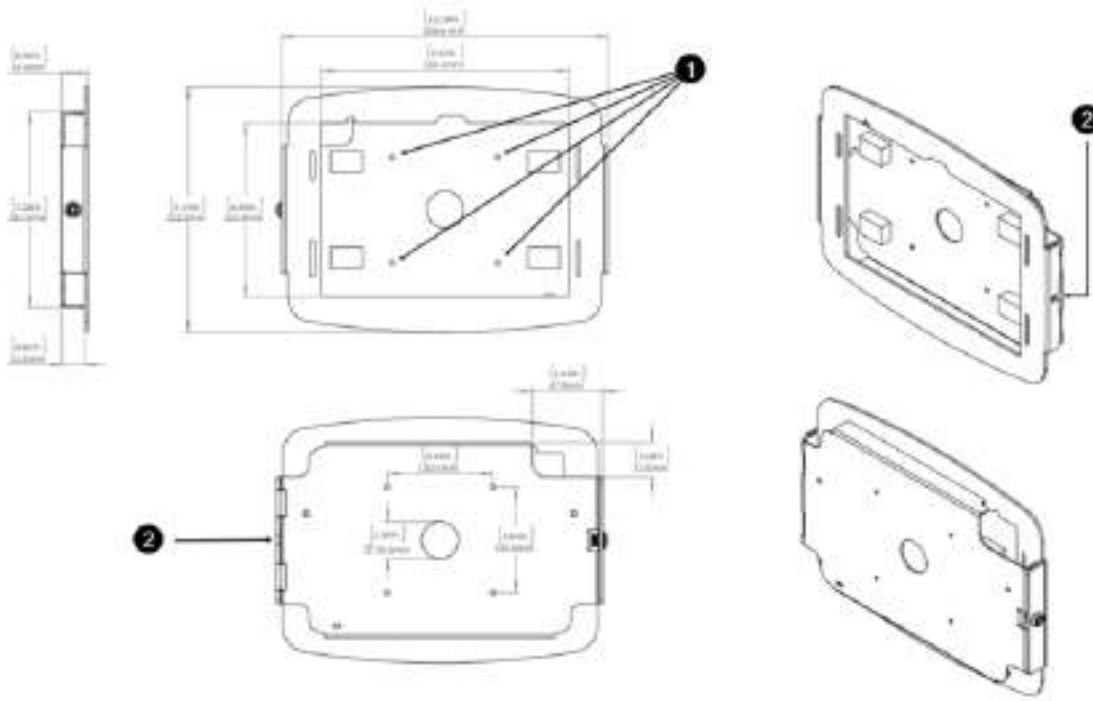
Floor stand features

The floor stand includes the following features:

- Free standing or floor mount option.
- The mount supports any tablet enclosure with a standard VESA mount (100mm x 100mm).
- Tablet power supply can be stored in the base.
- Tablet power cable can be concealed in the legs.
- The enclosure mounting surface can be rotated 90° degrees. This rotation function means that the iPad housing can be orientated on this floor stand for use in either *Portrait* or *Landscape* mode.

iPad enclosure

The following diagram illustrates the floor stand iPad enclosure dimensions.



¹ 4x holes for mounting iPad enclosure to floor stand.

² Opening for power supply cable.

Parent topic: [ClearID Self-Service Kiosk options](#)

Browse

- [ClearID Self-Service Kiosk options](#)
- [About ClearID Self-Service Kiosk](#)

Browse

- [ClearID Self-Service Kiosk Datasheet \(2 pages\)](#)

13.10.2 | ClearID Self-Service Kiosk floor stand printer shelf

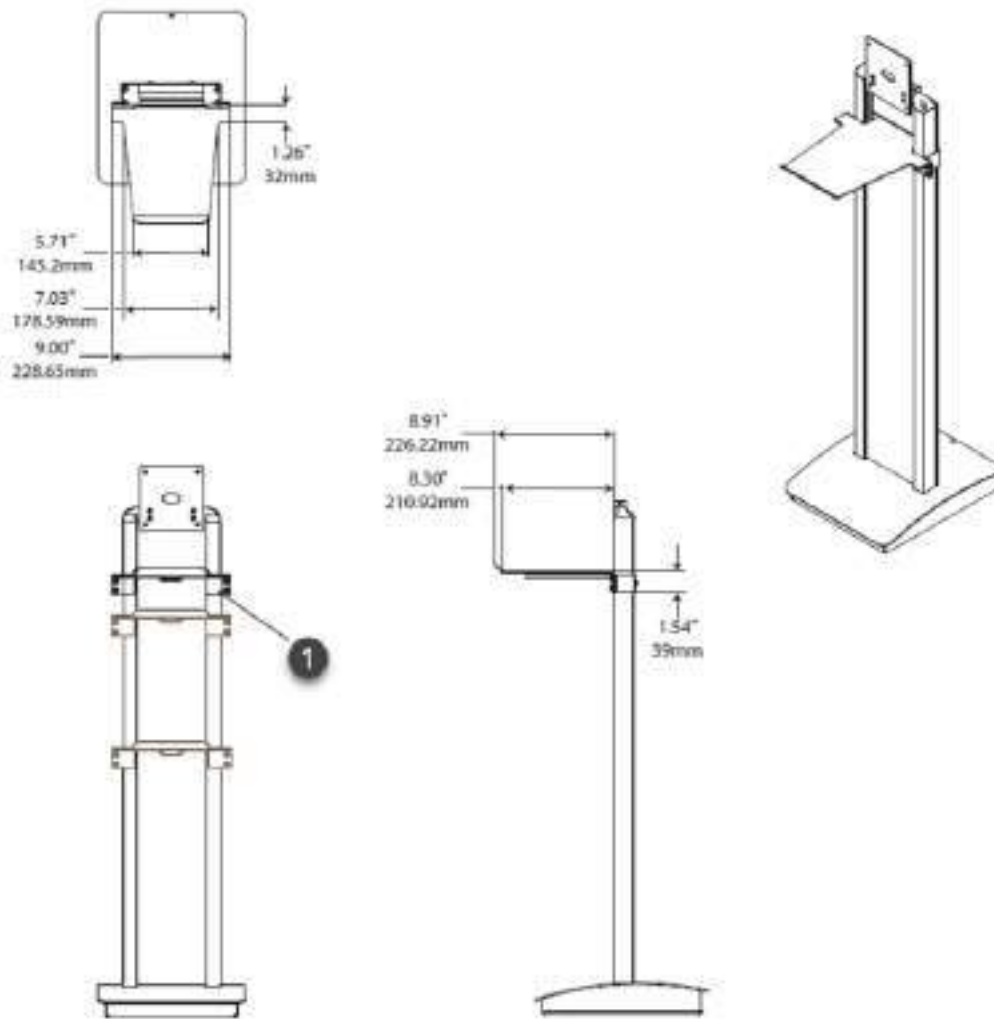
Use the following information to help you understand the dimensions and features of the printer shelf for the Genetec ClearID™ Self-Service Kiosk floor stand.



NOTE: Depending on the size and model of printer that you choose, you might need to trim or modify the center panel (graphic panel) of the floor stand to allow for cable access.

Printer shelf dimensions

The following diagram illustrates the printer shelf dimensions.



¹ Height adjustable printer shelf.

Printer shelf features

The printer shelf includes the following features:

- Mounts to floor stand
- Height adjustable
- Fits various printers

Parent topic: [ClearID Self-Service Kiosk options](#)

Browse

- [ClearID Self-Service Kiosk options](#)
- [About ClearID Self-Service Kiosk](#)

Browse

- [ClearID Self-Service Kiosk Datasheet \(2 pages\)](#)

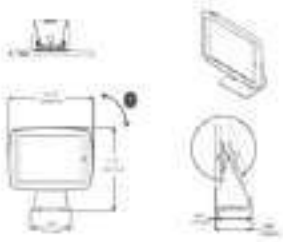
13.10.3 | ClearID Self-Service Kiosk tabletop stand

Use the following information to help you understand the Genetec ClearID™ Self-Service Kiosk tabletop stand dimensions, mounting, and features.



Tabletop stand dimensions

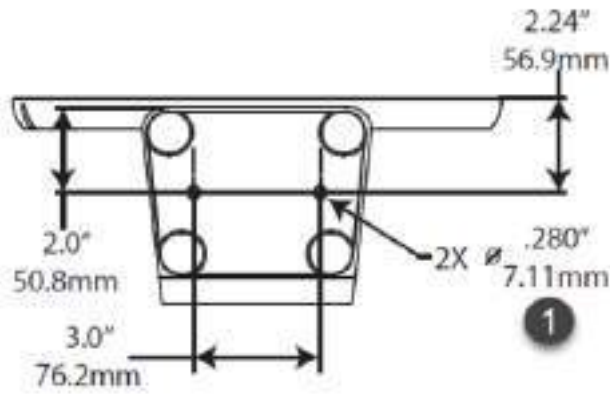
The following diagram illustrates the tabletop stand dimensions including the height and footprint of the stand.



¹ 90° rotation (portrait or landscape orientation).

Tabletop stand mounting

The following diagram illustrates the tabletop mount dimensions.



¹ 2x Tabletop mounting holes for 0.25inch or 6mm screw hardware (not included).

Tabletop stand features

The tabletop stand includes the following features:

- 90° degree rotation (portrait or landscape orientation).
- Flip tablet function.
- Counter mounting option.

Parent topic: [ClearID Self-Service Kiosk options](#)

Browse

- [ClearID Self-Service Kiosk options](#)
- [About ClearID Self-Service Kiosk](#)

Browse

- [ClearID Self-Service Kiosk Datasheet \(2 pages\)](#)

13.11 | Identity document types in ClearID

Use the following information to help you understand all the different identity document types that are supported in Genetec ClearID™ Self-Service Kiosk.

An extensive list of ID types can be used when using the ClearID Self-Service Kiosk during check-in.

NOTE: All identity document processing is performed locally on the ClearID Self-Service Kiosk iPad. This local processing during check-in ensures that ID data or pictures are never sent to the cloud for maximum security and compliance.

Supported identity documents (Asia)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Afghanistan	ID Card	تذکره الکترونیک	Front, back	Latin
Afghanistan	Paper Passport ^{BETA}	پاسپورٹ	Bio-data page	Latin
Armenia	ID Card	Նույնականացման քարտը	Front, back	Latin
Azerbaijan	ID Card	Şəxsiyyət vəsiqəsi	Front, back	Latin
Azerbaijan	Polycarbonate Passport ^{BETA}	Pasport	Bio-data page	Latin
Bangladesh	Driving License ^{BETA}	মোটর ড্রাইভিং লাইসেন্স	Front, back	Latin
Bangladesh	ID Card	জাতীয় পরিচয় পত্র	Front, back	Latin
Bangladesh	Paper Passport	পাসপোর্ট	Bio-data page	Latin
Brunei	ID Card	Kad Pengenalan (Kuning)	Front, back	Latin
Brunei	Military ID ^{BETA}	Kad Pengenalan Tentera (ABDB)	Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Brunei	Residence Permit ^{BETA}	Kad Pengenalan (Ungu)	Front, back	Latin
Brunei	Temporary Residence Permit ^{BETA}	Kad Pengenalan (Hijau)	Front, back	Latin
Cambodia	Driving License ^{BETA}	ប័ណ្ណបើកបរ	Front	Latin
Cambodia	ID Card	អត្តសញ្ញាណប័ណ្ណសញ្ជាតិខ្មែរ	Front	Latin
Cambodia	Polycarbonate Passport	លិខិតឆ្លងដែន	Bio-data page	Latin
China	ID Card	中华人民共和国居民身份证	Front, back	Latin
China	Paper Passport	中华人民共和国护照	Bio-data page	Latin
Hong Kong	ID Card	香港身份證	Front	Latin
Hong Kong	Polycarbonate Passport ^{BETA}	護照	Bio-data page	Latin
India	ID Card ^{BETA}	Aadhaar card, आधार कार्ड	Front, back	Latin
India	PAN Card	स्थायी खाता संख्या कार्ड	Front	Latin
India	Paper Passport		Bio-data page	Latin
India	Voter ID	भारतीय मतदाता पहचान पत्र	Front, vertical	Latin
India, Gujarat	Driving License ^{BETA}	ડ્રાઇવિંગ લાઇસેન્સ	Front	Latin
India, Karnataka	Driving License	ડ્રાઇવિંગ લાઇસેન્સ	Front	Latin
India, Kerala	Driving License ^{BETA}	ਡ્રાઇવિંગ લાઇસેન્સ	Front, back	Latin
India, Madhya Pradesh	Driving License ^{BETA}	ਡ્રાઇવિંગ લાઇસેન્સ	Front	Latin
India, Maharashtra	Driving License	ડ્રાઇવિંગ લાઇસેન્સ	Front	Latin
India, Punjab	Driving License ^{BETA}	ਡ્રਾઇવિંગ ਲਾਇਸੈਂਸ	Front	Latin
India, Tamil Nadu	Driving License ^{BETA}	ਡ્રਾઇવિંગ લાઇસેન્સ	Front, back	Latin
Indonesia	Driving License	Surat Izin Mengemudi (SIM)	Front	Latin
Indonesia	ID Card	Kartu Tanda Penduduk (KTP)	Front	Latin
Indonesia	Paper Passport	Paspor	Bio-data page	Latin
Japan	Driving License ^{BETA}	運転免許	Front	Latin
Japan	My Number Card	マイナンバーカード	Front	Latin
Japan	Paper Passport	旅券	Bio-data page	Latin
Japan	Residence Permit ^{BETA}	在留カード	Front	Latin
Kazakhstan	ID Card	Жеке куәлік, Удостоверение личности	Front, back	Latin
Kyrgyzstan	ID Card	идентификациялык карта, идентификационная карта	Front, back	Latin
Malaysia	Driving License	Lesen Memandu	Front	Latin
Malaysia	MyKAS		Front, back	Latin
Malaysia	MyKad		Front, back	Latin
Malaysia	MyKid		Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Malaysia	MyPR		Front, back	Latin
Malaysia	MyPolis ^{BETA}		Front, back	Latin
Malaysia	MyTentera		Front, back	Latin
Malaysia	Refugee ID	UNHCR Card	Front	Latin
Malaysia	Polycarbonate Passport	Pasport	Bio-data page	Latin
Malaysia	i-Kad		Front	Latin
Maldives	ID Card	ދިވެހިރާއްޖޭގެ ޖުމްހޫރިއްޔާގެ ރައްކާތެރިކަން	Front, back	Latin
Myanmar	Driving License	ယာဉ်မောင်းလိုင်စင်	Front, back	Latin
Nepal	Paper Passport	राहदानी	Bio-data page	Latin
Pakistan	Consular ID	National Identity Card for Overseas Pakistanis (NICOP)	Front, back	Latin
Pakistan	ID Card	Computerized National Identity Card (CNIC), Smart National Identity Card (SNIC)	Front, back	Latin
Pakistan	Paper Passport		Bio-data page	Latin
Pakistan, Punjab	Driving License		Front	Latin
Philippines	Driving License		Front	Latin
Philippines	ID Card	PhilSys ID, PhilID	Front, back	Latin
Philippines	Multipurpose ID	Unified Multi-Purpose ID	Front	Latin
Philippines	Paper Passport		Bio-data page	Latin
Philippines	Professional ID	PRC License	Front	Latin
Philippines	Social Security Card	SSS ID	Front	Latin
Philippines	Tax ID ^{BETA}	TIN ID card	Front	Latin
Philippines	Voter ID ^{BETA}		Front	Latin
Singapore	Driving License		Front, back	Latin
Singapore	Employment Pass		Front	Latin
Singapore	Fin Card		Front	Latin
Singapore	ID Card	NRIC (Pink)	Front, back	Latin
Singapore	Resident ID	NRIC (Blue)	Front, back	Latin
Singapore	Polycarbonate Passport		Bio-data page	Latin
Singapore	S Pass		Front, back	Latin
Singapore	Work Permit		Front, back	Latin
South Korea	Driving License	자동차운전면허증	Front	Latin
South Korea	ID Card ^{BETA}	주민등록증	Front	Latin
South Korea	Paper Passport ^{BETA}	여권	Bio-data page	Latin
Sri Lanka	Driving License	රියද්දිරු බලපත්‍රය	Front	Latin

Genetec ClearID®; User Guide

Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Sri Lanka	ID Card	ජාතික හැඳුනුම්පත, தேசிய அடையாள அட்டை	Front, back, vertical	Latin
Sri Lanka	Paper Passport	ගමන් බලපත්‍රය, கடவுச்சீட்டு	Bio-data page	Latin
Taiwan	ID Card ^{BETA}	中華民國國民身分證	Front	Latin
Taiwan	Temporary Residence Permit ^{BETA}	中華民國居留證 (ARC)	Front	Latin
Latin	Latin	Latin	Latin	Latin
Thailand	Alien ID	บัตรประจำตัวคนซึ่งไม่มีสัญชาติไทย (บัตรสีชมพู)	Front	Latin
Thailand	Driving License ^{BETA}	ใบอนุญาตขับรถ	Front, back	Latin
Thailand	ID Card	บัตรประจำตัวประชาชน	Front, back	Latin
Thailand	Polycarbonate Passport	หนังสือเดินทาง	Bio-data page	Latin
Vietnam	Driving License ^{BETA}	Giấy phép lái xe	Front	Latin
Vietnam	ID Card ^{BETA}	Căn cước công dân, Giấy chứng minh nhân dân	Front, back	Latin

Supported identity documents (Europe)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Albania	Driving License	Leje drejtimi	Front	Latin
Albania	Driver Card	Karta e drejtuesit të mjetit	Front	Latin
Albania	ID Card	Letërnjoftim	Front, back	Latin
Albania	Professional DL	Certifikatë aftësimi profesionale	Front	Latin
Albania	Polycarbonate Passport	Pasaportë	Bio-data page	Latin
Austria	Driving License	Führerschein	Front	Latin
Austria	ID Card	Personalausweis	Front, back	Latin
Austria	Paper Passport	Reisepass	Bio-data page	Latin
Austria	Residence Permit ^{BETA}	Aufenthaltstitel	Front, back	Latin
Belarus	Driving License	ВАДЗІЦЕЛЬСКАЕ ПАСВЕДЧАННЕ, ВОДИТЕЛЬСКОЕ УДОСТОВЕРЕНИЕ	Front	Latin
Belarus	Paper Passport	Пашпарт, Паспорт	Bio-data page	Latin
Belgium	Driving License	Rijbewijs, Permis de conduire, Führerschein	Front	Latin
Belgium	ID Card	Identiteitskaart, Carte d'identité, Personalausweis	Front, back	Latin
Belgium	Minors ID	Kids-ID	Front, back	Latin
Belgium	Paper Passport	Paspoort, Passeport, Reisepass	Bio-data page	Latin
Belgium	Residence Permit	Verblijfstitel, Titre de Séjour	Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Belgium	Resident ID	Document de Sejour, Verblijfsdocument, Aufenthaltsdokument, E Kaart, Carte E, E Karte; E+ Kaart, Carte E+, E+ Karte; F Kaart, Carte F, F Karte; F+ Kaart, Carte F+, F+ Karte	Front, back	Latin
Belgium	Polycarbonate Passport ^{BETA}	Paspoort, Passeport, Reisepass	Bio-data page	Latin
Bosnia and Herzegovina	Driving License	Vozačka dozvola	Front	Latin
Bosnia and Herzegovina	ID Card	Lična karta, Osobna iskaznica	Front, back	Cyrillic, Latin
Bosnia and Herzegovina	Polycarbonate Passport	Pasoš, Пасош, Putovnica	Bio-data page	Latin
Bulgaria	Driving License	Свидетелство за управление на МПС	Front	Cyrillic, Latin
Bulgaria	ID Card	Лична карта	Front, back	Cyrillic, Latin
Bulgaria	Paper Passport	Паспорт	Bio-data page	Latin
Croatia	Driving License	Vozačka dozvola	Front	Latin
Croatia	ID Card	Osobna iskaznica	Front, back	Latin
Croatia	Residence Permit ^{BETA}	Boravišna iskaznica, Dozvola boravka	Front, back	Latin
Croatia	Polycarbonate Passport	Putovnica	Bio-data page	Latin
Cyprus	Driving License	Sürüş ruhsatı, Αάδεια οδήγησης	Front	Latin
Cyprus	ID Card	Kimlik kartı, Δελτίο Ταυτότητας	Front, back	Latin
Cyprus	Paper Passport	Pasaport, Διαβατήριο	Bio-data page	Latin
Cyprus	Residence Permit	ΑΔΕΙΑ ΔΙΑΜΟΝΗΣ	Front, back	Latin
Czechia	Driving License	Řidičský průkaz	Front	Latin
Czechia	ID Card	Občanský průkaz	Front, back	Latin
Czechia	Residence Permit	Povolení k pobytu	Front, back	Latin
Czechia	Polycarbonate Passport	Cestovní pas	Bio-data page	Latin
Denmark	Driving License	Kørekort	Front	Latin
Denmark	Residence Permit ^{beta}	Opholdstilladelse, Opholdskort	Front, back	Latin
Denmark	Polycarbonate Passport	Pas	Bio-data page	Latin
Estonia	Driving License	Juhiluba	Front	Latin
Estonia	ID Card	Isikutunnistus	Front, back	Latin
Estonia	Paper Passport	Pass	Bio-data page	Latin
Estonia	Residence Permit ^{BETA}	Elamisluba	Front, back	Latin
Finland	Alien ID	Ulkomaalaisen henkilökortti, Identitetskort för utlänning	Front, back	Latin
Finland	Driving License	Ajokortti, Körkort	Front	Latin
Finland	ID Card	Henkilökortti, Identitetskort	Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Finland	Residence Permit	Oleskelulupa, Uppehållstillstånd	Front, back	Latin
Finland	Polycarbonate Passport	Passi, Pass	Bio-data page	Latin
France	Driving License	Permis de conduire	Front	Latin
France	ID Card	Carte d'identité	Front, back	Latin
France	Paper Passport ^{BETA}	Passeport	Bio-data page	Latin
France	Residence Permit ^{BETA}	Titre de séjour	Front, back	Latin
Georgia	Driving License	მართვის მოწმობა	Front	Latin
Georgia	ID Card	მოქალაქის პირადობის მოწმობა	Front, back	Latin
Georgia	Paper Passport ^{BETA}	პასპორტი	Bio-data page	Latin
Germany	Driving License	Führerschein	Front	Latin
Germany	ID Card	Personalausweis	Front, back	Latin
Germany	Minors Passport	Kinderreisepass	Bio-data page	Latin
Germany	Paper Passport	Reisepass	Bio-data page	Latin
Germany	Residence Permit	Aufenthaltstitel	Front, back	Latin
Germany	Polycarbonate Passport	Reisepass	Bio-data page	Latin
Greece	Driving License	Αάδεια οδήγησης	Front	Latin
Greece	ID Card	ΔΕΛΤΙΟ ΤΑΥΤΟΤΗΤΑΣ	Front, back	Latin
Greece	Paper Passport	Διαβατήριο	Bio-data page	Latin
Greece	Residence Permit	ΑΔΕΙΑ ΔΙΑΜΟΝΗΣ	Front, back	Latin
Hungary	Address Card ^{BETA}	Lakcímkártya, Lakcímgazolvány	Front, back	Latin
Hungary	Driving License	Vezetői engedély	Front	Latin
Hungary	ID Card	Személyazonosító igazolvány	Front, back	Latin
Hungary	Paper Passport	Útleve	Bio-data page	Latin
Hungary	Residence Permit ^{BETA}	Tartózkodási engedély	Front, back	Latin
Iceland	Driving License ^{BETA}	Ökuskírteini	Front	Latin
Iceland	Paper Passport ^{BETA}	Vegabréf	Bio-data page	Latin
Ireland	Driving License	Ceadúnas tiomána	Front	Latin
Ireland	Passport Card	Cárta Pas	Front, back	Latin
Ireland	Public Services Card	Cárta Seirbhísi Poiblí	Front, back	Latin
Ireland	Residence Permit ^{BETA}		Front, back	Latin
Ireland	Polycarbonate Passport	Pas	Bio-data page	Latin
Italy	Driving License	Patente di guida	Front	Latin
Italy	ID Card	Carta d'identità	Front, back	Latin
Italy	Paper Passport ^{BETA}	Passaporto	Bio-data page	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Italy	Residence Permit	Permesso di soggiorno	Front, back	Latin
Kosovo	Driving License	Patentë shoferi, возачка дозвола	Front	Latin
Kosovo	ID Card	Letërnjoftim, Лична карта	Front, back	Latin
Kosovo	Paper Passport	Pasaportë, Пасош	Bio-data page	Latin
Latvia	Alien ID	Nepilsoņa personas apliecība	Front, back	Latin
Latvia	Driving License	Vadītāja apliecība	Front	Latin
Latvia	ID Card	Personas apliecība	Front, back	Latin
Latvia	Residence Permit ^{BETA}	Uzturēšanās atļauja	Front, back	Latin
Latvia	Polycarbonate Alien Passport	Nepilsoņa pase	Bio-data page	Latin
Latvia	Polycarbonate Passport	Pase	Bio-data page	Latin
Liechtenstein	ID Card	Identitätskarte	Front, back	Latin
Lithuania	Driving License	Vairuotojo pažymėjimai	Front	Latin
Lithuania	ID Card	Asmens tapatybės kortelė	Front, back	Latin
Lithuania	Residence Permit ^{BETA}	Leidimas gyventi	Front, back	Latin
Lithuania	Polycarbonate Passport	Pasas	Bio-data page	Latin
Luxembourg	Driving License	Permis de conduire	Front	Latin
Luxembourg	ID Card	Carte d'Identité, Personalausweis	Front, back	Latin
Luxembourg	Residence Permit	Titre de séjour	Front, back	Latin
Luxembourg	Polycarbonate Passport	Pass, Passeport	Bio-data page	Latin
Malta	Driving License	Liċenzja tas-Sewqan	Front	Latin
Malta	ID Card	Karta tal-Identità	Front, back	Latin
Malta	Residence Permit	Permess ta' residenza, Residence documentation	Front, back	Latin
Moldova	ID Card ^{BETA}	Buletin de identitate	Front, back	Latin
Moldova	Paper Passport ^{BETA}	Pașaport	Bio-data page	Latin
Montenegro	Driving License	Vozačka dozvola, Возачка дозвола	Front	Latin
Montenegro	ID Card	Lična karta, Лична карта	Front, back	Latin
Montenegro	Polycarbonate Passport	Pasoš, Пасош	Bio-data page	Latin
Netherlands	Driving License	Rijbewijs	Front, back	Latin
Netherlands	ID Card	Identiteitskaart (ID-kaart)	Front, back	Latin
Netherlands	Residence Permit	Verblijfstitel, Verblijfskaart	Front, back	Latin
Netherlands	Polycarbonate Passport	Paspoort	Bio-data page	Latin
North Macedonia	Driving License	возачка дозвола, Patentë shoferi	Front	Cyrillic, Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
North Macedonia	ID Card	лична карта, Letërnjoftim	Front, back	Cyrillic, Latin
North Macedonia	Polycarbonate Passport	Пасош, Pasaportë	Bio-data page	Latin
Norway	Driving License	Førekort, Førarkort	Front	Latin
Norway	ID Card		Front, back	Latin
Norway	Residence Permit	Oppholdstillatelse, Oppholdsløyve	Front, back	Latin
Norway	Polycarbonate Passport	Pass	Bio-data page	Latin
Poland	Driving License	Prawo jazdy	Front	Latin
Poland	ID Card	Dowód osobisty	Front, back	Latin
Poland	Paper Passport	Paszport	Bio-data page	Latin
Poland	Residence Permit ^{BETA}	Karta pobytu	Front, back	Latin
Poland	Polycarbonate Passport	Paszport	Bio-data page	Latin
Portugal	Driving License	Carta de Condução	Front	Latin
Portugal	ID Card	Cartão de Cidadão (CC)	Front, back	Latin
Portugal	Paper Passport	Passaporte	Bio-data page	Latin
Portugal	Residence Permit ^{BETA}	Título de Residência, Cartão de Residência	Front, back	Latin
Romania	Driving License	Permis de conducere	Front	Latin
Romania	ID Card	Carte de identitate	Front	Latin
Romania	Polycarbonate Passport	Pasaport, Pașaport	Bio-data page	Latin
Russia	Driving License	Водительское удостоверение	Front	Latin
Russia	Polycarbonate Passport	(Заграничный) Паспорт	Bio-data page	Latin
Serbia	Driving License	Возачка дозвола, Vozačka dozvola	Front	Latin
Serbia	ID Card	Лична карта, Lična karta	Front, back	Cyrillic, Latin
Serbia	Polycarbonate Passport	Пасош, Pasoš	Bio-data page	Latin
Slovakia	Driving License	Vodičský preukaz	Front	Latin
Slovakia	ID Card	Občiansky preukaz	Front, back	Latin
Slovakia	Residence Permit	Povolenie na pobyt, Pobytový preukaz občana EÚ, Pobytový preukaz rodinného príslušníka občana EÚ	Front, back	Latin
Slovakia	Polycarbonate Passport	Cestovný pas	Bio-data page	Latin
Slovenia	Driving License	Vozniško dovoljenje	Front	Latin
Slovenia	ID Card	Osebná izkaznica	Front, back	Latin
Slovenia	Residence Permit	Dovoljenje za prebivanje	Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Slovenia	Polycarbonate Passport	Potni list	Bio-data page	Latin
Spain	Alien ID	Tarjeta de Identidad de Extranjero (TIE)	Front, back	Latin
Spain	Driving License	Permiso de Conducción	Front	Latin
Spain	ID Card	Documento Nacional de Identidad (DNI)	Front, back	Latin
Spain	Paper Passport	Pasaporte	Bio-data page	Latin
Spain	Residence Permit	Permiso de residencia	Front, back	Latin
Sweden	Driving License	Körkort	Front	Latin
Sweden	ID Card	Nationellt identitetskort	Front, back	Latin
Sweden	Residence Permit	Uppehållstillstånd, Uppehållskort	Front, back	Latin
Sweden	Polycarbonate Passport	Pass	Bio-data page	Latin
Sweden	Social Security Card	Identitetskort, Skatteverkets id-kort	Front	Latin
Switzerland	Driving License	Führerausweis, Permis de conduire, Licenza di condurre, Permiss da manischar	Front	Latin
Switzerland	ID Card	Identitätskarte, Carte d'identité, Carta d'identità, Carta d'identitad	Front, back	Latin
Switzerland	Paper Passport	Pass, Passeport, Passaporto, Passaport	Bio-data page	Latin
Switzerland	Residence Permit	Aufenthaltstitel, Titre de séjour, Permesso di soggiorno, Permissiun da dimora	Front, back	Latin
UK	Driving License	Trwydded yrru	Front	Latin
UK	Paper Passport		Bio-data page	Latin
UK	Proof Of Age Card	CitizenCard	Front	Latin
UK	Residence Permit		Front, back	Latin
UK	Polycarbonate Passport		Bio-data page	Latin
Ukraine	Driving License	Посвідчення водія, Водительское удостоверение	Front	Cyrillic, Latin
Ukraine	ID Card	Паспорт громадянина України	Front, back	Cyrillic, Latin
Ukraine	Residence Permit	Посвідка на постійне проживання (ППП)	Front, back	Cyrillic, Latin
Ukraine	Polycarbonate Passport	Паспорт	Bio-data page	Latin
Ukraine	Temporary Residence Permit	Посвідка на тимчасове проживання	Front, back	Cyrillic, Latin

Supported identity documents (Latin America and the Caribbean)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Antigua and Barbuda	Driving License ^{BETA}		Front	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Argentina	Alien ID	DNI para extranjeros	Front, back	Latin
Argentina	Driving License ^{BETA}	Licencia de Conducir	Front	Latin
Argentina	ID Card	Documento Nacional de Identidad (DNI)	Front, back	Latin
Argentina	Paper Passport	Pasaporte	Bio-data page	Latin
Bahamas	Driving License		Front	Latin
Bahamas	ID Card ^{BETA}	NIB Smart Card	Front	Latin
Barbados	ID Card ^{BETA}		Front, back	Latin
Bolivia	Driving License	Licencia para conducir	Front	Latin
Bolivia	ID Card	Cédula de identidad	Front, back	Latin
Bolivia	Minors ID	Cédula de identidad para menores	Front, back	Latin
Brazil	Consular Passport ^{BETA}	Passaporte	Bio-data page	Latin
Brazil	Driving License	Carteira Nacional de Habilitação (CNH)	Front, back	Latin
Brazil	ID Card ^{BETA}	Cédula de identidade	Front, back	Latin
Brazil	Paper Passport ^{BETA}	Passaporte	Bio-data page	Latin
Brazil, Rio De Janeiro	ID Card	Cédula de identidade	Front, back	Latin
Brazi, Rio Grande do Sul	ID Card ^{BETA}	Cédula de identidade	Front, back	Latin
Brazi, Sao Paulo	ID Card	Cédula de identidade	Front, back	Latin
Cayman Islands	Driving License ^{BETA}	Driver's license	Front	Latin
Chile	Alien ID	Cédula de identidad para extranjeros	Front, back	Latin
Chile	Driving License	Licencia de conducir	Front	Latin
Chile	ID Card	Cédula de Identidad	Front, back	Latin
Chile	Polycarbonate Passport	Pasaporte	Bio-data page	Latin
Columbia	Alien ID	Cédula de Extranjería (CE)	Front, back	Latin
Columbia	Driving License	Licencia de Conducción	Front, back	Latin
Columbia	ID Card	Cédula Digital Colombiana, Cédula de Ciudadanía (CC)	Front, back	Latin
Columbia	Minors ID	Tarjeta de identidad Biométrica (Azul)	Front, back	Latin
Columbia	Polycarbonate Passport	Pasaporte	Bio-data page	Latin
Costa Rica	Driving License ^{BETA}	Licencia de conducir	Front	Latin
Costa Rica	ID Card	Cédula de identidad	Front, back	Latin
Cuba	ID Card ^{BETA}	Carné de Identidad	Front, back	Latin
Cuba	Paper Passport	Pasaporte	Bio-data page	Latin
Dominican Republic	Driving License ^{BETA}	Licencia de conducir	Front, back	Latin
Dominican Republic	ID Card	Cédula de Identidad y Electoral (CIE)	Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Dominican Republic	Paper Passport	Pasaporte	Bio-data page	Latin
Ecuador	Driving License	Licencia de conducir	Front	Latin
Ecuador	ID Card	Cédula de Identidad, Cédula de Identidad Electrónica	Front, back	Latin
El Salvador	Driving License ^{BETA}	Licencia de conducir	Front, back	Latin
El Salvador	ID Card	Documento Único de Identidad (DUI)	Front, back	Latin
Guatemala	Consular ID	Tarjeta de Identificación Consular (TICG)	Front, back	Latin
Guatemala	Driving License	Licencia de conducir	Front, back	Latin
Guatemala	ID Card	Documento Personal de Identificación (DPI)	Front, back	Latin
Guatemala	Paper Passport	Pasaporte	Bio-data page	Latin
Haiti	Driving License	Permis de conduire	Front	Latin
Haiti	ID Card	Carte d'identification nationale (CIN), Kat Idantifikasyon Nasyonal	Front, back	Latin
Haiti	Paper Passport	Passeport, Paspò	Bio-data page	Latin
Honduras	Driving License ^{BETA}	Licencia de conducir	Front, back	Latin
Honduras	ID Card ^{BETA}	Tarjeta de identidad	Front, back	Latin
Honduras	Paper Passport ^{BETA}	Pasaporte	Bio-data page	Latin
Jamaica	Driving License	Motor vehicle license, MV license	Front, back	Latin
Mexico	Consular ID ^{BETA}	Matrícula consular	Front, back	Latin
Mexico	Paper Passport ^{BETA}	Pasaporte	Bio-data page	Latin
Mexico	Professional DL ^{BETA}	Licencia Federal de Conductor	Front	Latin
Mexico	Professional ID ^{BETA}	Cédula Profesional	Front, back, vertical	Latin
Mexico	Residence Permit ^{beta}	Tarjeta de Residencia Temporal y Residencia Permanente	Front, back	Latin
Mexico	Polycarbonate Passport	Pasaporte	Bio-data page	Latin
Mexico	Voter ID	Credencial para votar	Front, back	Latin
Mexico, Aguascalientes	Driving License	Licencia de Conducir	Front, back, vertical	Latin
Mexico, Baja California	Driving License	Licencia de Conducir	Front, back, vertical	Latin
Mexico, Baja California Sur	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Campeche	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Chiapas	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Chihuahua	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Ciudad de Mexico	Driving License	Licencia de Conducir	Front, vertical	Latin
Mexico, Coahuila	Driving License	Licencia de Conducir	Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Mexico, Colima	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Durango	Driving License	Licencia de Conducir	Front	Latin
Mexico, Guanajuato	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Guerrero Cocula	Driving License ^{BETA}	Licencia de Conducir	Front, back	
Mexico, Guerrero Juchitan	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Hidalgo	Driving License	Licencia de Conducir	Front, back, vertical	Latin
Mexico, Jalisco	Driving License	Licencia de Conducir	Front	Latin
Mexico, Mexico	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Michoacan	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Morelos	Driving License	Licencia de Conducir	Front	Latin
Mexico, Nayarit	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Nuevo Leon	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Oaxaca	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Puebla	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Quintana Roo Cozumel	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Quintana Roo Solidaridad	Driving License	Licencia de Conducir	Front, back, vertical,	Latin
Mexico, San Luis Potosi	Driving License	Licencia de Conducir	Front	Latin
Mexico, Sinaloa	Driving License ^{BETA}	Licencia de Conducir	Front	Latin
Mexico, Sonora	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Tabasco	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Tamaulipas	Driving License	Licencia de Conducir	Front, back, vertical,	Latin
Mexico, Tlaxcala	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Veracruz	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Yucatan	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Zacatecas	Driving License	Licencia de Conducir	Front, back	Latin
Nicaragua	ID Card	Cédula de Identidad Ciudadana	Front, back	Latin
Panama	Driving License	Licencia de Conducir	Front	Latin
Panama	ID Card	Cédula de Identidad	Front	Latin
Panama	Residence Permit	Carné de Residente Permanente	Front	Latin
Panama	Temporary Residence Permit	Carné de Residencia Provisional	Front, back	Latin
Paraguay	Driving License	Licencia de Conducir	Front, back	Latin
Paraguay	ID Card	Cédula de Identidad Civil	Front, back	Latin
Peru	Driving License	Licencia de conducir	Front, back	Latin

Genetec ClearID®; User Guide

Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Peru	ID Card	Documento Nacional de Identidad (DNI)	Front, back	Latin
Peru	Minors ID ^{BETA}	Documento Nacional de Identidad (DNI) para menores	Front, back	Latin
Peru	Paper Passport	Pasaporte	Bio-data page	Latin
Puerto Rico	Driving License	Licencia de Conducir	Front	Latin
Puerto Rico	Voter ID ^{BETA}	Tarjeta de Identificación Electoral (TIE), Electoral Identification Card	Front	Latin
Saint Lucia	ID Card ^{BETA}		Front, back	Latin
Trinidad and Tobago	Driving License		Front	Latin
Trinidad and Tobago	ID Card		Front, back	Latin
Uruguay	ID Card	Cédula de Identidad	Front, back	Latin
Venezuela	Driving License	Licencia para conducir	Front	Latin
Venezuela	ID Card	Cédula de Identidad	Front	Latin
Venezuela	Polycarbonate Passport	Pasaporte	Bio-data page	Latin

Supported identity documents (Middle East and Africa)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Algeria	Driving License	رخصة القيادة	Front, back	Latin
Algeria	ID Card	Carte nationale d'identité, بطاقة الهوية الوطني	Front, back	Latin
Algeria	Paper Passport	جواز السفر, Passeport	Bio-data page	Latin
Bahrain	ID Card	بطاقة الهوية, CPR Card	Front, back	Latin
Botswana	ID Card	Omang	Front, back	Latin
Burkina Faso	ID Card	Carte Nationale d'Identité Burkinabè (CNIB)	Front, back	Latin
Cameroon	ID Card	Carte Nationale d'Identité (CNI)	Front, back	Latin
Democratic Republic of the Congo	Driving License ^{BETA}	Permis de conduire (CONADEP)	Front, back	Latin
Egypt	Driving License ^{BETA}	رخصة القيادة	Front, back	Latin
Egypt	ID Card	بطاقة تحقيق الشخصية	Front, back	Arabic, Latin
Egypt	Paper Passport ^{BETA}	جواز سفر	Bio-data page	Latin
Eswatini	Paper Passport		Bio-data page	Latin
Ghana	Driving License		Front	Latin
Ghana	ID Card	Ghana Card	Front, back	Latin
Ghana	Paper Passport		Bio-data page	Latin
Iran	Paper Passport ^{BETA}	گذرنامه	Bio-data page	Latin
Iraq	ID Card	البطاقة الوطنية, كارتى نيشتمانى	Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Iraq	Paper Passport ^{BETA}	پاسپورت, جواز سفر	Bio-data page	Latin
Israel	Driving License	רשיון נהיגה	Front	Latin
Israel	ID Card	Tehudat Zehut, بطاقة هوية, תעודת זהות	Front, back	Latin
Israel	Paper Passport ^{BETA}	דרכון	Bio-data page	Latin
Ivory Coast	Driving License	Permis de conduire	Front	Latin
Ivory Coast	ID Card	Carte Nationale d'Identité (CNI)	Front, back	Latin
Jordan	Driving License ^{BETA}	رخصة القيادة	Front	Latin
Jordan	ID Card	بطاقة شخصية	Front, back	Arabic, Latin
Jordan	Paper Passport ^{BETA}	جواز سفر	Bio-data page	Latin
Kenya	ID Card	Kitambulisho	Front, back	Latin
Kenya	Polycarbonate Passport	Passport, Pasi	Bio-data page	Latin
Kuwait	Driving License	رخصة القيادة	Front, back	Latin
Kuwait	ID Card	بطاقة المدنية	Front, back	Latin
Kuwait	Resident ID	بطاقة المدنية	Front, back	Latin
Lebanon	ID Card	بطاقة الهوية	Front, back	Latin
Libya	Polycarbonate Passport	جواز سفر	Bio-data page	Latin
Mauritius	ID Card		Front, back	Latin
Morocco	Driving License	Permis de conduire, رخصة القيادة	Front, back	Latin
Morocco	ID Card	Carte nationale d'identité, بطاقة التعريف الوطنية	Front, back	Latin
Morocco	Paper Passport ^{BETA}	Passeport, جواز سفر	Bio-data page	Latin
Mozambique	Driving License ^{BETA}	Carta de Condução	Front	Latin
Mozambique	ID Card	Bilhete de Identidade (BI)	Front, back	Latin
Nigeria	Driving License		Front, back	Latin
Nigeria	ID Card	e-ID card	Front, back	Latin
Nigeria	Paper Passport		Bio-data page	Latin
Nigeria	Polycarbonate Passport ^{BETA}		Bio-data page	Latin
Nigeria	Voter ID	Permanent Voter Card (PVC)	Front, back	Latin
Oman	Driving License ^{BETA}	رخصة قيادة مركبة	Front, back	Latin
Oman	ID Card	بطاقة الهوية	Front, back	Latin
Oman	Resident ID	بطاقة مقيم	Front, back	Latin
Qatar	Driving License	رخصة القيادة	Front	Latin
Qatar	ID Card ^{BETA}	بطاقة إثبات شخصية	Front	Latin
Qatar	Paper Passport	جواز سفر	Bio-data page	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Qatar	Residence Permit	تصريح الإقامة	Front, back	Latin
Rwanda	ID Card	Indangamuntu	Front	Latin
Saudi Arabia	Driving License	رخصة قيادة	Front	Latin
Saudi Arabia	ID Card	بطاقة الأحوال المدنية	Front, back	Latin
Saudi Arabia	Paper Passport	جواز سفر	Bio-data page	Latin
Saudi Arabia	Resident ID	هوية المقيم, Iqama	Front	Latin
Senegal	ID Card	Carte d'identité biométrique CEDEAO, Carte nationale d'identité	Front, back	Latin
South Africa	Driving License	Bestuurslisensie	Front	Latin
South Africa	ID Card	Smart ID card	Front, back	Latin
South Africa	ID Card ^{BETA}	Green barcoded ID book	Front, vertical	Latin
South Africa	Polycarbonate Passport	Passeport	Bio-data page	Latin
Sudan	Polycarbonate Passport	جواز سفر	Bio-data page	Latin
Syria	Paper Passport	جواز سفر	Bio-data page	Latin
Tanzania	Driving License	Leseni ya udereva	Front	Latin
Tanzania	ID Card ^{BETA}	Kitambulisho cha Taifa, NIDA	Front, back	Latin
Tanzania	Voter ID ^{BETA}	Kadi ya mpiga kura, Voter Card	Front	Latin
Togo	ID Card	Permis de conduire	Front, back	Latin
Tunisia	Driving License	رخصة قيادة	Front	Latin
Tunisia	ID Card	بطاقة التعريف الوطنية	Front	Latin
Tunisia	Paper Passport	جواز سفر	Bio-data page	Latin
Turkey	Driving License	Sürücü belgesi	Front	Latin
Turkey	ID Card	Kimlik Kartı	Front, back	Latin
Turkey	Paper Passport	Pasaport	Bio-data page	Latin
Turkey	Residence Permit ^{BETA}	İkamet izni	Front, back	Latin
Turkey	Polycarbonate Passport	Pasaport	Bio-data page	Latin
UAE	Driving License	رخصة القيادة	Front, back	Latin
UAE	ID Card	بطاقة الهوية	Front, back	Arabic, Latin
UAE	Paper Passport	جواز سفر	Bio-data page	Arabic, Latin
UAE	Resident ID	بطاقة الهوية الوطنية	Front, back	Arabic, Latin
Uganda	Driving License		Front	Latin
Uganda	ID Card		Front, back	Latin
Zimbabwe	ID Card	National registration card (NRC)	Front, back	Latin
Zimbabwe	Paper Passport		Bio-data page	Latin

Supported identity documents (North America)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Bermuda	Driving License ^{BETA}		Front	Latin
Canada	Citizenship Certificate ^{BETA}	Canada citizenship card, Carte de citoyenneté canadienne	Front, back	Latin
Canada	Paper Passport	Passport, Passeport	Bio-data page	Latin
Canada	Residence Permit	Permanent residence (PR) card, Carte de résident permanent	Front, back	Latin
Canada	Social Security Card ^{BETA}	Social insurance card (SIN card), Carte d'assurance sociale (Carte de NAS)	Front	Latin
Canada	Tribal ID	Certificate of Indian Status, Certificat de statut Indien	Front, back	Latin
Canada	Weapon Permit	Possession and Aquisition License (PAL), Permis de possession et d'acquisition	Front	Latin
Canada, Alberta	Driving License		Front, back	Latin
Canada, Alberta	ID Card		Front, back	Latin
Canada, British Columbia	Driving License		Front, back	Latin
Canada, British Columbia	Driver License, Public Services Card (Combined)		Front, back	Latin
Canada, British Columbia	ID Card		Front, back	Latin
Canada, British Columbia	Minors Public Services Card		Front, back	Latin
Canada, British Columbia	Public Services Card		Front, back	Latin
Canada Manitoba	Driving License		Front, back	Latin
Canada Manitoba	ID Card		Front, back	Latin
Canada, New Brunswick	Driving License	Permis de conduire	Front, back	Latin
Canada, Newfoundland and Labrador	Driving License		Front, back	Latin
Canada, Nova Scotia	Driving License		Front, back	Latin
Canada, Nova Scotia	ID Card ^{BETA}		Front, back	Latin
Canada, Nova Scotia	Driving License		Front, back	Latin
Canada, Nova Scotia	ID Card ^{BETA}		Front, back	Latin
Canada, Ontario	Driving License		Front, back	Latin
Canada, Ontario	ID Card	Photo card	Front, back	Latin
Canada, Quebec	Driving License	Permis de conduire	Front, back	Latin
Canada, Saskatchewan	Driving License		Front, back	Latin
Canada, Saskatchewan	ID Card ^{BETA}		Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Canada, Yukon	Driving License	Permis de conduire	Front, back	Latin
USA	Border Crossing Card	BCC	Front, back	Latin
USA	Global Entry Card		Front, back	Latin
USA	Green Card	Permanent resident card	Front, back	Latin
USA	Military ID	Common Access Card (CAC)	Front, back, vertical	Latin
USA	Nexus Card ^{BETA}		Front, back	Latin
USA	Paper Passport		Bio-data page	Latin
USA	Passport Card		Front, back	Latin
USA	Polycarbonate Passport		Bio-data page	Latin
USA	Social Security Card ^{BETA}		Front	Latin
USA	Veteran ID	VIC	Front	Latin
USA	Work Permit	Employment authorization document, EAD Card	Front, back	Latin
USA, Alabama	Driving License		Front, back, vertical	Latin
USA, Alabama	ID Card		Front, back, vertical	Latin
USA, Alaska	Driving License		Front, back	Latin
USA, Alaska	ID Card		Front, back	Latin
USA, Arizona	Driving License		Front, back, vertical	Latin
USA, Arizona	ID Card		Front, back, vertical	Latin
USA, Arkansas	Driving License		Front, back, vertical	Latin
USA, Arkansas	ID Card		Front, back, vertical	Latin
USA, California	Driving License		Front, back, vertical	Latin
USA, California	ID Card		Front, back, vertical	Latin
USA, Colorado	Driving License		Front, back, vertical	Latin
USA, Colorado	ID Card		Front, back	Latin
USA, Connecticut	Driving License		Front, back, vertical	Latin
USA, Connecticut	ID Card		Front, back	Latin
USA, Delaware	Driving License		Front, back, vertical	Latin
USA, District of Columbia	Driving License		Front, back, vertical	Latin
USA, District of Columbia	ID Card		Front, back, vertical	Latin
USA, Florida	Driving License		Front, back, vertical	Latin
USA, Florida	ID Card		Front, back, vertical	Latin
USA, Georgia	Driving License		Front, back, vertical	Latin
USA, Georgia	ID Card		Front, back, vertical	Latin
USA, Hawaii	Driving License		Front, back, vertical	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
USA, Hawaii	ID Card		Front, back	Latin
USA, Idaho	Driving License		Front, back, vertical	Latin
USA, Idaho	ID Card		Front, back	Latin
USA, Illinois	Driving License		Front, back, vertical	Latin
USA, Illinois	ID Card		Front, back, vertical	Latin
USA, Indiana	Driving License		Front, back	Latin
USA, Indiana	ID Card		Front, back	Latin
USA, Iowa	Driving License		Front, back, vertical	Latin
USA, Iowa	ID Card		Front, back, vertical	Latin
USA, Kansas	Driving License		Front, back, vertical	Latin
USA, Kansas	ID Card		Front, back, vertical	Latin
USA, Kentucky	Driving License		Front, back, vertical	Latin
USA, Kentucky	ID Card		Front, back, vertical	Latin
USA, Louisiana	Driving License		Front, back	Latin
USA, Maine	Driving License		Front, back, vertical	Latin
USA, Maine	ID Card		Front, back	Latin
USA, Maryland	Driving License		Front, back, vertical	Latin
USA, Maryland	ID Card		Front, back, vertical	Latin
USA, Massachusetts	Driving License		Front, back, vertical	Latin
USA, Massachusetts	ID Card		Front, back, vertical	Latin
USA, Michigan	Driving License		Front, back, vertical	Latin
USA, Michigan	ID Card		Front, back, vertical	Latin
USA, Minnesota	Driving License		Front, back, vertical	Latin
USA, Minnesota	ID Card		Front, back, vertical	Latin
USA, Missouri	Driving License		Front, back, vertical	Latin
USA, Missouri	ID Card		Front, back, vertical	Latin
USA, Montana	Driving License		Front, back	Latin
USA, Montana	ID Card		Front, back	Latin
USA, Nebraska	Driving License		Front, back, vertical	Latin
USA, Nebraska	ID Card		Front, back	Latin
USA, Nevada	Driving License		Front, back, vertical	Latin
USA, Nevada	ID Card		Front, back, vertical	Latin
USA, New Hampshire	Driving License		Front, back, vertical	Latin
USA, New Hampshire	ID Card ^{BETA}		Front, back	Latin
USA, New Jersey	Driving License		Front, back, vertical	Latin
USA, New Jersey	ID Card		Front, back, vertical	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
USA, New Mexico	Driving License		Front, back, vertical	Latin
USA, New Mexico	ID Card		Front, back	Latin
USA, New York	Driving License		Front, back, vertical	Latin
USA, New York	ID Card		Front, back, vertical	Latin
USA, New York City	ID Card		Front, back	Latin
USA, North Carolina	Driving License		Front, back, vertical	Latin
USA, North Carolina	ID Card		Front, back, vertical	Latin
USA, North Dakota	Driving License		Front, back, vertical	Latin
USA, North Dakota	ID Card ^{BETA}		Front, back	Latin
USA, Ohio	Driving License		Front, back, vertical	Latin
USA, Ohio	ID Card		Front, back, vertical	Latin
USA, Oklahoma	Driving License		Front, back, vertical	Latin
USA, Oklahoma	ID Card		Front, back, vertical	Latin
USA, Oregon	Driving License		Front, back, vertical	Latin
USA, Oregon	ID Card		Front, back	Latin
USA, Pennsylvania	Driving License		Front, back, vertical	Latin
USA, Pennsylvania	ID Card		Front, back, vertical	Latin
USA, Rhode Island	Driving License		Front, back, vertical	Latin
USA, Rhode Island	ID Card		Front, back	Latin
USA, South Carolina	Driving License		Front, back, vertical	Latin
USA, South Carolina	ID Card		Front, back, vertical	Latin
USA, South Dakota	Driving License		Front, back, vertical	Latin
USA, South Dakota	ID Card ^{BETA}		Front, back	Latin
USA Tennessee	Driving License		Front, back, vertical	Latin
USA Tennessee	ID Card		Front, back, vertical	Latin
USA, Texas	Driving License		Front, back, vertical	Latin
USA, Texas	ID Card		Front, back, vertical	Latin
USA, Texas	Weapon Permit	License to Carry a Handgun (LTC)	Front	Latin
USA, Utah	Driving License		Front, back, vertical	Latin
USA, Utah	ID Card		Front, back, vertical	Latin
USA, Vermont	Driving License		Front, back	Latin
USA, Virginia	Driving License		Front, back, vertical	Latin
USA, Virginia	ID Card		Front, back	Latin
USA, Washington	Driving License		Front, back, vertical	Latin
USA, Washington	ID Card		Front, back, vertical	Latin
USA, West Virginia	Driving License		Front, back	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
USA, Wisconsin	Driving License		Front, back, vertical	Latin
USA, Wisconsin	ID Card		Front, back	Latin
USA, Wyoming	Driving License		Front, back	Latin
USA, Wyoming	ID Card		Front, back	Latin

Supported identity documents (Oceania)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Australia	Paper Passport		Bio-data page	Latin
Australia, Australian Capital Territory	Driving License		Front	Latin
Australia, New South Wales	Driving License		Front	Latin
Australia, New South Wales	ID Card		Front	Latin
Australia, Northern Territory	Driving License ^{BETA}		Front, back	Latin
Australia, Northern Territory	Proof Of Age Card	NT Evidence of age card	Front, back	Latin
Australia, Queensland	Driving License		Front, back	Latin
Australia, South Australia	Driving License		Front, back	Latin
Australia, South Australia	Proof Of Age Card		Front	Latin
Australia, Tasmania	Driving License		Front, back	Latin
Australia, Victoria	Driving License		Front, back	Latin
Australia, Victoria	Proof Of Age Card		Front	Latin
Australia, Western Australia	Driving License		Front, back	Latin
New Zealand	Driving License		Front	Latin
New Zealand	Polycarbonate Passport	Uruwhenua	Bio-data page	Latin

Browse

- [About ClearID Self-Service Kiosk](#)

14 | Troubleshooting

14.1 | Plugin installed, but missing from Security Desk and Config Tool

If the Properties tab for the plugin is missing, then the plugin is not installed on your local machine. The plugin must be installed on a Genetec™ Server (main or expansion).

To help you troubleshoot this issue, refer to the possible causes and their respective solutions below.

Possible symptoms:

- In Config Tool, you see the plugin in the Plugins task, and you can add a new plugin role, but the new role is missing the Properties tab.
- In Security Desk, the plugin does not appear on the Options page.

Genetec ClearID™ User Guide Displayed in the header

Description of cause: The plugin is not installed on the local computer, the license (certificate) is invalid, or you are missing required user privileges.

Solution 1: Install the plugin on your local computer.

Solution 2: Make sure that a Genetec™ Server has the plugin installed, the role created, and is configured correctly.

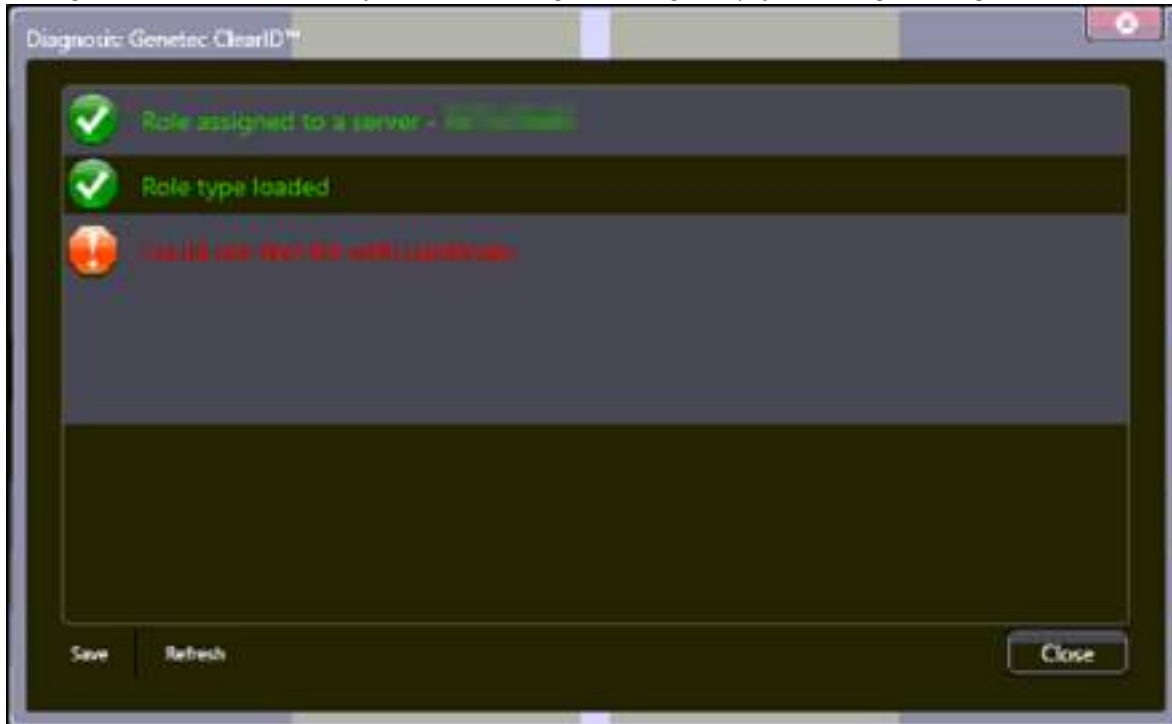
Solution 3: Confirm that the plugin is installed on your Security Center computer: from the homepage in Security Desk or Config Tool, click About > Installed components and look in the list for the entry Genetec.Iams.SCPlugin.Client.

Solution 4: Confirm that your system has a license (certificate) for the plugin: from the homepage in Security Desk or Config Tool, click About > Certificates, look in the list for the name of the plugin, and make sure that your access permissions are set to Unlimited or a number representing the number of licenses.

14.2 | Plugin role could not find file with certificate

When adding the Genetec ClearID™ plugin role, the role is unable to start and a Could not find file with certificate error message is displayed.

In Config Tool, in the Roles section of the System task the following error message is displayed in the diagnosis dialog.



Cause

The CD-SC-PLUGIN license is missing for that system (GSC does not have the ClearID license part).

Solution

Make sure that the plugin role is correctly configured with the required license part.

1. In Config Tool, click About > Certificates and look for ClearID.
2. If the ClearID certificate is not found, add the CD-SC-PLUGIN part to the license, apply the license to the system, and restart the system.

14.3 | Custom fields not displayed in Security Desk

If custom fields are not displayed in Security Desk, check the user privileges and ensure that the relevant user or user groups have been configured for the custom field.

To troubleshoot the issue, learn about the possible causes and their respective solutions.

Incorrect user privileges

Description of cause: A custom field is not displayed because the user lacks the required privileges.

Solution: Add the required privileges.

1. From the Config Tool homepage, open the User management task.

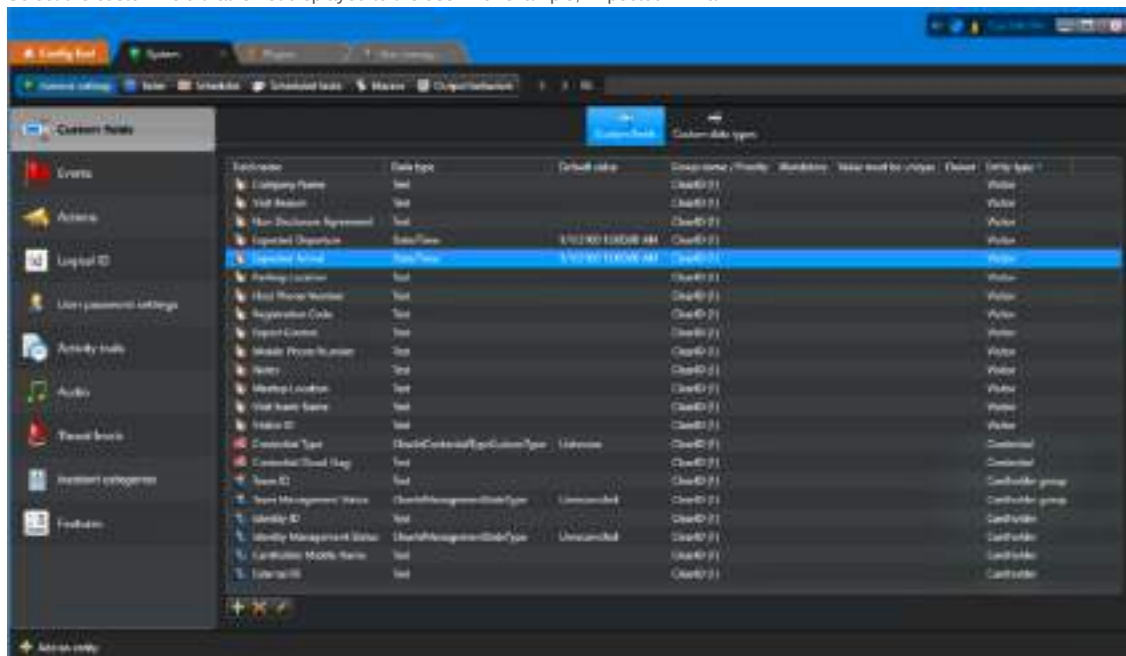
2. Select the relevant user, and click the Privileges tab.
3. Set the following privileges to Allow:
 - Application privileges > Security Desk
 - Application privileges > Config Tool
 - Administrative privileges > System management > View role properties
 - Administrative privileges > System management > View server properties
 - Task privileges > Administration > Plugins
4. (Optional) Set the custom field privileges that you require to Allow.
 - Administrative privileges > Access control management > View cardholder group properties > Modify cardholder group properties > Modify custom fields
 - Administrative privileges > Access control management > View cardholder properties > Modify cardholder properties > Modify custom fields
 - Administrative privileges > Access control management > View credential properties > Modify credential properties > Modify custom fields
 - Administrative privileges > Access control management > View visitor properties > Modify visitor properties > Modify custom fields
 - Administrative privileges > System management > View general settings > Modify custom field definitions
5. Click Apply.

Custom field not configured for user or user group

Description of cause: The custom field has not been configured to display to the user or user group.

Solution: Configure the custom field to display to the user or user group.

1. From the Config Tool homepage, open the System task.
2. Click General settings > Custom Fields.
3. Select the custom field that is not displayed to the user. For example, Expected Arrival.



4. Click Edit the item (✎) to modify the custom field settings.
5. In the Security section of the Edit custom field dialog box, click Add an item (+).
6. Navigate to and select a user or user group from the list and click OK.

In the following example, we configured the *Expected Arrival* custom field so that it is visible to the *Genetec Receptionists* user group.

Edit custom field

Definition

Entity type: Visitor

Data type: Date/Time

Name: Expected Arrival

Default value: 01 / 01 / 2100 12 : 00 : 00 AM

Layout (Optional)

Group name: ClearID

Priority: 1

Security

Visible to administrators and

- Genetec Receptionists

+ X

Cancel Save and close

7. Click Save and close then click Apply.

Browse

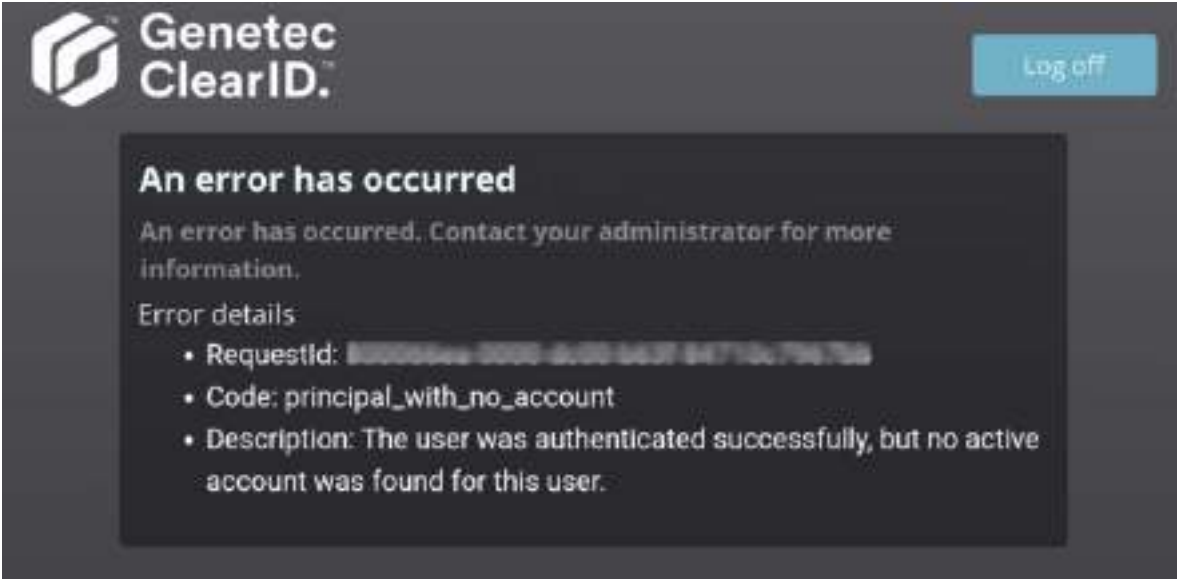
- Granting user privileges for the ClearID plugin
- About custom fields in ClearID

14.4 | No active account found for user

If no active account was found for the user during single sign-on (SSO) logon, use another identity or grant access to the Genetec ClearID™ web portal.

Cause

The user was authenticated successfully, but no active account was found for the user.



The identity associated with the email that was used to log on does not have web portal access.

Solution

Grant user access to the web portal.

14.5 | Visit email notifications not received by visitors

If visitors aren't receiving email notifications, check that the visit event or visit area request has been approved.

To troubleshoot the issue, learn about the possible causes and their respective solutions.

Cause

Visit email notifications aren't received because the visit event or visit area request wasn't approved.

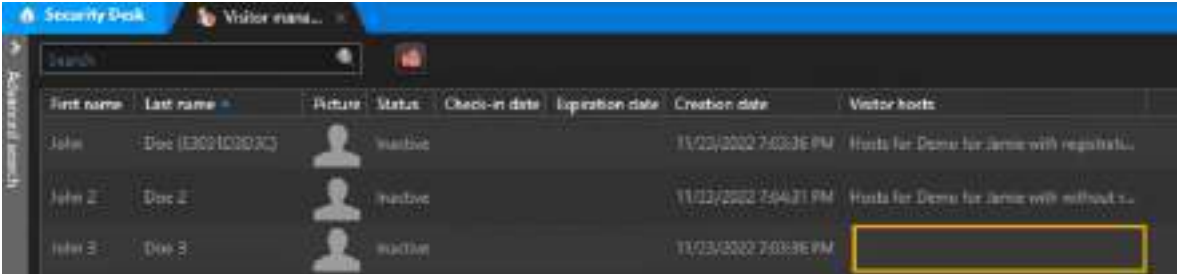
Solution

Review any visit event or visit area requests to identify the request waiting for approval:

- 1. Approve area access requests.
- 2. Approve visit events.

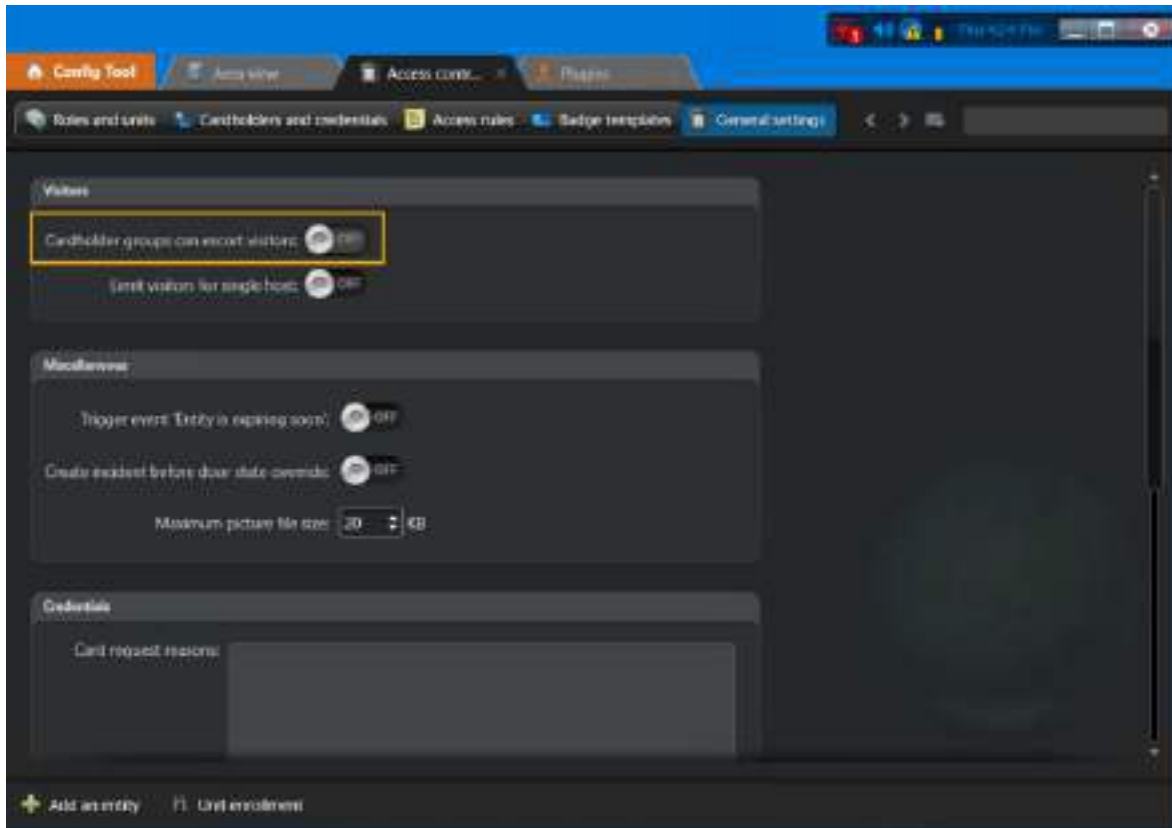
14.6 | Visitor hosts fields in Security Desk are empty

If the Visitor hosts fields in Security Desk are empty, then the Cardholder groups can escort visitors setting might not be configured correctly for Genetec ClearID™.



Cause

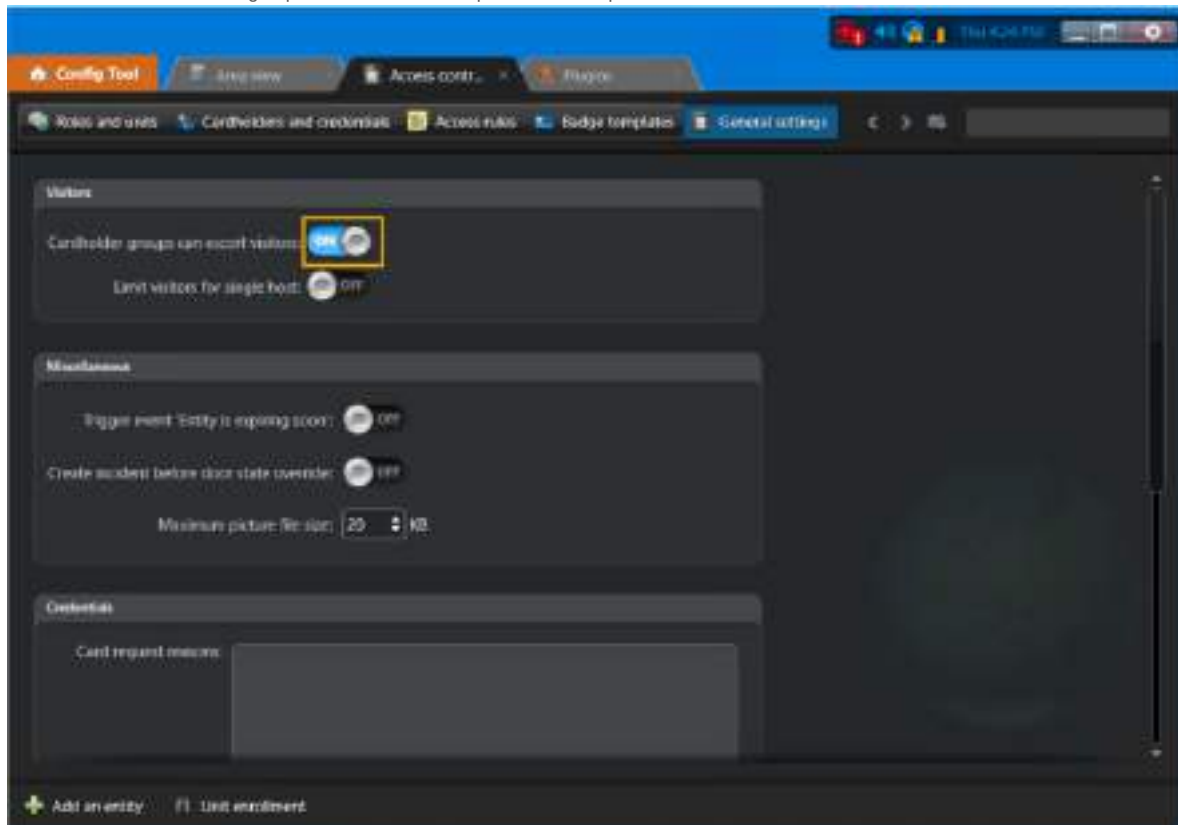
In the Visitors section of the Access control task, the Cardholder groups can escort visitors setting in Config Tool could be disabled (OFF).



Solution

In the Visitors section of the Access control task, make sure that the Cardholder groups can escort visitors setting is enabled (ON).

1. From the Config Tool homepage, open the Access control task.
2. Click General settings.
3. Click or slide the Cardholder groups can escort visitors option to the ON position.



4. (Optional) In ClearID, create a new visit request to verify that the option is working as expected.
5. (Optional) In Security Desk, check that the Visitor hosts field contains host information.

14.7 | ClearID One Identity Synchronization Tool connectivity issues

If you encounter connectivity issues when using the Genetec ClearID™ One Identity Synchronization Tool, check your API integration or Azure AD application connection details.

To help you troubleshoot the issue, learn about the possible causes and their respective solutions.

Unable to connect to Genetec ClearID™

Description: The synchronization tool is unable to connect to ClearID.

Solution: Review the One Identity ConfigurationTool logs.

1. Click , then click Open logs folder.

Tip: You can also open the ConfigurationTool logs manually here:
Code

```
%ProgramData%\Genetec\OneIdentity\Logs\ConfigurationTool
```



2. Review the One Identity ConfigurationTool logs for error messages related to ClearID connectivity issues.
3. Check your API integration connection.
 - a. Click Administration > Automation and select your API integration.
 - b. Check that your API integration key and Client ID details are correct.
4. [Check your connection settings.](#)

Unable to connect to Azure AD

Description: The synchronization tool is unable to connect to Azure Active Directory.

Solution: Review the One Identity ConfigurationTool logs.

1. Click , then click Open logs folder.

Tip: You can also open the ConfigurationTool logs manually here:
Code

```
%ProgramData%\Genetec\OneIdentity\Logs\ConfigurationTool
```



2. Review the One Identity ConfigurationTool logs for error messages related to Azure AD connectivity issues.
3. Check your Azure AD application connection details.

Browse

- [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

14.8 | ClearID One Identity Synchronization Tool data synchronization issues

If you encounter connectivity issues when using the Genetec ClearID™ One Identity Synchronization Tool, check your service logs for errors. To help you troubleshoot the issue, learn about the possible causes and their respective solutions.

Missing data fields

Description: Data fields are missing.

Solution: Review the One Identity Service logs.

1. Click , then click Open logs folder.

Tip: You can also open the ConfigurationTool logs manually here:
Code

```
%ProgramData%\Genetec\OneIdentity\Logs\Service
```



2. Review the One Identity Service logs for error messages related to missing data fields.

For more information about attribute fields, see [One Identity Synchronization Tool attribute fields](#).

3. [Check your Azure AD API permissions.](#)

Missing name fields (first name, last name)

Description: Name fields (first name or last name) are missing.

Solution: Review the One Identity Service logs.

1. Click , then click Open logs folder.

Tip: You can also open the ConfigurationTool logs manually here:

Code

```
%ProgramData%\Genetec\OneIdentity\Logs\Service
```



2. Review the One Identity Service logs for error messages related to name fields.

For more information about attribute fields, see [One Identity Synchronization Tool attribute fields](#).

3. Check your Azure AD API permissions.

Missing email addresses

Description: Email address fields are missing.

Solution: Review the One Identity Service logs.

1. Click , then click Open logs folder.

Tip: You can also open the ConfigurationTool logs manually here:

Code

```
%ProgramData%\Genetec\OneIdentity\Logs\Service
```



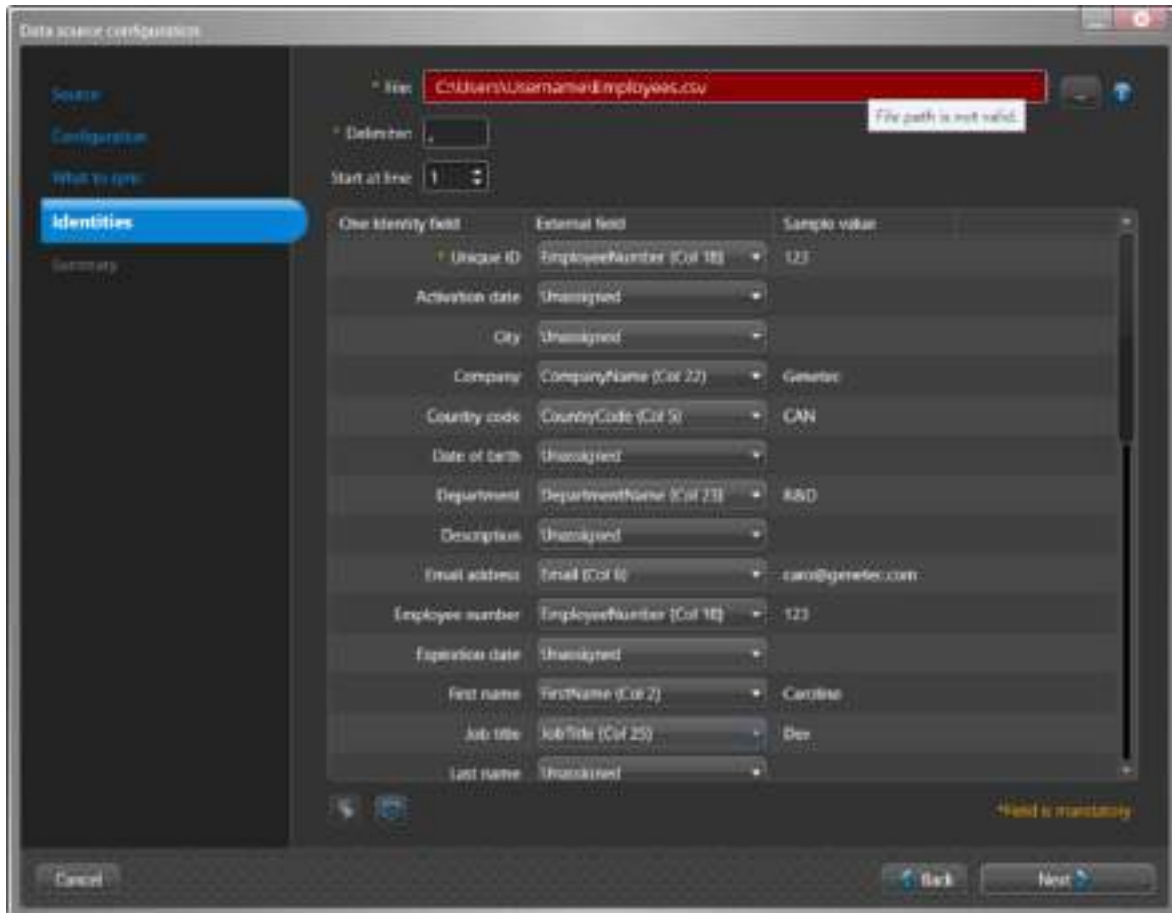
2. Review the One Identity Service logs for error messages related to email address fields.

For more information about attribute fields, see [One Identity Synchronization Tool attribute fields](#).

3. Check your Azure AD API permissions.

File path is not valid

Description: User permission issues encountered when using CSV files as the data source for Identities because the file path is not valid.



Solution:

Best Practice: To avoid user permission issues when using CSV files with the ClearID One Identity Synchronization Tool, save your files to a C: or C:\temp folder location. Do not save your CSV files in user-controlled file or folder locations (c:\Users folders or desktop folder location) or you might encounter File path is not valid user permissions issues.

Browse

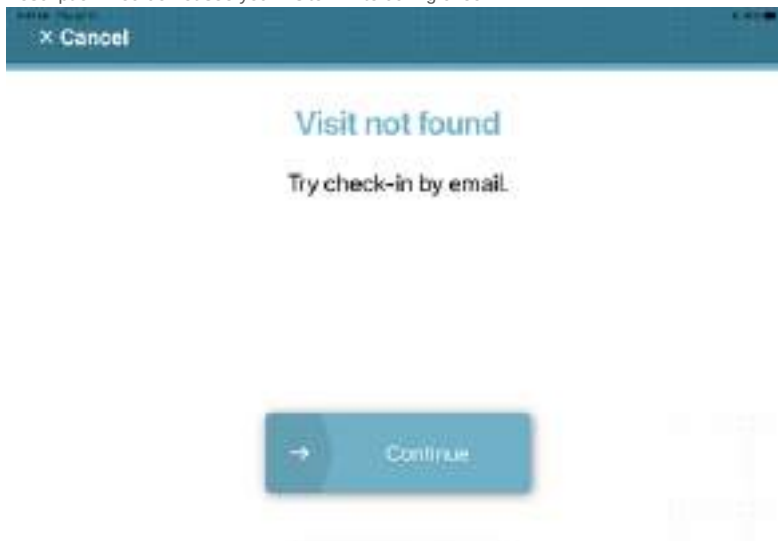
- Synchronizing identities using One Identity Synchronization Tool in ClearID

14.9 | ClearID Self-Service Kiosk issues

If the Genetec ClearID™ Self-Service Kiosk check-in function or the kiosk does not work as expected, you can perform additional troubleshooting steps.

Visitor invite or visit event not found

Description: You do not see your visitor invite during check-in.



The *visit not found* issue can occur for various reasons:

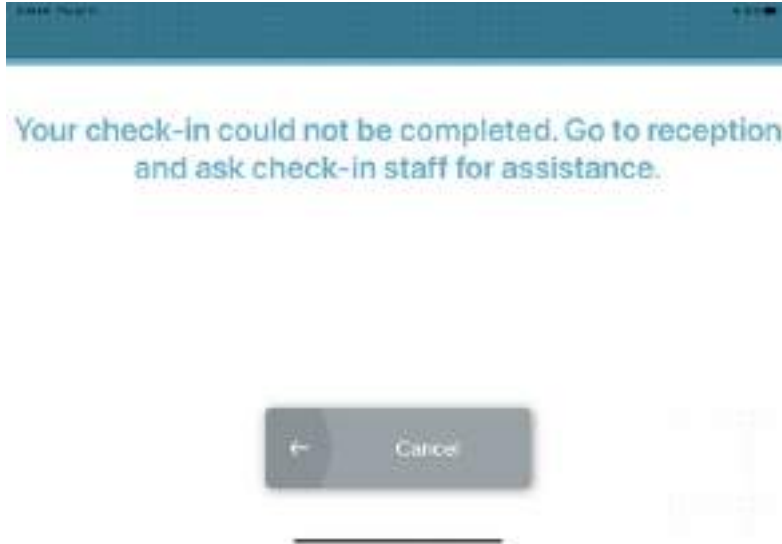
- Visitor check-in is too early (1hr+ before event start time).
- Visitor check-in is too late (1hr+ after event end time).
- Visitor is not listed in visit event invite.
- The visitor name in the visit event invite contains a mistake or typo.

Solution:

- Check the visit event start and end times. Visitors can check in up to 1 hour before or after a visit event.
- Check visitor names listed in the visit event. Look for any visitors not listed or any mistakes in the visitor details.

Check-in could not be completed

Description: You are unable to complete your check-in.



Solution: Check your site and area settings. Self check-in can fail due to one or more of the following:

1. Visitor management is not enabled for the site.
 - a. In Genetec ClearID™, click Organization > Sites.
 - b. Select your site and click Visitor Management.
 - c. Select Enable visitor management for this site.
 - d. Click Save.
2. Visitor management permissions for the site have not been configured.
 - a. In ClearID, click Organization > Sites.
 - b. Select your site and click Visitor Management > Permissions.
 - c. Check identity permissions.
 - d. Modify permissions as required and click Save.

For example, Add role permissions or give all identities access to invite visitors.
3. Visitor management is enabled for the site but no areas are defined or there is no default area.
 - a. In ClearID, check visitor management is enabled for the area. (Areas > Select an area > Visitor Management).
 - b. Check the Automatically add this area when creating visit requests is enabled.
4. Visitor management is enabled for the site and there is at least one default area under that site. However, the host does not have the authority to invite visitors for that site.
 - a. Refer to [Step 2](#).
5. Site is set to approval required. Visit event approval workflow should be set to No approval required.
 - a. In ClearID, click Organization > Sites and select your site.
 - b. Click Visitor Management, then in Advanced section check Visitor event approval workflow is set to No approval required.

Camera errors

Description: The Self-Service Kiosk can occasionally encounter the following camera issues:

- Unable to initialize the front camera.
- An error was encountered while configuring the camera. Try again.

Solution: Check the following:

1. On the iPad, tap Settings and scroll down to the Self-Service Kiosk app then tap Camera to enable the camera.
2. On the iPad, tap Settings > Privacy & Security and check that the Self-Service Kiosk has access to the camera.

Tip: These settings might not be visible on your iPad if you have not used the Scan QR code function before. In this situation, you can try the following: Tap Check-in > QR code, then tap Cancel and try the previous solution steps again.

14.10 | ClearID Self-Service Kiosk label printer issues

If the Genetec ClearID™ Self-Service Kiosk label printer is not performing as expected, you can check the configuration, check the hardware, or perform additional troubleshooting steps.

To help you troubleshoot Self-Service Kiosk label printer issues, refer to the possible causes and their respective solutions that follow.

No Bluetooth label printers detected

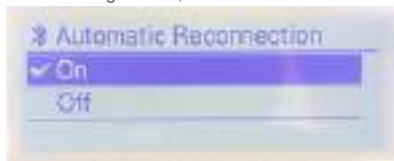
Description: No Bluetooth label printers were detected. This issue can be caused by a configuration or hardware issue.

Solution:

1. Check that the printer is powered on and ready for use.
2. Check that Bluetooth is enabled on the label printer.
 - a. In the Settings menu, select Bluetooth > Bluetooth (On/Off) > On and press OK.



- b. In the Settings menu, select Bluetooth > Automatic Reconnection (On/Off) > On and press OK.



3. Check that Bluetooth is enabled in the ClearID Self-Service Kiosk mobile app.
4. Check that Bluetooth is enabled on the iPad.
5. Check that the printer is paired with the ClearID Self-Service Kiosk.
6. (Optional) Perform a hard reset of the Self-Service Kiosk iPad.
 - a. Configure your Self-Service Kiosk iPad.
 - b. Do one of the following:
 - Configuring the ClearID Self-Service Kiosk label printer for Bluetooth mode (Brother QL-820NWBc or QL-820NWB).
 - Configuring the ClearID Self-Service Kiosk label printer for Bluetooth mode (Brother TD-4550DNWB).
 - c. Select a label printer.
 - d. Print a test badge.

No Wi-Fi label printers detected

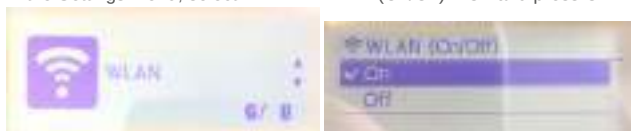
Description: No label printers were detected on the Wi-Fi network. This issue can be caused by a configuration or hardware issue.

Solution:

1. Check that the printer is powered on and ready for use.
2. Check that the Wi-Fi network is available.

The Wi-Fi network must be enabled for use and support the following:

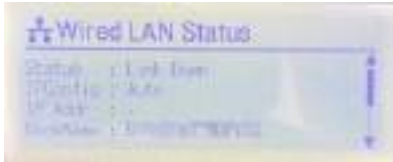
 - Bonjour - required for device search.
 - SNMP - required to check printer status information.
 - UDP or TCP Port 9100 - required to send print data.
3. Check that Wi-Fi is enabled on the label printer.
 - a. In the Settings menu, select WLAN > WLAN (On/Off) > On and press OK.



4. Check that Wi-Fi is enabled on the iPad.
5. Check that the Self-Service Kiosk iPad and the label printer are on the same Wi-Fi network.
6. (Optional) Perform a hard reset of the Self-Service Kiosk iPad.
 - a. Configure your Self-Service Kiosk iPad.
 - b. Do one of the following:
 - Configuring the ClearID Self-Service Kiosk label printer for Wi-Fi mode (Brother QL-820NWBc, QL-820NWB, or QL-810W).
 - Configuring the ClearID Self-Service Kiosk label printer for Wi-Fi mode (Brother TD-4550DNWB).
 - c. Select a label printer.
 - d. Print a test badge.

No Ethernet label printers detected

Description: The label printer is showing the Wired LAN Status Link Down.

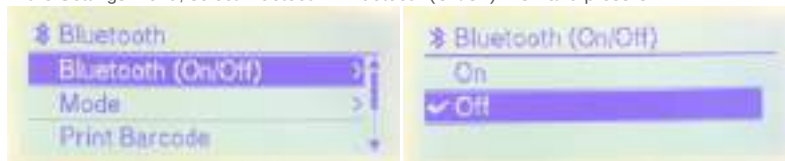


Solution:

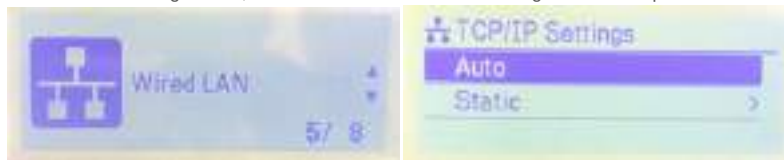
1. Check that the printer is powered on and ready for use.
2. Check that the Wi-Fi function on the label printer is turned off.
 - a. From the label printer Settings menu, turn OFF WLAN (Wi-Fi).



3. Check that the Bluetooth function on the label printer is turned off.
 - a. In the Settings menu, select Bluetooth > Bluetooth (On/Off) > Off and press OK.



4. Check that the Ethernet network is available.
5. Check that Ethernet is enabled on the label printer.
 - a. In the Settings menu, select Wired LAN > TCP/IP Settings > Auto and press OK.



6. Check that the printer is connected to a LAN port and not to a WAN port (either on your router or your organizations network).
7. Verify that you are using the correct type of LAN cable.
Best Practice: Use a straight-through Category 5 (or greater) twisted-pair cable for 10BASE-T or 100BASE-TX Fast Ethernet Network.
8. (Optional) Perform a hard reset of the Self-Service Kiosk iPad.
 - a. Configure your Self-Service Kiosk iPad.
 - b. Do one of the following:
 - Configuring the ClearID Self-Service Kiosk label printer for Ethernet mode (Brother QL-820NWBc or QL-820NWB).
 - Configuring the ClearID Self-Service Kiosk label printer for Ethernet mode (Brother TD-4550DNWB).
 - c. Select a label printer.
 - d. Print a test badge.

Printing: A printing error has occurred. There is no paper in the printer.

Description: The label printer has run out of labels or has jammed.

Solution:

1. Check for the end of the label roll and replace if necessary:
 - o Brother QL-820NWBc or QL-820NWB: DK Roll - 62mm Black (Brother Part No: DK-2205) or 62mm Red and Black (Brother Part No: DK-2251)
 - o Brother TD-4550DNWB: RD Roll - 57mm Black (Brother Part No: RD001U1S)
2. Check the printer for a label jam or feed error.

Brother QL-820NWBc or QL-820NWB: A printing error has occurred

Description: The Brother QL-820NWBc or QL-820NWB label printer has encountered an unknown printing error.



Solution:

1. Check the [Label Printer Led Status indicators FAQ](#) database for possible causes.
2. Check the [Connecting to a Mobile Device](#) section for possible causes.
3. Check the [FAQs & Troubleshooting Printing](#) section for possible causes.

Brother QL-820NWBC or QL-820NWB: Printer turns off unexpectedly

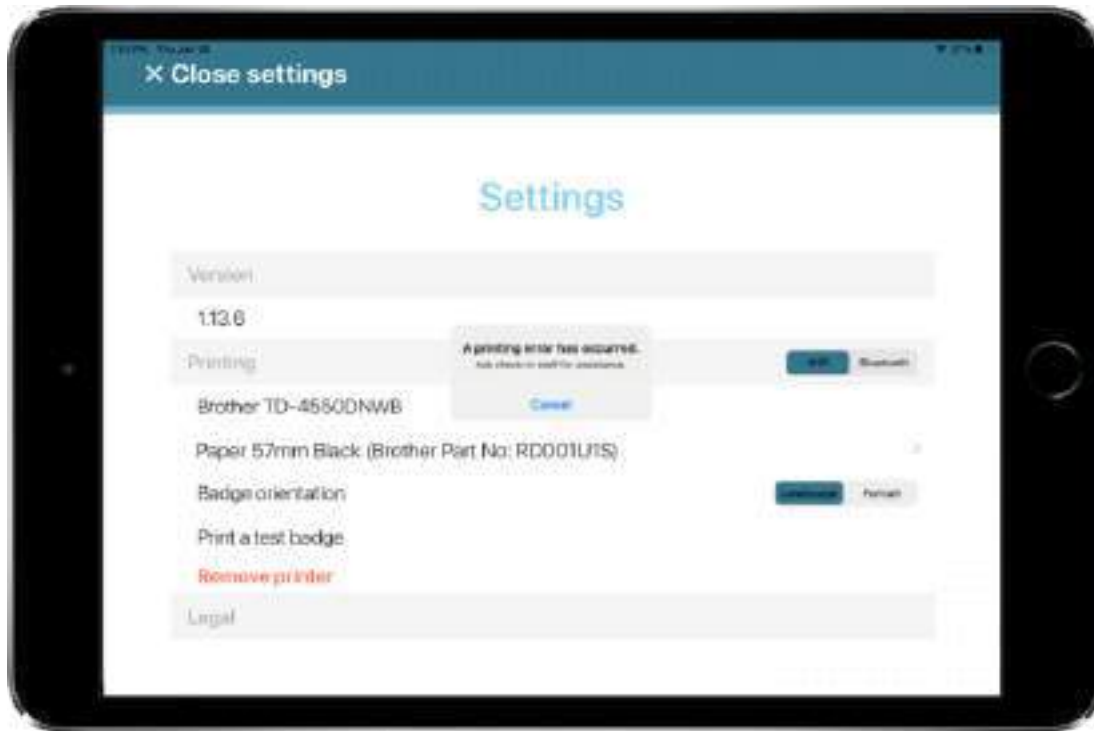
Description: The label printer turns off automatically at the same time every day.

Solution: Change the settings from the printer menu.

1. Press the Menu button.
2. Select Settings using the ▲ ▼ buttons, and then press the OK button.
3. Select Auto Power Off using the ▲ ▼ buttons, and then press the OK button.
4. Select Adapter using the ▲ ▼ buttons, and then press the OK button.
5. Select Off using the ▲ ▼ buttons, and then press the OK button.
6. (Optional) Also set the time to Off for [Li-ion battery], following the steps above.

Brother TD-4550DNWB: A printing error has occurred

Description: The Brother TD-4550DNWB label printer has encountered an unknown printing error.



Solution:

1. Check the [Label Printer Led Status indicators FAQ](#) database for possible causes.
2. Check the [Connecting to a Mobile Device](#) section for possible causes.
3. Check the [FAQs & Troubleshooting Printing](#) section for possible causes.

Brother TD-4550DNWB: Badge printout never arrives

Description: When printing a badge, the badges are sent to the printer but the printed badge never arrives.

Solution:

1. Check the printer LCD display to confirm you are not in a configuration or settings menu.
NOTE: Leaving the printer in a configuration or settings menu can cause badge printing to be paused until you complete your changes.
2. If you left the printer in a configuration or settings menu, press the Menu button or use the printer controls to return to the homepage.

After returning to the homepage, badge printing should resume as normal.

Brother TD-4550DNWB: Badges do not print as expected

Description: The label printer prints a partial label or label orientation appears to be messed up. For example, in some situations the printer can print half a badge or print across two labels.

Solution:

1. Before printing any badges, check your label alignment and orientation.



IMPORTANT: The first label must be aligned with the front edge of the printer to ensure correct printing. Make sure that none of the labels have advanced past the front edge of the printer before printing. The printer only detects the label edges automatically after printing the first label, if the first label is misaligned badge printing issues can occur.

For more information about how to load labels or sensor positioning for different label types, see [Load the RD roll](#) and [Check the Sensor Position](#) in the Brother online printer documentation.

Browse

- [Resetting the ClearID Self-Service Kiosk mobile app](#)
- [Firewall ports used in ClearID](#)



Genetec ClearID™ User Guide

Date: 2025-08-12

<https://techdocs.genetec.com>
Contact Us | Privacy Policy | Terms of Use © 2013-2020 Genetec Inc.

1. About ClearID

- 1.1. What is ClearID?
- 1.2. About ClearID architecture
 - 1.2.1. ClearID subprocessors list
- 1.3. About ClearID information security
- 1.4. How is ClearID different from traditional access control systems?
- 1.5. About workflows in ClearID
- 1.6. How the ClearID plugin works with Security Center
- 1.7. Integration overview for the ClearID plugin
- 1.8. Supported features list for ClearID
- 1.9. Supported languages in ClearID
- 1.10. ClearID terminology
- 1.11. ClearID videos
- 1.12. About reports in ClearID
- 1.13. Logging on to ClearID
- 1.14. Logging off from ClearID
- 1.15. Enabling preview features in ClearID
- 1.16. Disabling preview features in ClearID
- 1.17. Customizing portal branding in ClearID
- 1.18. Customizing help menu links in ClearID

2. What's new

- 2.1. What's new in ClearID
- 2.2. Previous features and enhancements in ClearID

3. Deployment preparation

- 3.1. License options for ClearID system integration
- 3.2. Compatibility for ClearID
- 3.3. System requirements for ClearID
- 3.4. Firewall ports used in ClearID
- 3.5. Supported devices for ClearID
- 3.6. ClearID Best practices
 - 3.6.1. Best practices for setting up ClearID for a new Synergis system
 - 3.6.2. Best practices for setting up ClearID with an existing Synergis system

4. ClearID plugin

- 4.1. About ClearID plugin for Security Center
- 4.2. About cardholder and identity relationships
- 4.3. Downloading and installing the ClearID plugin
- 4.4. Creating the ClearID plugin role
- 4.5. Connecting Security Center to ClearID
 - 4.5.1. Reviewing cardholders and identities information in ClearID
 - 4.5.2. Adding a system to ClearID
 - 4.5.3. Downloading an activation file for ClearID
 - 4.5.4. Configuring connection settings for ClearID
- 4.6. Granting user privileges for the ClearID plugin
- 4.7. About ClearID system states
- 4.8. About custom fields in ClearID
 - 4.8.1. Modifying ClearID custom fields in Config Tool
 - 4.8.2. Custom fields relationships

5. Managing identities and users

- 5.1. Creating identities in ClearID
- 5.2. Identity fields in ClearID
- 5.3. About custom identity fields in ClearID
- 5.4. Creating custom identity fields in ClearID
- 5.5. Granting additional permissions for identities and roles in ClearID
- 5.6. Granting additional permissions for supervisors in ClearID
- 5.7. Viewing additional permissions in ClearID
 - 5.7.1. Modifying additional permissions in ClearID
- 5.8. Viewing identities in ClearID
- 5.9. Modifying identities in ClearID
- 5.10. Deleting identities in ClearID
- 5.11. Synchronizing ClearID identity pictures with Security Center
- 5.12. About webhooks in ClearID
- 5.13. Creating webhooks in ClearID
 - 5.13.1. Modifying webhooks in ClearID
- 5.14. Viewing webhook logs in ClearID
- 5.15. Granting access to the ClearID web portal
 - 5.15.1. Granting user access to the ClearID web portal
 - 5.15.2. Granting administrator access to the ClearID web portal

- 5.16. Viewing your profile in ClearID
 - 5.16.1. Configuring your ClearID portal theme preferences
- 5.17. Viewing your site and area access in ClearID
- 5.18. Setting request visibility for users in ClearID
- 5.19. About access request workflow in ClearID
- 5.20. Requesting access in ClearID
- 5.21. Adding supervisors manually in ClearID
- 5.22. Viewing direct reports in ClearID
- 5.23. Managing direct reports in ClearID
- 5.24. Transferring direct reports in ClearID
- 5.25. About direct reports report in ClearID
- 5.26. Resetting user passwords in ClearID
- 5.27. About email notifications in ClearID
 - 5.27.1. Customizing the email banner for sites in ClearID
 - 5.27.2. Configuring email notification preferences in ClearID (administrator)
 - 5.27.3. Configuring your ClearID email notification preferences
- 5.28. About delegation in ClearID
- 5.29. Delegating ClearID tasks to another user
- 5.30. About user activity report in ClearID
- 5.31. Viewing a user activity report in ClearID
- 5.32. User levels in ClearID
- 5.33. About identity request workflow in ClearID
- 5.34. Creating an identity template in ClearID
 - 5.34.1. Modifying an identity template in ClearID
- 5.35. Requesting identities in ClearID
 - 5.35.1. Requesting an identity in ClearID
 - 5.35.2. Requesting multiple identities using a CSV import in ClearID
- 5.36. Canceling identity requests in ClearID
- 5.37. Approving identity requests in ClearID
 - 5.37.1. Modifying an identity request in ClearID
- 5.38. About identity requests report in ClearID
- 5.39. Checking the status of identity requests in ClearID

6. Credential synchronization

- 6.1. Configuring credential replication in ClearID
- 6.2. Viewing credential synchronization logs in ClearID
- 6.3. Forcing credential synchronization in ClearID

7. Managing sites

- 7.1. About sites in ClearID
- 7.2. Creating sites in ClearID
 - 7.2.1. Adding site owners in ClearID
 - 7.2.2. Enabling visitor management for sites in ClearID
 - 7.2.2.1. Viewing sites where a user can invite visitors
- 7.3. Modifying sites in ClearID
- 7.4. Setting a maximum duration for site access in ClearID
- 7.5. Configuring access request documents for sites in ClearID
- 7.6. Customizing email notifications for sites in ClearID
 - 7.6.1. Customizing ClearID email notification branding
- 7.7. About access reviews in ClearID
- 7.8. Setting up automatic expiration for access reviews
- 7.9. Setting up area access reviews in ClearID
 - 7.9.1. Scheduling area access reviews in ClearID
- 7.10. Setting up identity access reviews in ClearID
 - 7.10.1. Scheduling identity access reviews in ClearID
- 7.11. Modifying access reviews in ClearID
- 7.12. About access reviews report in ClearID
- 7.13. Checking the status of access reviews in ClearID
- 7.14. Completing an area access review (site owner) in ClearID
- 7.15. Completing an area access review (area manager or role manager) in ClearID
- 7.16. Completing an identity access review (supervisor) in ClearID
- 7.17. Generating an access review summary in ClearID
- 7.18. About access requests report in ClearID
- 7.19. Checking the status of access requests in ClearID
- 7.20. About site activity report in ClearID
- 7.21. Viewing a site activity report in ClearID
- 7.22. About site and area owners report in ClearID
- 7.23. Viewing a site and area owners report in ClearID

8. Managing areas

- 8.1. About areas in ClearID

- 8.2. Creating areas in ClearID
 - 8.2.1. Adding doors to areas in ClearID
 - 8.2.2. Enabling visitor management for areas in ClearID
 - 8.2.3. About nested areas in Security Center
 - 8.2.4. Granting access to areas in Security Center automatically
- 8.3. Adding area owners and managers in ClearID
- 8.4. Adding schedules to an area in ClearID
- 8.5. Configuring access request documents for areas in ClearID
- 8.6. Granting access to an area in ClearID
- 8.7. Reviewing area access in ClearID
- 8.8. Approving area access requests in ClearID
- 8.9. Rejecting area access requests in ClearID
- 8.10. Creating exceptions to the access request approval workflow in ClearID

9. Managing visitors

- 9.1. About visit request workflow in ClearID
- 9.2. About visit request watchlist workflow in ClearID
- 9.3. Inviting visitors in ClearID
 - 9.3.1. Inviting visitors manually in ClearID
 - 9.3.2. Inviting visitors using a CSV import in ClearID
 - 9.3.3. SMS alerts in ClearID
- 9.4. Reviewing visit events in ClearID
- 9.5. About visit event logs in ClearID
- 9.6. Viewing visit event logs in ClearID.
- 9.7. Copying a visit event in ClearID
- 9.8. Modifying visit events in ClearID
- 9.9. Approving visit event requests in ClearID
- 9.10. Adding ClearID visit events to your calendar
- 9.11. About visitors report in ClearID
- 9.12. Viewing a visitors report in ClearID
- 9.13. QR codes as a credential for visitors in ClearID
 - 9.13.1. Importing a custom card format (QR code credential) in Synergis
 - 9.13.2. Enabling QR code credentials for visitors in ClearID
 - 9.13.3. Configuring Qscan devices for ClearID
 - 9.13.3.1. Connecting a Qscan barcode reader to a Mercury Controller for ClearID
 - 9.13.3.2. Configuring Qscan barcode reader to support 40-bit hexadecimal QR codes for ClearID
 - 9.13.4. Configuring STid devices for ClearID
 - 9.13.4.1. About STid QR code readers in ClearID
 - 9.13.4.2. Creating an STid QR code reader configuration for ClearID
 - 9.13.4.3. Transferring your reader configuration to your STid QR code reader for ClearID
 - 9.13.5. Automating visitor access and check-in using a macro in Security Center

10. Managing visitor watchlists

- 10.1. About watchlists in ClearID
- 10.2. Adding watchlist managers in ClearID
- 10.3. Adding watchlists in ClearID
 - 10.3.1. Adding an individuals watchlist entry in ClearID
 - 10.3.2. Adding a companies watchlist entry in ClearID
 - 10.3.3. Importing watchlist entries from a file in ClearID
 - 10.3.4. Exporting watchlist entries to a file in ClearID
 - 10.3.5. Testing watchlist entries in ClearID
 - 10.3.6. Deleting watchlist entries in ClearID
- 10.4. Modifying watchlists in Genetec ClearID
- 10.5. Deleting watchlists in Genetec ClearID
- 10.6. Screening visitors manually in ClearID
- 10.7. Unblocking visitors blocked by a watchlist in ClearID

11. Role-based access control

- 11.1. About role-based access control in ClearID
- 11.2. Adding roles in ClearID
- 11.3. Configuring role managers in ClearID
- 11.4. Configuring role-based access control policies in ClearID
 - 11.4.1. Scenario 1: Adding employees to an IT role in ClearID
 - 11.4.2. Scenario 2: Adding contractors to a certified contractor engineering role in ClearID
 - 11.4.3. Scenario 3: Adding employees to an ADA personnel role in ClearID
- 11.5. Adding custom provisioning attributes to an identity in ClearID
- 11.6. Adding role members in ClearID
- 11.7. About role activity report in ClearID
- 11.8. Viewing a role activity report in ClearID

12. Connecting to other systems

- 12.1. Authenticating your connection with ClearID
- 12.2. Setting up data synchronization
- 12.3. Synchronizing identities using an API in ClearID
 - 12.3.1. About the ClearID API
- 12.4. Synchronizing identities using the SCIM integration in ClearID
 - 12.4.1. About the SCIM standard in ClearID
 - 12.4.2. About Microsoft Entra ID attribute fields in Microsoft Azure

- 12.4.3. Configuring the SCIM integration in ClearID
 - 12.4.3.1. Generating a SCIM key in ClearID
 - 12.4.3.2. Creating an enterprise application in Microsoft Azure
 - 12.4.3.3. Connecting your ClearID SCIM integration to Microsoft Entra ID
 - 12.4.3.4. Disabling Microsoft Entra ID groups setting in Microsoft Azure
 - 12.4.3.5. Configuring Microsoft Entra ID user settings in Microsoft Azure
 - 12.4.3.6. Configuring the ClearID SCIM integration synchronization settings in Microsoft Azure
- 12.4.4. Resetting SCIM integration identity data in ClearID
- 12.4.5. Reviewing the SCIM integration synchronization status in Microsoft Azure

12.5. Synchronizing identities using One Identity Synchronization Tool in ClearID

- 12.5.1. About the ClearID One Identity Synchronization Tool
- 12.5.2. About ClearID One Identity Synchronization Tool attribute fields
- 12.5.3. About the Azure web app for ClearID One Identity Synchronization Tool
- 12.5.4. Installing the ClearID One Identity Synchronization Tool
 - 12.5.4.1. Uninstalling the ClearID One Identity Synchronization Tool
 - 12.5.4.2. Upgrading the ClearID One Identity Synchronization Tool
- 12.5.5. Configuring the ClearID One Identity Synchronization Tool
 - 12.5.5.1. Configuring connection settings for the ClearID One Identity Synchronization Tool
 - 12.5.5.2. Configuring the data source for Azure AD synchronization in the ClearID One Identity Synchronization Tool
 - 12.5.5.3. Configuring the data source for Database synchronization in the ClearID One Identity Synchronization Tool
 - 12.5.5.4. Configuring the data source for File synchronization in the ClearID One Identity Synchronization Tool
 - 12.5.5.5. Configuring synchronization settings in the ClearID One Identity Synchronization Tool
- 12.5.6. Reviewing synchronization status for the ClearID One Identity Synchronization Tool
- 12.5.7. About ClearID One Identity Synchronization Tool logs
- 12.5.8. Viewing the ClearID One Identity Synchronization Tool logs
- 12.5.9. Updating existing identities from an external data source using ClearID One Identity Synchronization Tool

12.6. Synchronizing identities using LDAP in ClearID

- 12.6.1. About ClearID LDAP Synchronization Agent
- 12.6.2. LDAP attributes to ClearID attribute mappings
- 12.6.3. Configuring the ClearID LDAP Synchronization Agent

13. Visitor management devices

13.1. About ClearID Self-Service Kiosk

- 13.1.1. About ClearID Self-Service Kiosk check-in
- 13.1.2. About ClearID Self-Service Kiosk Self registration

13.2. Configuring the ClearID Self-Service Kiosk iPad

- 13.2.1. Customizing the ClearID Self-Service Kiosk configuration
- 13.2.2. Customizing the ClearID Self-Service Kiosk visitor badge logo
- 13.2.3. Adding visitor compliance documents to the ClearID Self-Service Kiosk
- 13.2.4. Activating badge reprinting for the ClearID Self-Service Kiosk
- 13.2.5. Disabling visitor photo during ClearID Self-Service Kiosk check-in
- 13.2.6. Activating visitor photo retention in ClearID

13.3. About ClearID mobile operator check-in

13.4. Configuring ClearID mobile operator check-in

13.5. Configuring the ClearID Self-Service Kiosk label printer (Brother QL-820NWBc, QL-820NWB, or QL-810W)

- 13.5.1. Configuring the ClearID Self-Service Kiosk label printer for Bluetooth mode (Brother QL-820NWBc or QL-820NWB)
- 13.5.2. Configuring the ClearID Self-Service Kiosk label printer for Wi-Fi mode (Brother QL-820NWBc, QL-820NWB, or QL-810W)
- 13.5.3. Configuring the ClearID Self-Service Kiosk label printer for Ethernet mode (Brother QL-820NWBc or QL-820NWB)

13.6. Configuring the ClearID Self-Service Kiosk label printer (Brother TD-4550DNWB)

- 13.6.1. Configuring the ClearID Self-Service Kiosk label printer for Bluetooth mode (Brother TD-4550DNWB)
- 13.6.2. Configuring the ClearID Self-Service Kiosk label printer for Wi-Fi mode (Brother TD-4550DNWB)
- 13.6.3. Configuring the ClearID Self-Service Kiosk label printer for Ethernet mode (Brother TD-4550DNWB)

13.7. Selecting a ClearID Self-Service Kiosk label printer

13.8. Printing a test badge from the ClearID Self-Service Kiosk

13.9. Resetting the ClearID Self-Service Kiosk mobile app

13.10. ClearID Self-Service Kiosk options

- 13.10.1. ClearID Self-Service Kiosk floor stand
- 13.10.2. ClearID Self-Service Kiosk floor stand printer shelf
- 13.10.3. ClearID Self-Service Kiosk tabletop stand

13.11. Identity document types in ClearID

14. Troubleshooting

- 14.1. Plugin installed, but missing from Security Desk and Config Tool
- 14.2. Plugin role could not find file with certificate
- 14.3. Custom fields not displayed in Security Desk
- 14.4. No active account found for user
- 14.5. Visit email notifications not received by visitors
- 14.6. Visitor hosts fields in Security Desk are empty
- 14.7. ClearID One Identity Synchronization Tool connectivity issues
- 14.8. ClearID One Identity Synchronization Tool data synchronization issues
- 14.9. ClearID Self-Service Kiosk issues
- 14.10. ClearID Self-Service Kiosk label printer issues

1 | About ClearID

1.1 | What is ClearID?

Genetec ClearID™ is a smarter way to manage physical access using a self-service solution for Synergis™. Using ClearID, you can take control of access and compliance by using a rule-based approach through a web-based interface.

- You can access the system from any standard browser. All data and files that are imported to the system are automatically encrypted.
- The ClearID system is also integrated with Active Directory. This integration means that organizations can use their existing Active Directory service to authenticate users and manage system access.

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

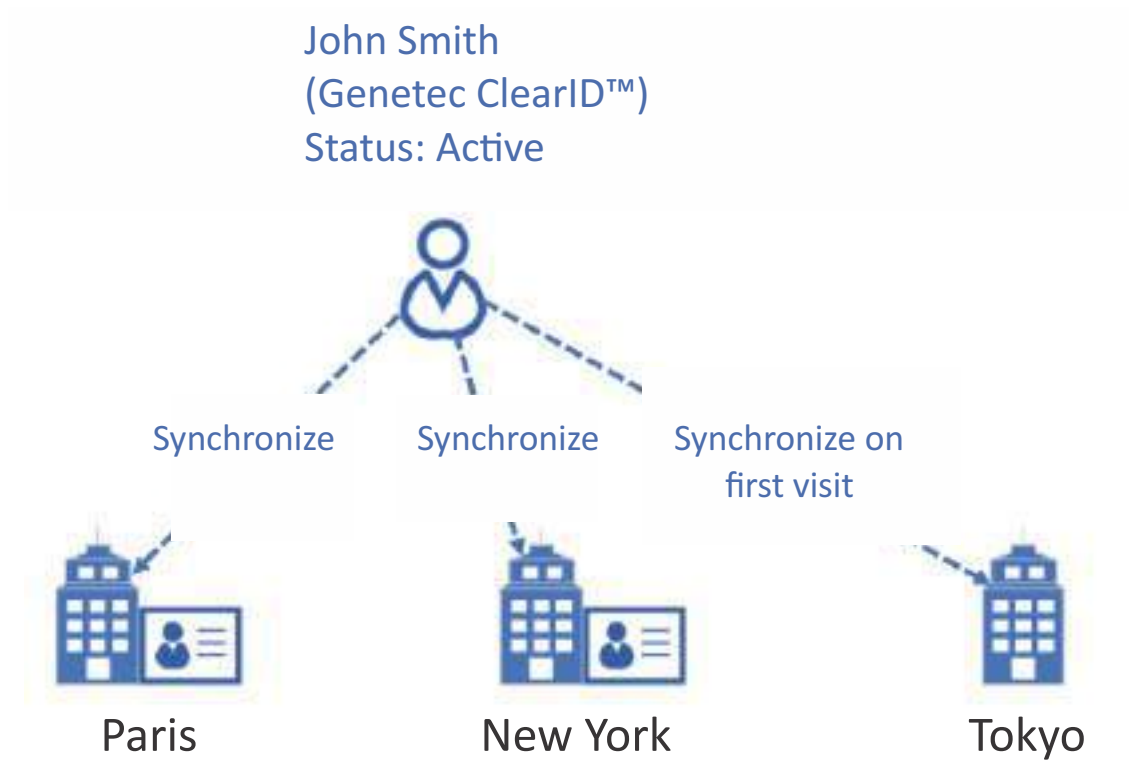
For a complete product description, visit the [ClearID](#) product page.

Advantages of the ClearID system

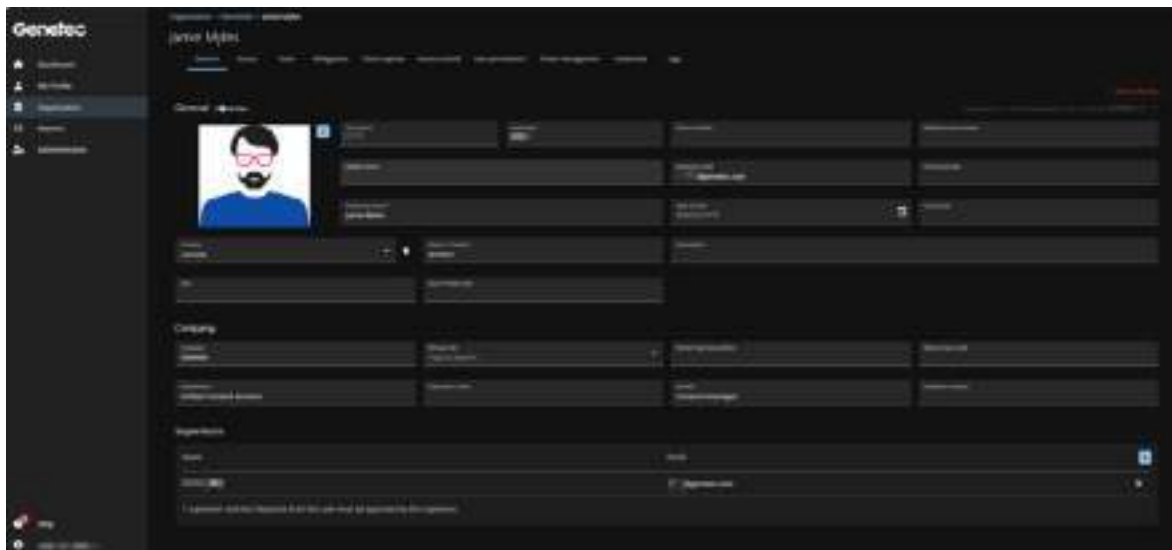
- Improve the flow of people by using the self-service solution to manage physical access.
- Reduce the risk of security breaches by simplifying access rights management.
- Standardize and automate security policies for onboarding, offboarding, access requests, and issuing credentials for multiple independent sites.
- Connect to and enhance your existing physical security system.
- Benefit from an off-the-shelf approach with faster deployment and fewer integrations to maintain.
- Maintain less infrastructure by using the distributed cloud-based approach.
- Increase efficiency and compliance with internal and external regulations, such as GDPR and export control screening.

One identity

ClearID uses one single identity to synchronize the access information for multiple independent sites managed using different instances of Synergis.



To minimize the personal information replicated in each local access control system, ClearID automatically creates the cardholder only when someone requests a site visit for the first time.



After access is granted to a new site, the system automatically synchronizes all the permanent credentials linked to the Identity. If the corporation shares the same card technology for different sites, the badge works without any manual interventions at the new site.

When an identity is deactivated in ClearID, the cardholder is deactivated. The identity is automatically synchronized to all cardholders linked to all the different areas in all sites. The credentials remain active in Security Center, but access is automatically denied because the cardholder is inactive.

Browse

- [ClearID videos](#)

Browse

- [ClearID Technical Brochure \(8 pages\)](#)
- [ClearID - Product page](#)
- [ClearID - Portfolio page](#)
- [Genetec Compliance Portal](#)

1.2 | About ClearID architecture

Genetec ClearID™ offers United States-only, European-only, Canadian-only, or Australian-only location options for data centers. Each option allows synchronization between local sites. The web application modules perform tasks or share data between the authoritative sources, ClearID, and the endpoints.

IMPORTANT: Transferring or copying a customer account from one instance to another isn't supported.

USA distributed architecture

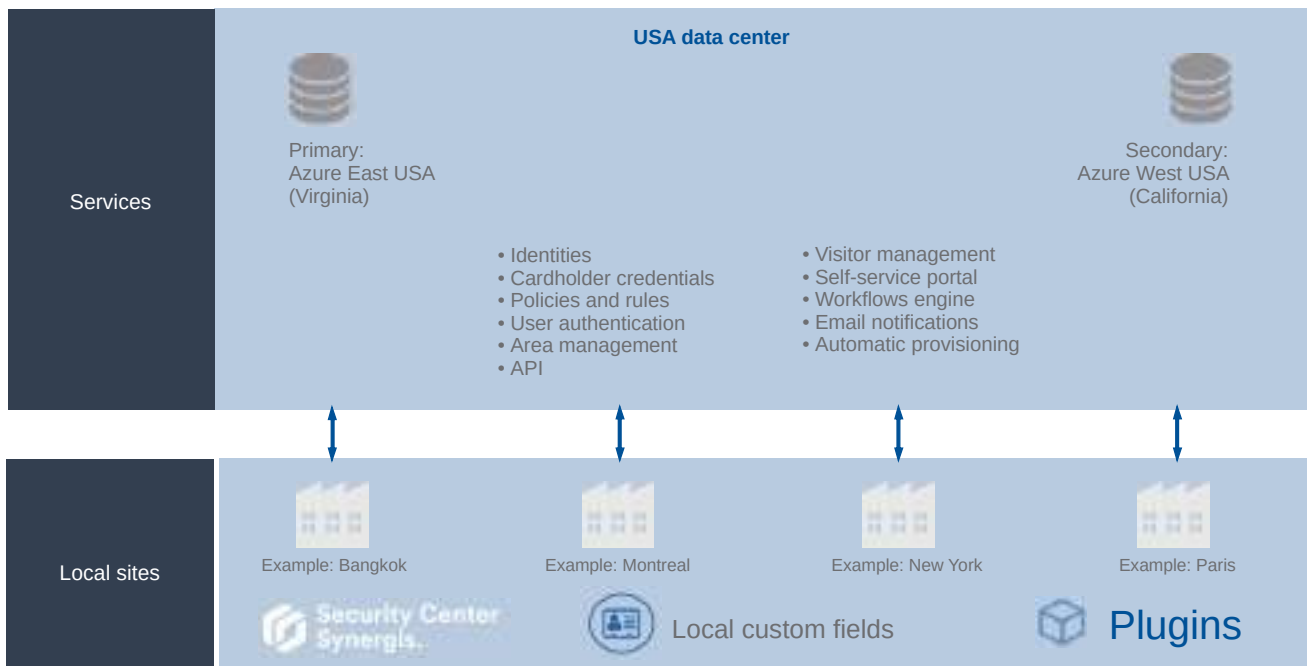
The following diagram illustrates the USA distributed solution. The diagram shows what data is stored, where data is stored, and how data flows between the local sites and the regional services.

NOTE: Regional services data is stored in the cloud.

ClearID takes advantage of the following:

- Multiple Azure data centers to minimize the risk of downtime.
- Encrypted employee data to minimize the risk of data theft.
- Geo-localized data to maintain less infrastructure and provide an optimized approach for data flow performance.

Genetec ClearID™ USA only architecture



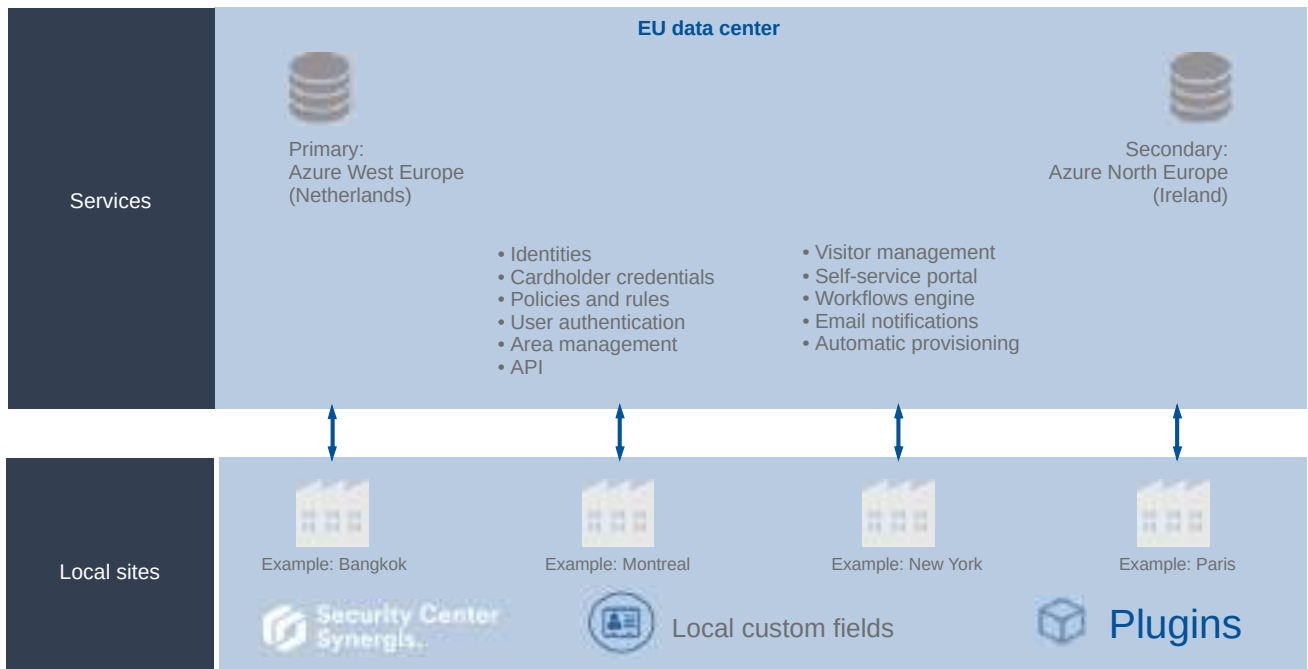
NOTE: ¹For more information about which data centers are used in the regional deployments, see the *Microsoft Corporation* entry in the ClearID section of the Genetec Subprocessors list.

For visitors, the relevant guest information is stored with the visit event information. This information is then transferred to the Security Center managing the site visited.

Europe only architecture

The following diagram illustrates the Europe-only solution where data is stored in European data centers. For example, when customers or company policies require data to be stored in European data centers.

Genetec ClearID™ Europe only architecture



NOTE: You can also choose from Canada-only and Australia-only data storage solutions.

Canadian data centers

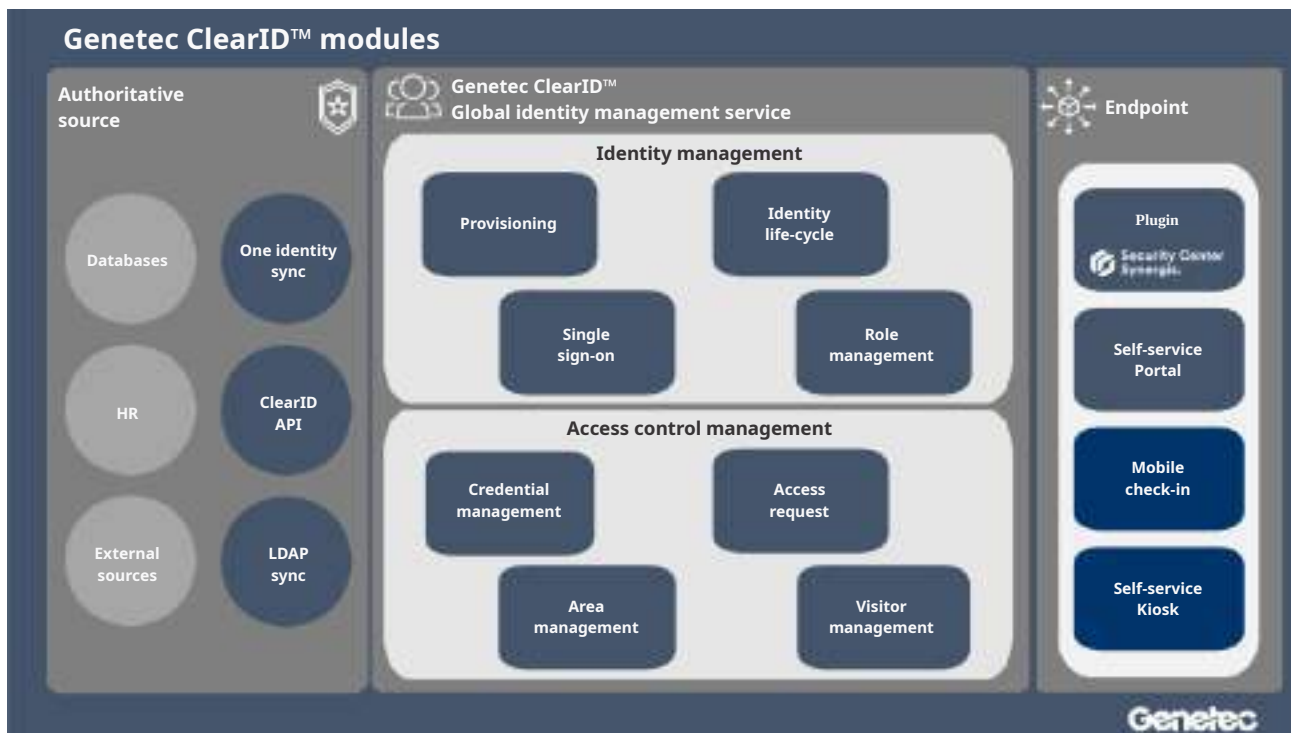
- Primary data center: Azure Central Canada (Ontario)
- Secondary data center: Azure East Canada (Quebec)

Australian data centers

- Primary data center: Azure East Australia (New South Wales)
- Secondary data center: Azure Central Australia (Canberra)

ClearID modules

The following diagram illustrates the ClearID web application modules that are available to customers:



Authoritative source

Shows the identity provisioning options that are available to customers. You can create identities in ClearID from one of the data sources (Databases, HR, External sources) by using one of the tools (Genetec ClearID™ One Identity Synchronization Tool, Genetec ClearID™ API, or the Genetec ClearID™ LDAP Synchronization Agent).

Global identity management service

Shows an overview of the features and services offered by the ClearID platform.

Endpoint

Shows the modules that customers directly interact with. These modules are where the customer enters their data or configures their system.

Cloud architecture

ClearID is deployed on the Microsoft Azure cloud platform, to take advantage of its industry-recognized security. Microsoft Azure has been audited against SOC 1, SOC 2, and SOC 3 standards. Audits are conducted in accordance with ISO SSAE 16 and ISAE 3,402 standards. Certifications are regularly updated and can be provided upon request. Azure is also compliant with ISO 27001.

The service architecture is built for High availability (HA) and scalability. Data stored in ClearID is redundant, ensuring the redundancy of critical data and mitigating the impact of hardware failure. This architecture, coupled with the robustness of the underlying Microsoft Azure cloud, means that we can provide a 99.9% SLA.

Security controls

Microsoft Azure adheres to a rigorous set of security controls that govern operations and support. Microsoft deploys a combination of preventive, defensive, and reactive controls including the following mechanisms that help to protect against unauthorized developer or administrative activity:

- Strict access controls on sensitive data, including a requirement for two-factor smart card-based authentication to perform sensitive operations.
- Combinations of controls that enhance independent detection of malicious activity.
- Multiple levels of monitoring, logging, and reporting.
- Security reports can be used to monitor access patterns and to identify and reduce potential threats proactively.
- Microsoft administrative operations, including system access, are logged to provide an audit trail if unauthorized or accidental changes are made.

High availability

Azure facilities are designed to run 24x7x365 and use various measures to help protect operations from power failures, physical intrusions, and network outages. These data centers comply with industry standards for physical security and availability. Microsoft operations personnel manage, monitor, and administer these Azure facilities.

Browse

- [Global Privacy Policy](#)
- [Product Privacy Sheet - ClearID](#)
- [Genetec Compliance Portal](#)

1.2.1 | ClearID subprocessors list

Genetec ClearID™ uses third-party vendors to assist Genetec™ in the provision of ClearID cloud services and which, as part of their responsibilities, might collect, access, store, or otherwise process customer data (including personal data).

For the latest information regarding third-party subprocessor vendors, see [List of Subprocessors](#).

Parent topic: [About ClearID architecture](#)

Browse

- [About ClearID information security](#)

1.3 | About ClearID information security

All data and files imported in Genetec ClearID™ are encrypted, and all communication with the platform is secure. These encryption and security measures ensure that sensitive data, files, and communications are only seen by users with the appropriate access.

Cryptography standards

Data encryption

All personal information managed by ClearID is automatically encrypted using Advanced Encryption Standard 256 bits (AES-256) with symmetric keys that are dynamically generated. This automatic encryption ensures that each blob of data like an identity is given a unique AES key.

For extra protection, the AES key is also encrypted with a public key unique to the account's private key. All the cryptographic keys used by ClearID are securely managed using the Azure Key Vault, which supports FIPS 140-2 Level 2 validated HSMs.

Data integrity

A digital signature (SHA 512 with RSA) is generated to detect any attempts to modify data and ensure the integrity of the data and actions in the system. Analyzing and uniquely identifying all data using a complex algorithm prevents attackers from deleting, modifying, or adding content to data stored in ClearID.

Communication encryption

Communication in the platform is secured using Hypertext Transfer Protocol Secure (HTTPS) protocol and Transport Layer Security (TLS) certificates to ensure that only trusted parties have access to data managed by ClearID. This communication encryption ensures the confidentiality of the information and reduces the possibility of malicious attempts to intercept or alter communication in transit.

Network and information security

As a trusted provider of security solutions for government agencies and high-profile public and private organizations worldwide, we take compliance with local laws seriously. This compliance includes the laws related to data security and protection of privacy in the territories where we sell our products and services.

To ensure that all customer data is stored and used appropriately and securely, ClearID is an ISO/IEC 27001 certified Information Security Management System.

Secure development and operations

Our development and operations teams have been certified ISO 27001:2013. Our dedicated security team administrates and reviews architecture and design requirements, ensuring that we meet the highest industry standards and regulations, including General Data Protection Regulation (GDPR). Every change in ClearID undergoes a strict series of automated security tests and regular penetration tests performed by industry leaders in Information Security.

Zero-trust architecture

Customer data is segmented over a series of microservices. Each microservice has one specific role in the system and the service has access only to the minimum data required to perform that task. There is no central repository of data that can be attacked. The information is distributed across siloed, independent repositories. The data center network is considered unsafe in our zero-trust architecture. All data transmitted and received between microservices is encrypted and digitally signed.

Service monitoring

We subscribe to various security threat feeds and services, including Check Point, Microsoft, Mandiant, and Hyphen. Based on the nature of evolving threats, we adapt our controls as often as necessary.

Production environments are constantly monitored using the following monitoring services:

- Perform a series of synthetic transactions every 5 minutes to emulate users from different locations in the world.
- Constantly measure a series of metrics from the servers to detect any anomalies, such as a high number of web request failures.
- Automatically raise the alarm to our development and operations team, who take immediate action to correct the issue and mitigate any impact in the production environment.

The goal is to detect transient errors, data center issues, performance degradation, and ISP outages, before users notice any impact to their system.

User authentication

By default, ClearID uses Microsoft Entra ID B2C and Entra ID B2B for user authentication. Organizations can also federate their existing Active Directory (AD) user identities through Microsoft Entra ID, or any system that supports the OpenID Connect standard, to provide a single sign-on (SSO) experience and ensure that the system meets the corporate policies requirements for user authentication.

The authentication system is based on a passive authentication model with OAuth 2.0 and OpenID Connect, which allows the identity server (AD or others) to present the connection page immediately. Identity administrators can define how users are authenticated. For example, passwords, tokens, biometrics, or a combination of these techniques.

By using Active Directory, organizations can enforce a large variety of user and password validation rules and expiration requirements. A few examples of requirements include multi-factor authentication, deactivating a user credential after several failed sign in attempts, and many other configuration options.

Browse

- [Global Privacy Policy](#)
- [Product Privacy Sheet - ClearID](#)
- [Genetec Compliance Portal](#)

1.4 | How is ClearID different from traditional access control systems?

Use the following information to help you understand how Genetec ClearID™ is different from traditional access control systems.

In traditional access control systems, security personnel are constantly involved to grant or deny access to physical locations:

- Security personnel must verify with the room owners before granting access to someone.
- When the access is no longer required, the person never goes back to security to ask to be removed from the room.
- Most sites do not track or record why access was required.

In ClearID, the self-service Web portal reduces effort and increases flexibility by using *workflows* when employees, managers, and owners of the different secure areas request and grant access.

Requests are processed as follows:

1. Separate requests and approval workflows are created for each request.

Each request includes the requester identity, time of request, reason for request, and other audit trail information.

2. Each request generates email notifications for the requester and for approvers.
3. After the request summary is confirmed, it is automatically assigned to the right individuals for approval.

4. The employee manager, area owners, and other approvers receive an email requiring them to approve, deny, or modify the submitted request.
5. After the approval process occurs, the requester receives an email notifying them whether their request was approved or rejected.

NOTE: Access, visit, or identity requests can be limited to a specific period, as opposed to the traditional method of an infinite period.

Using the self-service portal, employees can request access to specific areas in the same building or in a different site. Even when the site is managed by a different instance of Security Center.

If a person is traveling for the first time to an office managed by a different instance of Synergis™, the system automatically creates a cardholder and synchronizes all the credentials a few hours before the travelers arrive on site. On the last day of the trip, as specified in the access request, the system automatically revokes access to the secure area.

Browse

- [About workflows in ClearID](#)

1.5 | About workflows in ClearID

Genetec ClearID™ uses workflows to process, and then approve or reject, access requests, visit requests, or identity requests.

NOTE: Depending on how you configure your sites and areas, some of the workflow processes might not apply to your environment.

The following *workflows* are provided to support the different request types:

Access request workflow

An access request workflow is a series of activities performed by the system or authorized people during the life cycle of an access request. The activities can change the state and properties of access requests, affect other entities in the system, or wait for a condition to be met.

Visit request workflow

A visit request workflow is a series of activities performed by the system or authorized people during the life cycle of a visit request. The activities can change the state and properties of visit requests, affect other entities in the system, or wait for conditions to be met.

Visit request watchlist workflow

A watchlist workflow is a series of activities performed by the system or authorized people during the life cycle of a visit request if watchlists are enabled. The activities can change the state and properties of watchlists, affect other entities in the system, or wait for conditions to be met.

Identity request workflow

An identity request workflow is a series of activities performed by the system or authorized people during the life cycle of an identity request. The activities can create an individual identity, or multiple identities using a CSV import, and add each new identity to a role to inherit relevant access for a specified period.

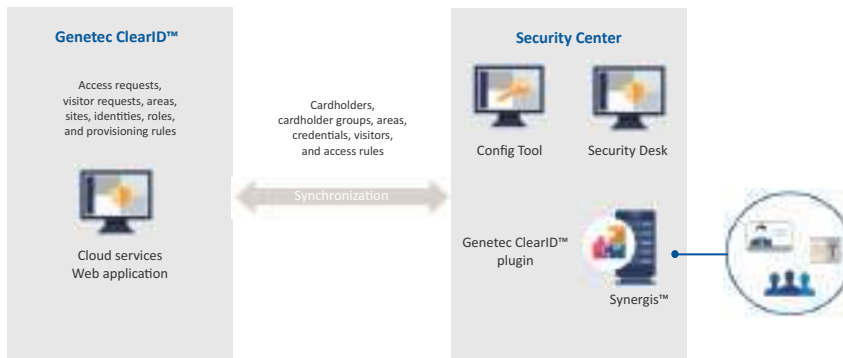
Browse

- [About access request workflow in ClearID](#)
- [About visit request workflow in ClearID](#)
- [About visit request watchlist workflow in ClearID](#)
- [About identity request workflow in ClearID](#)
- [Creating exceptions to the access request approval workflow in ClearID](#)

1.6 | How the ClearID plugin works with Security Center

The Genetec ClearID™ plugin is required to synchronize data between the Genetec ClearID™ web application and Security Center.

The components of the ClearID plugin integration



ClearID

Genetec ClearID™ is a smarter way to manage physical access using a self-service solution for Synergis™.

ClearID plugin

The ClearID plugin is installed on a Security Center server and runs as a plugin role.

The Genetec ClearID™ Plugin integrates Genetec ClearID™ with Security Center and connects Synergis™ and ClearID cloud services. Any actions performed in ClearID are automatically synchronized with Synergis.

Security Center

Security Center is a truly unified platform that blends IP video surveillance, access control, automatic license plate recognition, intrusion detection, and communications within one intuitive and modular solution. By taking advantage of a unified approach to security, your organization becomes more efficient, makes better decisions, and responds to situations and threats with greater confidence.

The ClearID plugin is installed on a Security Center server. The plugin can be installed on the Directory or an expansion server.

Config Tool

The ClearID plugin is also installed on a Config Tool workstation. The Security Center administrator uses Config Tool to create and configure the plugin role, configure database settings, and connection settings for ClearID. You can also configure a proxy connection if required. For example, when servers do not have internet access.

Security Desk

Security Desk operators can create credentials, check in visitors, or assign and print badges.

Synergis

Security Center Synergis™ is the IP access control system (ACS) that heightens your organization's physical security and increases your readiness to respond to threats. Synergis™ supports an ever-growing portfolio of third-party door control hardware and electronic locks. Using Synergis™, you can leverage your existing investment in network and security equipment.

The following information is extracted from Synergis for use by ClearID:

- Access rules
- Areas
- Cardholders
- Cardholder groups
- Credentials
- Schedules
- Visitors

NOTE: In Config Tool and Security Desk, entities managed by ClearID are highlighted with a blue dot in the bottom-right corner of the entity icon as follows:

- Access rules (🟡)
- Areas (🏠)
- Cardholders (👤)
- Cardholder groups (👥)
- Credentials (🔑)
- ClearID partitions (🌐)
- Visitors (👤)

Browse

- [Downloading and installing the ClearID plugin](#)

1.7 | Integration overview for the ClearID plugin

You can integrate the Genetec ClearID™ web application with Security Center by installing and configuring the ClearID plugin and following a sequence of steps.

Genetec ClearID®; User Guide

Displayed in the header

The following table lists the tasks required for the integration with Security Center, and how to verify that the integration is successful.

Step	Task	Where to find more information
Understand the prerequisites and key issues before deploying		
1	Learn about what you can do using ClearID.	- What is ClearID? - How is ClearID different from traditional access control systems? - About workflows in ClearID. - Supported features list for ClearID. - Supported languages in ClearID.
2	Before installing the plugin, read the release notes to learn about the new features.	What's new in ClearID.
3	Familiarize yourself with the common terms and their equivalents in Security Center.	ClearID terminology.
4	Learn about the different components and how they connect.	- How the ClearID plugin works with Security Center. - About ClearID architecture. - ClearID subprocessors list. - About ClearID information security.
5	Learn about key features and understand the product.	ClearID videos.
Deployment Preparation		
1	Ensure that the plugin is installed on a server that meets the recommended system requirements and is running a compatible version of Security Center.	- Compatibility for ClearID. - System requirements for ClearID. - Firewall ports used in ClearID.
2	Learn about the devices that are supported for use with ClearID.	Supported devices for ClearID.
3	Familiarize yourself with deployment best practices.	- ClearID Best practices. - Best practices for setting up ClearID for a new Synergis system. - Best practices for setting up ClearID with an existing Synergis system.
Prepare Security Center		
1	Verify that the Security Center license has a valid certificate for the plugin. Go to the Config Tool homepage, click About > Certificates, and confirm that the ClearID plugin is in the list.	- Your license information is included in the license update email that we sent you. This email includes links to the download package and other license information. - To acquire a license, see License options.
2	To manage visitors in ClearID, verify that the Synergis™ visitor management module is enabled. Go to the Config Tool homepage, click About > Synergis™, and confirm that Visitors is in the list.	- Your license information is included in the license update email that we sent you. This email includes links to the download package and other license information. - To acquire a license, see License options.
Deploy the plugin		
1	On a Security Center server, download and install the plugin.	Downloading and installing the ClearID plugin.

Genetec ClearID®; User Guide

Displayed in the header

Step	Task	Where to find more information
2	Create the plugin role. IMPORTANT: Each plugin role can only connect to or communicate with one unique ClearID system name at a time. For environments with multiple systems, you must create a plugin role for each system.	Creating the ClearID plugin role.
3	Connect Security Center to ClearID. NOTE: For environments with multiple systems, repeat these tasks for each system.	- Connecting Security Center to ClearID. - Reviewing cardholders and identities information in ClearID. - Adding a system to ClearID. - Downloading an activation file for ClearID. - Configuring connection settings for ClearID.
4	Grant users the privileges they require to use the plugin. NOTE: Security Desk operators do not need special privileges to use this plugin.	- Granting user privileges for the ClearID plugin. - Assigning privileges to users . - For a list of all available privileges, refer to the Security Center privileges spreadsheet for your version.
5	Learn about system states.	About ClearID system states.
6	Learn about identity fields.	Identity fields in ClearID.
7	Learn about custom fields.	- About custom fields in ClearID. - Modifying ClearID custom fields in Config Tool. - Custom fields relationships.
Manage identities and users		
1	Create, view, or modify your identities.	- Creating identities in ClearID. - Viewing identities in ClearID. - Modifying identities in ClearID. - Granting additional permissions for identities and roles in ClearID. - Granting additional permissions for supervisors in ClearID. - Viewing additional permissions in ClearID. - Modifying additional permissions in ClearID. - Deleting identities in ClearID
2	Grant users or administrators access to the web portal.	- Granting user access to the ClearID web portal. - Granting administrator access to the ClearID web portal.
3	View your profile.	Viewing your profile in ClearID.
4	View your site and area access.	Viewing your site and area access in ClearID.
5	Learn about and submit access requests.	- About access request workflow in ClearID. - Requesting access in ClearID.
6	Add your supervisors.	Adding supervisors manually in ClearID.
7	View and manage direct reports.	- Viewing direct reports in ClearID. - Managing direct reports in ClearID. - Transferring direct reports in ClearID.

Genetec ClearID®; User Guide

Displayed in the header

Step	Task	Where to find more information
8	Learn how to reset user passwords.	Resetting user passwords in ClearID.
9	Learn about email notifications sent by ClearID.	- About email notifications in ClearID. - Customizing the email banner for sites in ClearID.
10	Learn about delegation.	- About delegation in ClearID. - Delegating ClearID tasks to another user.
11	Understand the different user levels and what they can do.	User levels in ClearID.
12	Learn about and submit identity requests.	- About identity request workflow in ClearID. - Creating an identity template in ClearID. - Requesting identities in ClearID. - Requesting an identity in ClearID. - Requesting multiple identities using a CSV import in ClearID. - Canceling identity requests in ClearID - Approving identity requests in ClearID - About identity requests report in ClearID - Checking the status of identity requests in ClearID
Credential replication		
1	Configure credentials replication.	Configuring credential replication in ClearID
2	Review the credentials logs	Viewing credential synchronization logs in ClearID
3	Force a credentials synchronization	Forcing credential synchronization in ClearID
Manage your sites		
1	Learn about sites.	About sites in ClearID.
2	Create your sites in ClearID.	Creating sites in ClearID.
3	Enable visitor management for sites.	- Enabling visitor management for sites in ClearID. - Viewing sites where a user can invite visitors.
4	Grant users permission to access ClearID.	Granting access to the ClearID web portal.
5	Learn about access reviews.	About access reviews in ClearID.
6	Set up access reviews.	- Setting up area access reviews in ClearID. - Scheduling area access reviews in ClearID. - Setting up identity access reviews in ClearID. - Scheduling identity access reviews in ClearID.
7	Learn about access reviews report.	About access reviews report in ClearID.

Genetec ClearID®; User Guide

Displayed in the header

Step	Task	Where to find more information
8	Check the status of access reviews.	Checking the status of access reviews in ClearID.
9	Complete an access review.	- Completing an area access review (site owner) in ClearID. - Completing an area access review (area manager or role manager) in ClearID. - Completing an identity access review (supervisor) in ClearID.
10	Generate an access reviews report.	Generating an access review summary in ClearID.
11	Learn about access requests report.	About access requests report in ClearID.
12	Check the status of your access requests.	Checking the status of access requests in ClearID.
13	Learn about site activity report.	About site activity report in ClearID.
14	Learn about and manage webhook integrations.	- About webhooks in ClearID. - Creating webhooks in ClearID. - Modifying webhooks in ClearID. - Viewing webhook logs in ClearID.
Manage your areas		
1	Learn about areas.	About areas in ClearID.
2	Create your areas in ClearID.	Creating areas in ClearID.
3	Add doors to areas.	Adding doors to areas in ClearID.
4	Enable visitor management for your areas.	Enabling visitor management for areas in ClearID.
5	Learn about nested areas and access rules	- About nested areas in Security Center - Granting access to areas in Security Center automatically
6	Add your area owners and managers.	Adding area owners and managers in ClearID.
7	Add your area schedules.	Adding schedules to an area in ClearID.
8	Grant people access to an area.	Granting access to an area in ClearID.
9	Review who has access to your area.	Reviewing area access in ClearID.
10	Approve requests for access to your area.	Approving area access requests in ClearID.
11	Reject requests for access to your area.	Rejecting area access requests in ClearID.
Manage your visitors		

Genetec ClearID®; User Guide

Displayed in the header

Step	Task	Where to find more information
1	Learn about visit request workflows.	- About visit request workflow in ClearID. - About visit request watchlist workflow in ClearID.
2	Invite visitors.	- Inviting visitors in ClearID. - Inviting visitors manually in ClearID. - Inviting visitors using a CSV import in ClearID.
3	Review visit events.	Reviewing visit events in ClearID.
4	Copy a visit event.	Copying a visit event in ClearID.
5	Modify a visit event	Modifying visit events in ClearID.
6	Learn about visitors report.	About visitors report in ClearID.
7	View a visitors report.	Viewing a visitors report in ClearID.
8	Learn about QR codes as a credential for visitors.	QR codes as a credential for visitors in ClearID.
9	Import the custom card format (QR code credential).	Importing a custom card format (QR code credential) in Synergis.
10	Enable QR code credentials for visitors.	Enabling QR code credentials for visitors in ClearID.
11	Configure Qscan barcode readers for ClearID.	- Configuring Qscan devices for ClearID. - Connecting a Qscan barcode reader to a Mercury Controller for ClearID. - Configuring Qscan barcode reader to support 40-bit hexadecimal QR codes for ClearID.
12	Configure STid devices for ClearID.	- Configuring STid devices for ClearID. - About STid QR code readers in ClearID. - Creating an STid QR code reader configuration for ClearID. - Transferring your reader configuration to your STid QR code reader for ClearID.
13	Configure macro for automatic check-in and access to a parking entrance or gated facility.	Automating visitor access and check-in using a macro in Security Center.
Managing visitor watchlists		
1	Learn about watchlists.	About watchlists in ClearID.
2	Add your watchlist managers.	Adding watchlist managers in ClearID.

Genetec ClearID®; User Guide

Displayed in the header

Step	Task	Where to find more information
3	Add your watchlists.	- Adding watchlists in ClearID. - Adding an individuals watchlist entry in ClearID. - Adding a companies watchlist entry in ClearID. - Importing watchlist entries from a file in ClearID. - Exporting watchlist entries to a file in ClearID. - Testing watchlist entries in ClearID.
4	Screen your visitors manually	Screening visitors manually in ClearID.
5	Unblock visitors blocked by a watchlist.	Unblocking visitors blocked by a watchlist in ClearID.
Managing role-based access control		
1	Learn about role-based access control.	About role-based access control in ClearID.
2	Add your roles.	Adding roles in ClearID.
3	Add your role managers.	Configuring role managers in ClearID.
4	Configure your role-based access control policies.	Configuring role-based access control policies in ClearID.
5	Add custom provisioning attributes to an identity.	Adding custom provisioning attributes to an identity in ClearID.
6	Add your role members.	Adding role members in ClearID.
Connecting other systems		
1	Learn how to authenticate non-user system connections.	Authenticating your connection with ClearID.
2	Synchronize identity attributes using LDAP.	- Synchronizing identities using LDAP in ClearID. - About ClearID LDAP Synchronization Agent. - LDAP attributes to ClearID attribute mappings. - Configuring the ClearID LDAP Synchronization Agent.
3	Synchronize identity attributes using an API.	- Synchronizing identities using an API in ClearID. - About the ClearID API.
4	Synchronizing identity attributes using One Identity.	- Synchronizing identities using One Identity Synchronization Tool in ClearID. - About the ClearID One Identity Synchronization Tool. - About ClearID One Identity Synchronization Tool attribute fields. - Installing the ClearID One Identity Synchronization Tool. - Configuring the ClearID One Identity Synchronization Tool. - Reviewing synchronization status for the ClearID One Identity Synchronization Tool. - About ClearID One Identity Synchronization Tool logs. - Viewing the ClearID One Identity Synchronization Tool logs. - Updating existing identities from an external data source using ClearID One Identity Synchronization Tool.
Visitors self-service check-in		

Genetec ClearID™; User Guide

Displayed in the header

Step	Task	Where to find more information
1	Learn about Genetec ClearID™ Self-Service Kiosk.	- About ClearID Self-Service Kiosk. - About ClearID Self-Service Kiosk check-in. - About ClearID Self-Service Kiosk Self registration.
2	Learn about the different ClearID Self-Service Kiosk options that are available.	- ClearID Self-Service Kiosk options. - ClearID Self-Service Kiosk floor stand. - ClearID Self-Service Kiosk floor stand printer shelf. - ClearID Self-Service Kiosk tabletop stand.
3	Learn about the Identity Document (ID) types that the ClearID Self-Service Kiosk ID scanning function supports.	Identity document types in ClearID.
4	Configure your ClearID Self-Service Kiosk.	- Configuring the ClearID Self-Service Kiosk iPad. - Customizing the ClearID Self-Service Kiosk configuration. - Customizing the ClearID Self-Service Kiosk visitor badge logo. - Configuring the ClearID Self-Service Kiosk label printer (Brother QL-820NWBc, QL-820NWB, or QL-810W). - Configuring the ClearID Self-Service Kiosk label printer (Brother TD-4550DNWB). - Selecting a ClearID Self-Service Kiosk label printer. NOTE: The Brother TD-4550DNWB printer is no longer available for purchase through Genetec. We now support and sell the Brother QL820NWBc (CD-KIOSK-PRINTER-NA-KIT).
5	Test your visitor badge printing.	Printing a test badge from the ClearID Self-Service Kiosk.
6	Reset the ClearID Self-Service Kiosk mobile app (If required).	Resetting the ClearID Self-Service Kiosk mobile app.
Troubleshooting		
1	Learn how to troubleshoot issues that might occur.	- Plugin installed, but missing from Security Desk and Config Tool. - Plugin role could not find file with certificate. - Custom fields not displayed in Security Desk. - No active account found for user. - Visit email notifications not received by visitors. - Visitor hosts fields in Security Desk are empty. - ClearID One Identity Synchronization Tool connectivity issues. - ClearID One Identity Synchronization Tool data synchronization issues. - ClearID Self-Service Kiosk issues. - ClearID Self-Service Kiosk label printer issues. - Viewing webhook logs in ClearID.

Browse

- License options for ClearID system integration

1.8 | Supported features list for ClearID

Discover the Genetec ClearID™ supported features.

The following table lists the features that are available in ClearID.

Feature
Identity management

Genetec ClearID®; User Guide

Displayed in the header

Feature
Supervisor management of direct reports.
Transfer of direct reports
Configuration for supervisors to have elevated management permission for their direct reports. - Update profile information fields. - Update access control settings.
Identity request workflow and approval for onboarding: - One identity at a time. - Many identities at a time (CSV import).
Permissions for identities or roles to view and edit identities.
Area management
Delegate the management of controlled areas to one or more area owners.
Area owner or area manager can view, add, and remove people from Areas.
Area owner or area manager can view, add, and remove roles from Areas.
Area owner or area manager can grant temporary access to a role.
A permanent cardholder can request temporary access to an area (built-in workflow).
Actions in workflow are captured and available in the workflow history.
Area managers can approve or deny access requests.
Area managers can perform area access reviews.
Employee supervisor can be required to approve employee access request.
Email notifications when an access request is submitted.
Email notifications when an access request is approved or denied.
Role management
Delegate the management roles or cardholder group to one or more role owners.
Role managers can add or remove people from their groups.
Automatic provisioning and synchronization of cardholder groups for multiple sites
Role owners can request access to an area for their entire group.
Role managers can perform role access reviews.
Multi-site management
Global management of cardholders for multiple Synergis™ systems
Time zone support (built-in)
Automatic synchronization of permanent credentials when someone travels between sites.
Synchronization of cardholders only happens when cardholders are changed, if the cardholder has access on that Synergis system. This approach minimizes the number of cardholders synchronized to each Synergis system.
Synchronization of cardholder groups only happens when cardholder groups are changed, if the cardholder group has access on that Synergis system. This approach minimizes the amount of cardholder groups synchronized to each Synergis system.
Site owners can configure access review schedules or manually trigger access reviews.

Genetec ClearID®; User Guide

Displayed in the header

Feature
Site owners can generate an access reviews report.
Visitor management
Preregister visitors using a web portal
The visitor approval workflow can be customized based on the area selected.
Automatic provisioning of visitors with the required areas automatically assigned
Visitor check-in using Security Desk
Paper badges and temporary credentials - Paper badges are typically used for large volumes of visitors who require temporary access, for example: - Hosting a conference or trade show for business partners. - To identify people visiting an area, temporary visitor badges can also be stuck on visitors' clothing. - Security or reception issue temporary credentials after visitors check-in. These temporary credentials are returned to security or reception when leaving the <i>site</i> or <i>area</i>.
Visitor escort with multiple visitor hosts
Email notifications when a visitor is approved.
Capture and report the visit reason. Security staff can use the visit reason information to help track who enters or exits a building and the reason for the visit.
Email invitation sent to visitor with a meeting invite, site details, and optional file attachments
Send SMS notifications to the host when a visitor checks in. These SMS notifications can be sent to any valid phone number.
Send email notifications to the watchlist manager when visitor details match a person of interest or company of interest on an individuals or companies block or notify watchlist.
Visitor entry is blocked when visitor details match a person of interest or company of interest on an individuals or companies block watchlist.
Configurable Genetec ClearID™ Self-Service Kiosk options. For example, customizing the welcome screen QR code, ID, check-in, check-out, and self-registration option combinations that are displayed.
Configurable options to capture extra visitor information during the creation process for a visit event. For example, delivery ID, vehicle, passenger name, ID number, or license plate.
Configurable automatic visitor check-out (grace period).
Reports
Reports including CSV downloads (where applicable). Workflow request reports: - Access requests report - Access reviews report - Visitors report Audit trail reports: - Role activity report - Site activity report - Site and area owners report - User activity report
Platform
Corporate logo for Portal and email notifications

Feature
Cloud platform ClearID is a cloud service. A dedicated server is not required. However, a communications connection to the Synergis servers is required. This connection is provided by the ClearID plugin.
HTML5 web interface with mobile support Users can use their mobile devices to navigate the ClearID portal.
REST API available to automate any functions available in the Web portal. • Create or edit an identity in the system. • Disable access for a person. • Add a person to a role. • Remove a person from a role. • Create a visitor event. • Acknowledge an access request.
Synchronize identity using Microsoft SQL Server.
Synchronize identity from custom source using Identity REST API.
Security and authentication
Support multi-factor authentications for users using OpenID connect
Single sign-on using Microsoft Office 365
Single sign-on using Microsoft Entra ID
ISO 27001 certification For more information, see Cybersecurity resources.
AES-256 encryption with RSA Personal data managed by ClearID is always encrypted.

Browse

- [Genetec Compliance Portal](#)

1.9 | Supported languages in ClearID

Genetec ClearID™ is available in the following languages.

ClearID web portal

- English
- French
- Spanish
- Dutch
- German
- Italian
- Portugese
- Japanese

NOTE: The language that is displayed in the web portal user interface is determined by your web browser language settings.

ClearID plugin

- English

Genetec ClearID™ One Identity Synchronization Tool

- English

Genetec ClearID™ LDAP Synchronization Agent

- English

Genetec ClearID™ Self-Service Kiosk mobile app

- English
- French
- Spanish
- Dutch
- German
- Italian
- Portuguese
- Japanese

Documentation

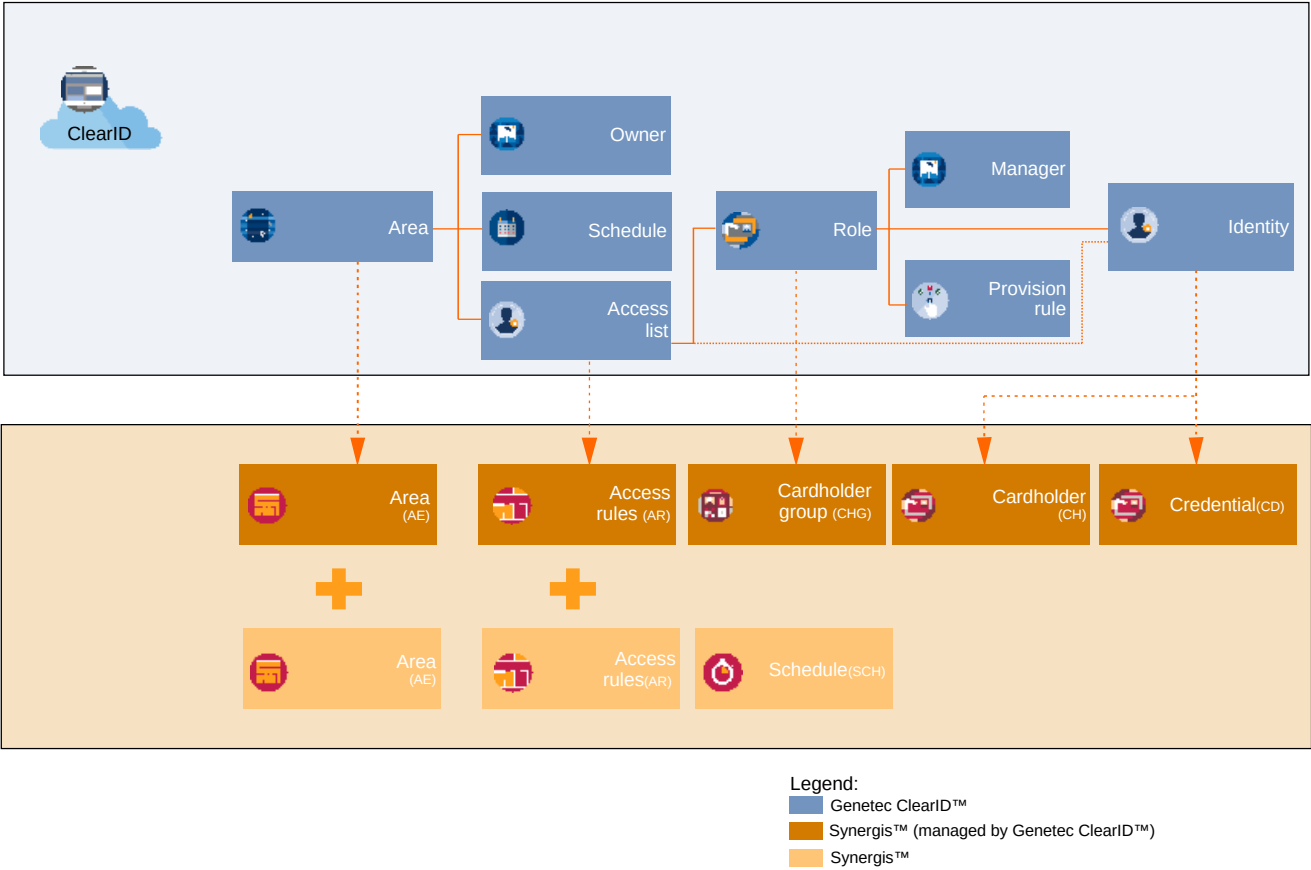
- [ClearID User Guide \(English\)](#)
- [ClearID User Guide \(French\)](#)
- [ClearID User Guide \(Spanish\)](#)

IMPORTANT: Translation of documentation is ongoing. Documentation in languages other than English might not be complete at the time of release.

1.10 | ClearID terminology

Genetec ClearID™ uses specific terms. Here are the definitions of some common terms and their equivalents in Security Center.

The following diagram shows ClearID terms and their equivalents in Security Center:



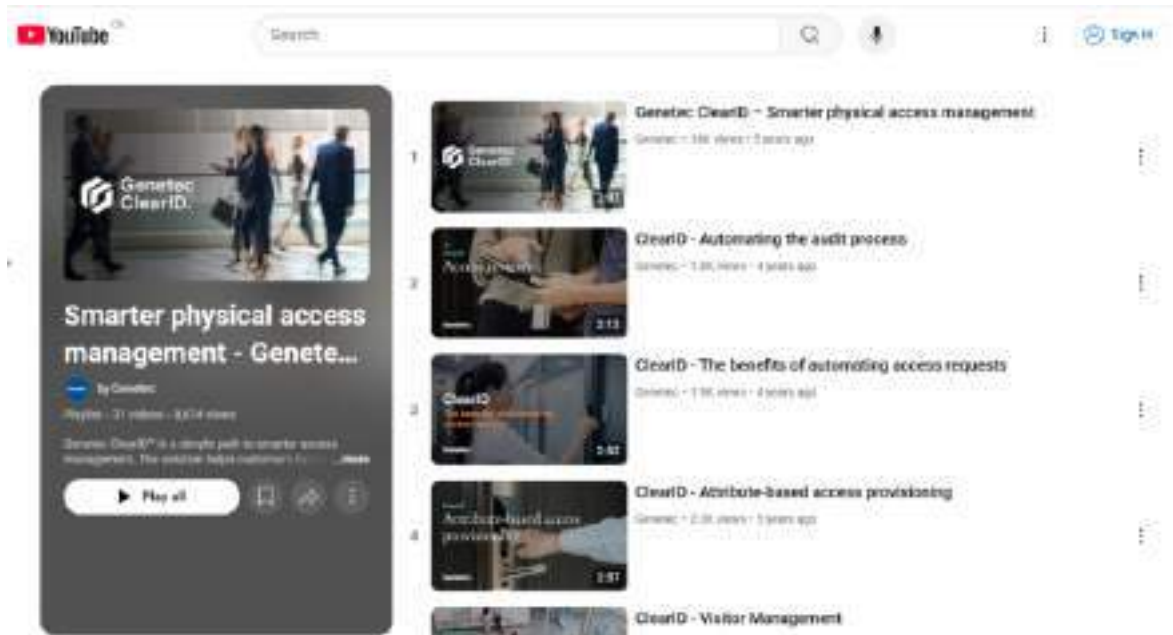
The following table lists ClearID terms and their equivalents in Security Center:

ClearID	Security Center
Identity	Cardholder
Area	Area

ClearID	Security Center
Role	Cardholder group
Schedule (defined in Security Center) and access list (defined in ClearID)	Access rules

1.11 | ClearID videos

Use the Genetec ClearID™ videos to help you learn about key features and understand the product. You can access all the videos in one place, the [ClearID videos playlist](#).



Click the image to access the ClearID videos playlist.

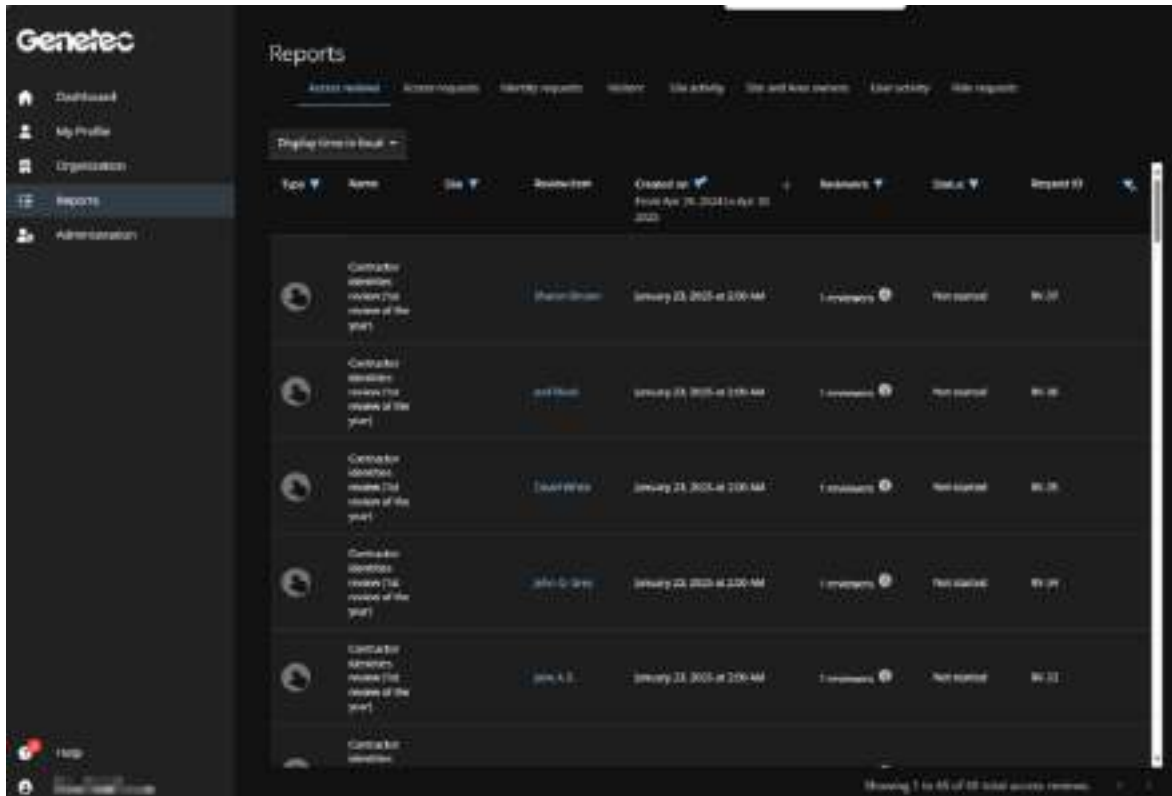
Videos can also be launched individually from relevant topics or the documentation homepage.

Browse

- [What is ClearID?](#)

1.12 | About reports in ClearID

Genetec ClearID™ provides several reports to manage your site and various activities. The reports can help you understand the status of access requests, access reviews, and current or upcoming visit events. Reports can also be used to review audit trail information about roles, sites, site and area owners, and users.



You can use the following reports to check the status of the following:

- Access reviews report
- Access requests report
- Identity requests report
- Direct reports report
- Site and area owners report
- Visitors report

You can use the following reports to review audit trail information about the following:

- Role activity report
- Site activity report
- User activity report

1.13 | Logging on to ClearID

Log on to your Genetec ClearID™ account to submit visitor or access requests.

Before you begin

- Enable cookies in the web browser that you are using
- If you are not using a corporate Active Directory system, activate your ClearID account by clicking the activation link in your email.

Procedure

1. In your web browser, enter or select the required host as detailed in your account activation email.

For example:

- United States: <https://portal.clearid.io/>
- Australia: <https://portal.au.clearid.io/>
- Canada: <https://portal.ca.clearid.io/>
- Europe: <https://portal.eu.clearid.io/>

NOTE: If a corporate log on (single sign-on using Microsoft Office 365 or similar) is used, the account is automatically activated and no activation email is received.

2. On the logon page, enter your *username* and click Logon.

You are redirected to your user account's logon page.

3. (Optional) Select an account.

- The account ID is shown in the URL of every page.

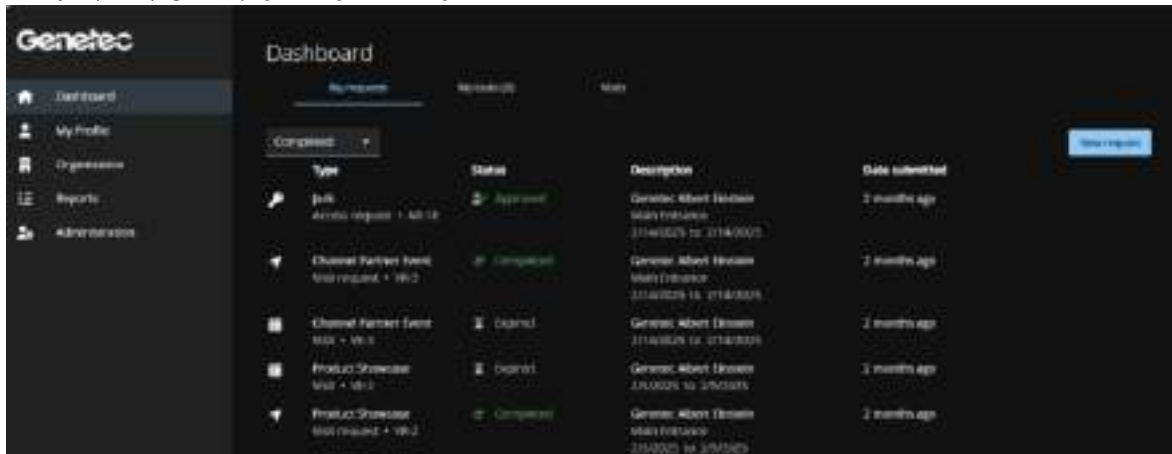
For example, <https://hostname/accountid/currentpage>.

- The account ID can change depending on the user account that is logged on.

Tip: If you have more than one account, you can switch accounts at any time by clicking Change account from the account options under the user ID.

Results

The My requests page is displayed and you are ready to use ClearID.



Browse

- Creating identities in ClearID
- Authenticating your connection with ClearID

1.14 | Logging off from ClearID

To exit from Genetec ClearID™, you can log off from your user account.

What you should know

You are logged off from the system automatically after a specified period of inactivity. The inactivity period varies depending on your environment configuration. The default is 30 minutes.

Procedure

At the top of the page, click your name, and then click Log off.

Tip: After you log off from of your account, close all browser windows that were used for ClearID.

1.15 | Enabling preview features in ClearID

When available, users can enable one or more preview features in Genetec ClearID™ to get early access to evaluate new functions before they are released.

Before you begin

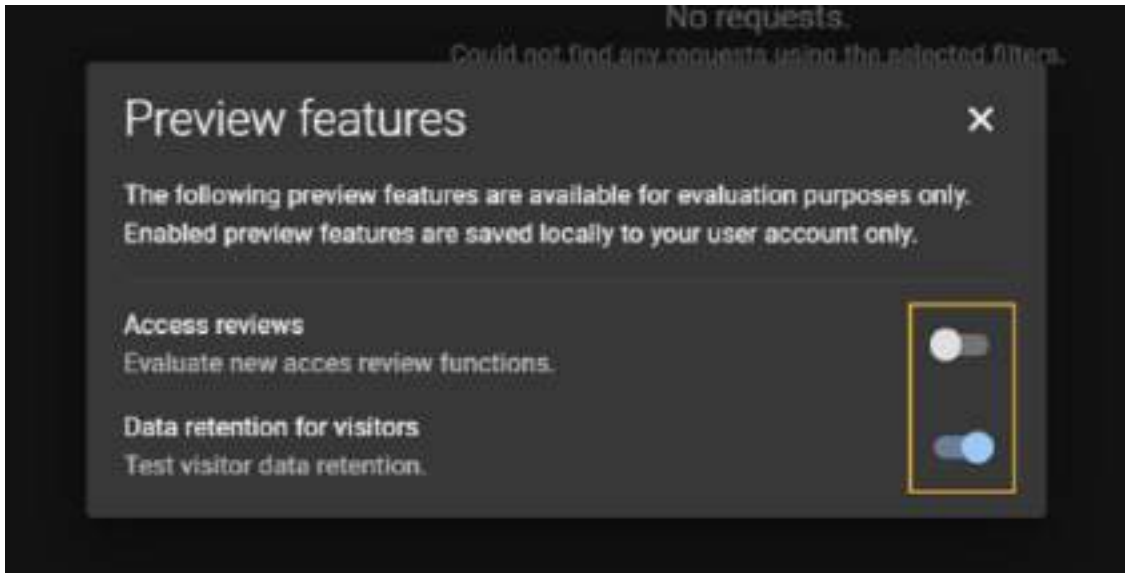
The Preview features function must be enabled for your organization.

What you should know

- Preview features are for evaluation purposes only.
- Enabled preview features are saved locally to your user account only.

Procedure

1. In the ClearID web portal, click your user name.
2. Click Preview features.
3. In the Preview features dialog, use the preview features slider controls to enable the features you want to evaluate.



4. Click  to close the dialog.

1.16 | Disabling preview features in ClearID

Users can disable one or more preview features in Genetec ClearID™ if they no longer want to use or see the new preview features.

Before you begin

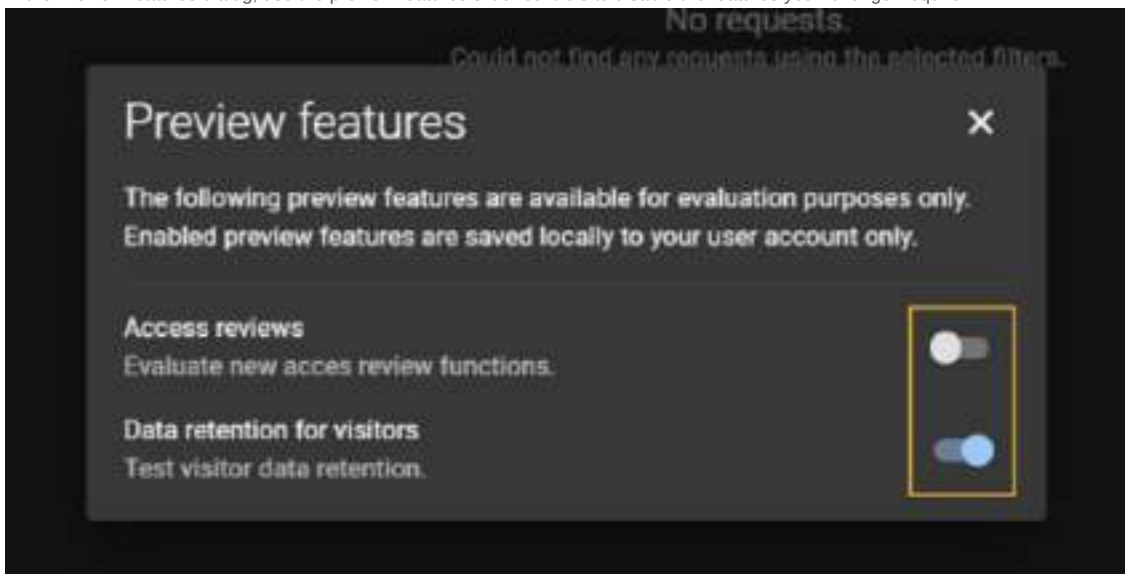
The Preview features function must be enabled for your organization.

What you should know

- Preview features are for evaluation purposes only.
- Enabled preview features are saved locally to your user account only.

Procedure

1. In the ClearID web portal, click your user name.
2. Click Preview features.
3. In the Preview features dialog, use the preview features slider controls to disable the features you no longer require.



4. Click  to close the dialog.

1.17 | Customizing portal branding in ClearID

As an account administrator, you can customize the Genetec ClearID™ portal logo and accent color to align with your company's branding.

Before you begin

You must be an *Account administrator* to customize the ClearID portal branding.

What you should know

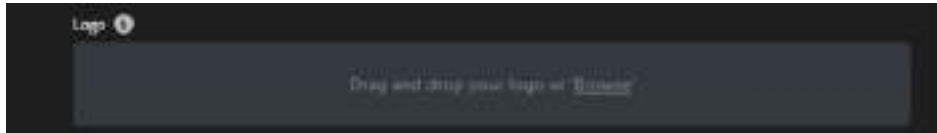
- You can set different branding options for light and dark themes in ClearID.

Procedure

- In the ClearID web portal, click Administration > Account configuration.
- In the Branding section, choose either light theme or dark theme.
 - Select the logo and accent color.

Logo

Click Browse or drag and drop an image from your file browser to upload your logo. The image must have a resolution within the range of 20x20 and 2000x500 pixels.



Accent color

Use the color picker to select a color and adjust the opacity, or type the hexadecimal code of the color in the Accent color field.



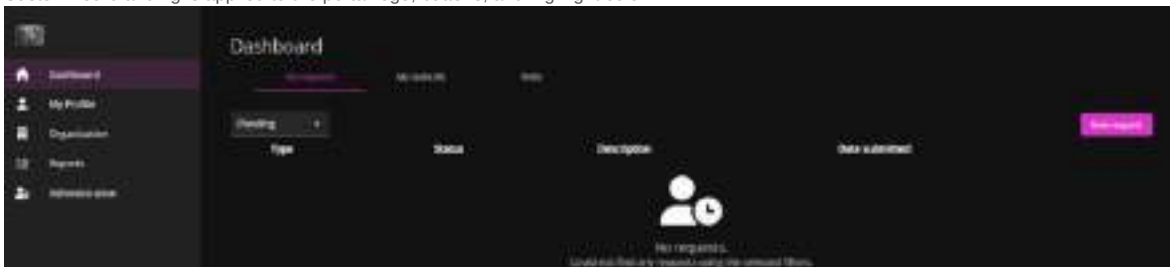
(Optional)

Click Restore default theme to restore the portal branding to default.

- Click Save.
- (Optional) Repeat steps 2 - 3 for other themes as required.

Example

Customized branding is applied to the portal logo, buttons, and highlight color.



1.18 | Customizing help menu links in ClearID

As an *Account administrator*, you can customize the Genetec ClearID™ Help menu links, directing portal users to your company's support resources and pages.

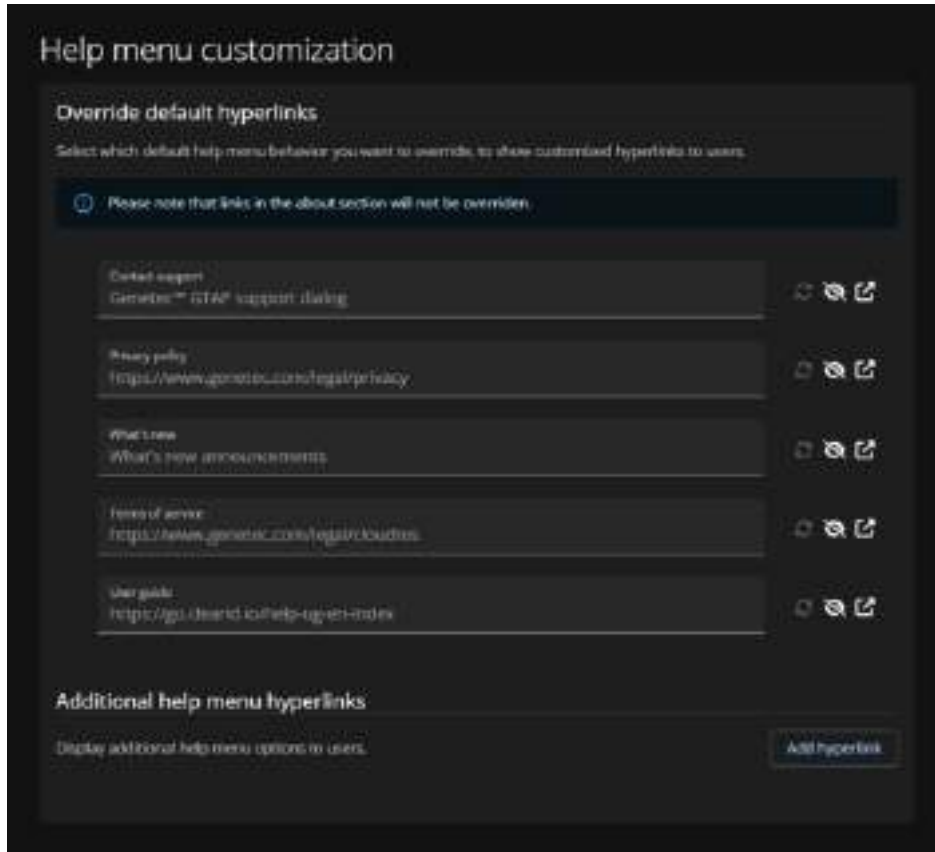
Before you begin

You must be an *Account administrator* to customize the links in the ClearID Help menu.

Procedure

1. In the ClearID web portal, click Administration > Account configuration.
2. In the Override default hyperlinks section, modify the default Help menu links.

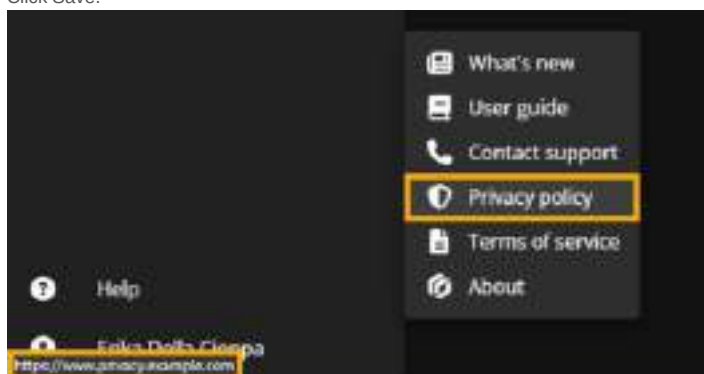
NOTE: You can't override the About link.



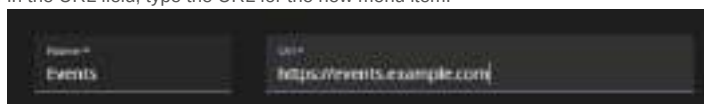
- a. Select the Help menu item you want to modify.
- b. Type the URL you want the user to be directed to under the selected header.



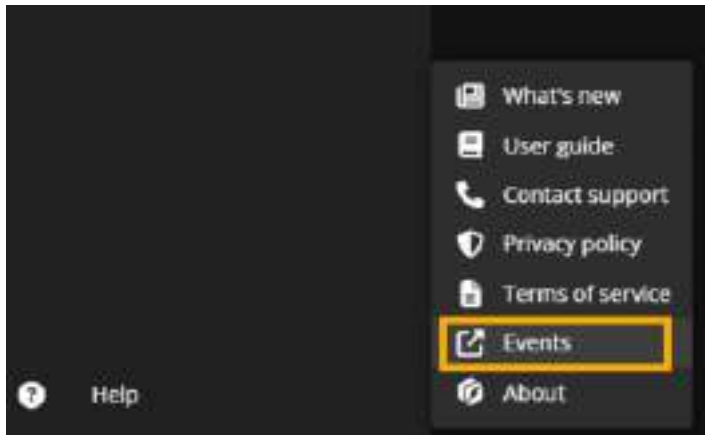
- c. Click Save.



3. (Optional) In the Additional help menu hyperlinks subsection, add more links to the menu.
 - a. Click Add hyperlink to add a new menu item.
 - b. In the Name field, type a name for your new menu item.
 - c. In the URL field, type the URL for the new menu item.



- d. Click Save.
The new link is added to the menu below the default portal links.



4. (Optional) Use the icons beside each link to reset, hide, or view menu items.

- Click Revert to default (🔄) to revert the customized link to the portal default.
- Click Hide (🔒) to hide the link from the menu.
- Click Show (🔓) to show a previously hidden link.
- Click Go to URL (🔗) to go to the linked page.
- Click Delete (🗑️) to delete the custom link.

2 | What's new

2.1 | What's new in ClearID

Check out what's new in the latest update to Genetec ClearID™.

What's New: July 2025

Updated part numbers

Genetec™ has updated and simplified ClearID part numbers to support changes in pricing for ClearID systems. There are now fewer part numbers required to build your system.

For more information, see [License options for ClearID system integration](#) and [ClearID Self-Service Kiosk options](#).

Create custom identity fields

As an *Account administrator*, you can now create and manage custom fields for identities directly in the ClearID web portal. With custom identity fields, you can store extra information like vehicle profiles, employee types, worker schedules, and more for all identities.



For more information, see [About custom identity fields in ClearID](#) and [Creating custom identity fields in ClearID](#).

Skip access request approval workflow

You can now exclude users and roles from the access request approval workflow for an area. For example, you can decide to bypass the workflow and automatically approve access requests for people who belong to a specific role, like Upper Management.

For more information, see [Creating exceptions to the access request approval workflow in ClearID](#).

Save visitor photos

You can now save photos of visitors taken during check-in to the Genetec ClearID™ web portal. You can access saved photos for incident management and auditing purposes by going to [Reports > Visitors](#).

For more information, see [Activating visitor photo retention in ClearID](#).

For a complete list of all prior announcements, see [Previous features and enhancements](#).

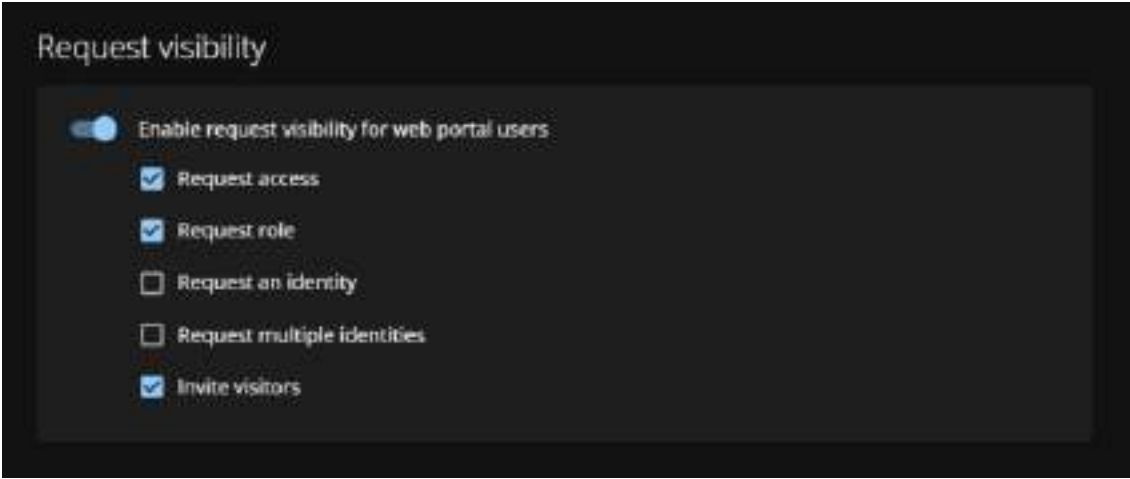
2.2 | Previous features and enhancements in ClearID

The Genetec ClearID™ solution includes the following features and enhancements.

What's New: June 2025

Change visible request types

As an *Account administrator*, you can configure permitted request types for users, limiting the types of requests users can make in the ClearID web portal.

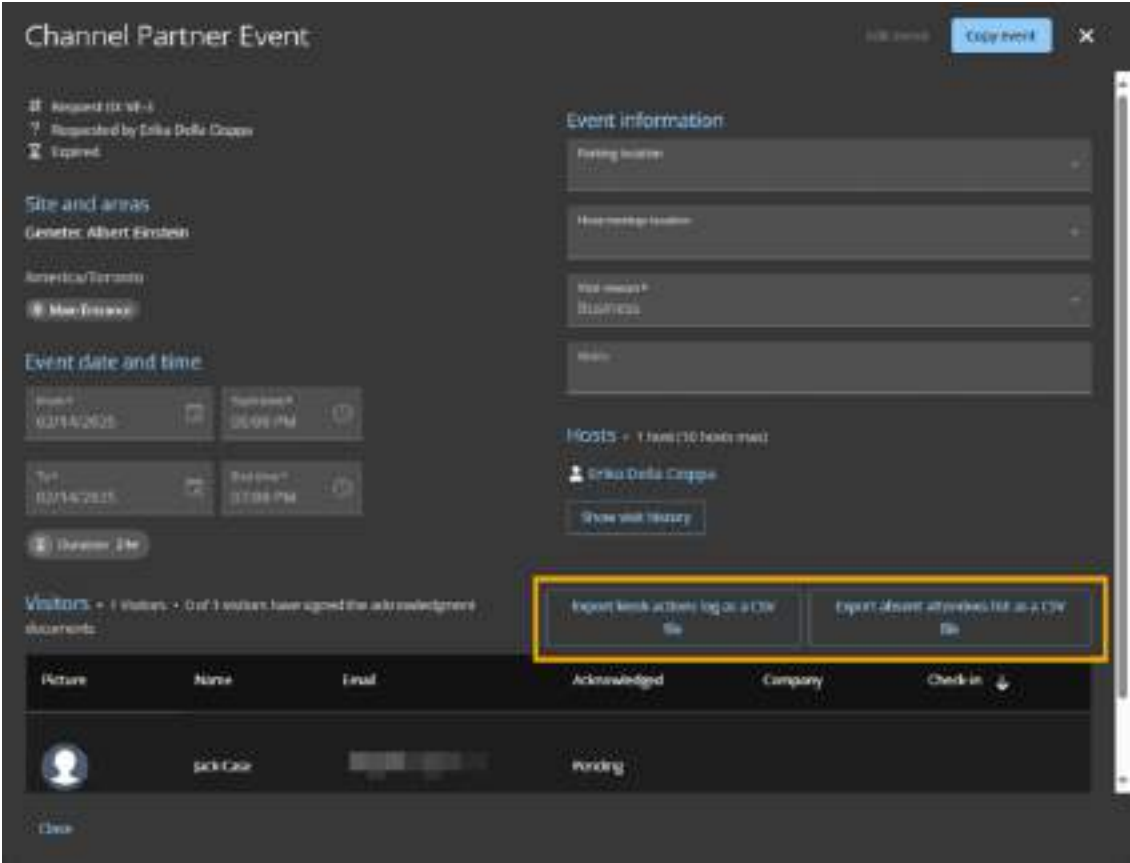


For more information, see [Setting request visibility for users in ClearID](#).

What's New: May 2025

Visit event logs

Account administrators, *Site owners*, and *hosts* can track operator and visitor actions on check-in devices and export lists of invited visitors who didn't check in.



For more information, see [About visit event logs in ClearID](#) and [Viewing visit event logs in ClearID](#).

Account-level notification preferences

Account administrators can manage the default email notification preferences for all ClearID portal users and decide which stakeholders receive notifications. You can also configure whether users can opt out of certain email notifications in their personal email notification preferences.



For more information, see [Configuring email notification preferences in ClearID \(administrator\)](#).

Add visit events to your calendar

Hosts and guests can now keep track of events by adding visits to their digital calendars using the ICS files attached to visit confirmation emails.

For more information, see [Adding ClearID visit events to your calendar](#).

What's New: January 2025

Check visitors in using ClearID mobile operator check-in

Previously, visitors could only check in to events using the Self-Service Kiosk iPad. Now, receptionists, security guards, and attendants at hosted events can quickly check visitors in using the ClearID Self Service Kiosk app on an iPhone. Mobile operator check-in uses the iPhone to scan QR codes and look up visit information.

For more information, see [About ClearID mobile operator check-in](#) and [Configuring ClearID mobile operator check-in](#).

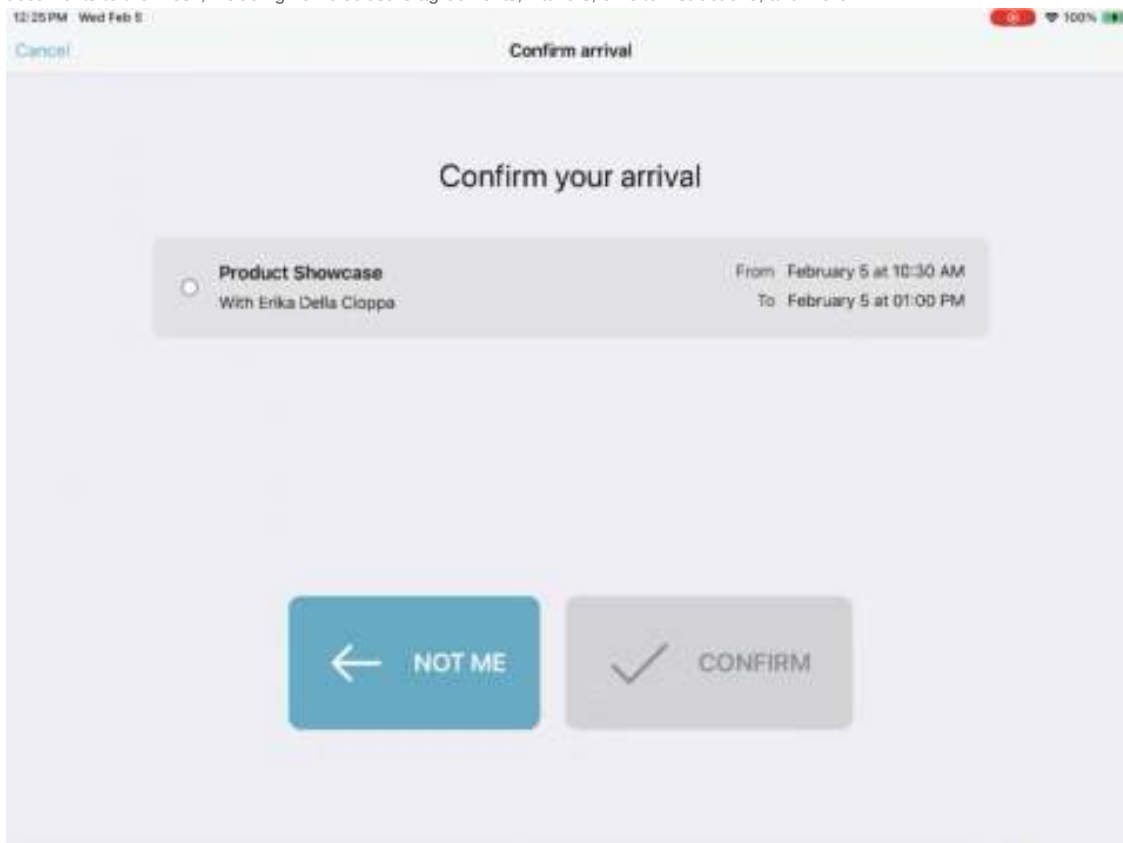
Make informed decisions when granting employees access

You can now specify that employees upload supporting documents when submitting access requests for secure areas where specialized certifications are required to gain access. *Site owners* and *Area approvers* can review submitted documents to ensure that employees requiring access comply with industry regulations and company policies before granting them access.

For more information, see [Configuring access request documents for sites in ClearID](#) and [Configuring access request documents for areas in ClearID](#).

Ensure visitors comply with site requirements

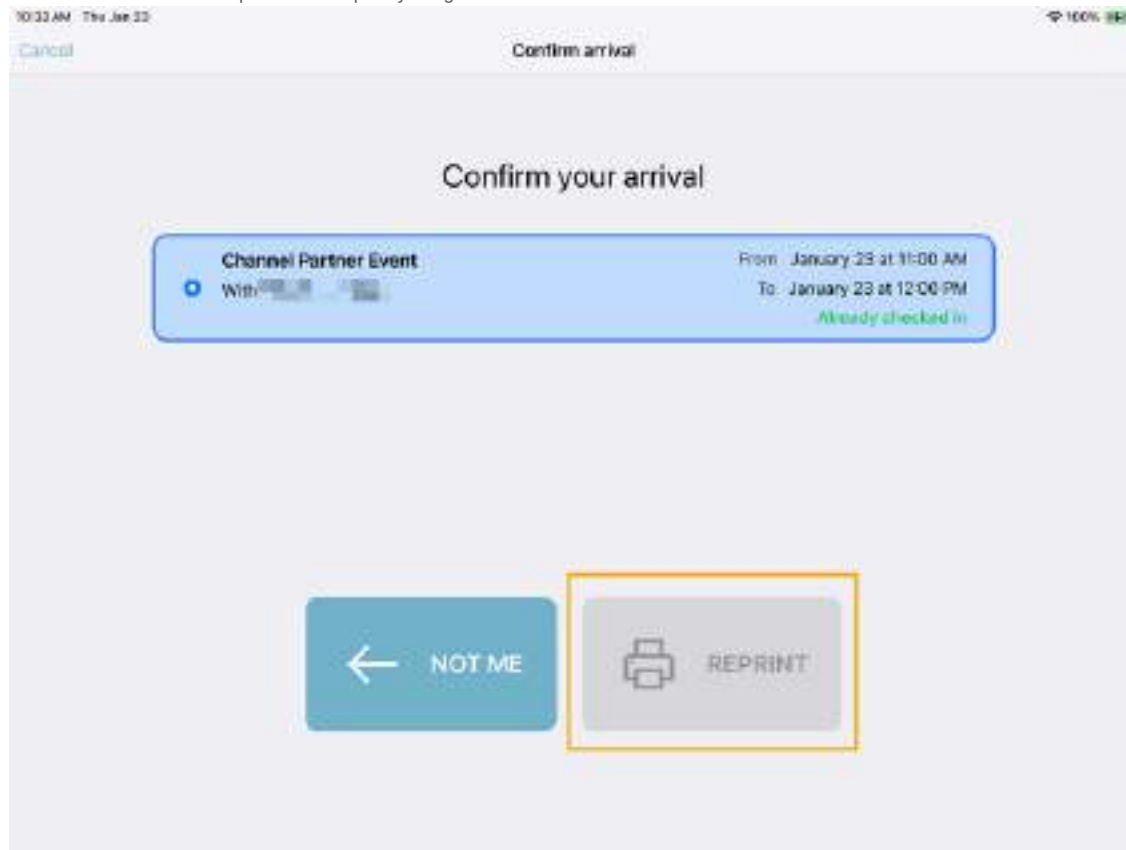
You can now specify that visitors read and sign required compliance documents during a Self-Service Kiosk check-in. *Account administrators* can add up to five documents to the Kiosk, including non-disclosure agreements, waivers, on-site instructions, and more.



For more information, see [Adding PDF acknowledgment documents to the Self-Service Kiosk](#).

Visitors can reprint badges

Visitors can now reprint lost or damaged badges directly from the Self-Service Kiosk. As a *Site owner*, you can activate the Re-print badge option so that visitors can return to the Kiosk to reprint their temporary badge.



For more information, see [Activating badge reprints](#).

Protect visitor privacy

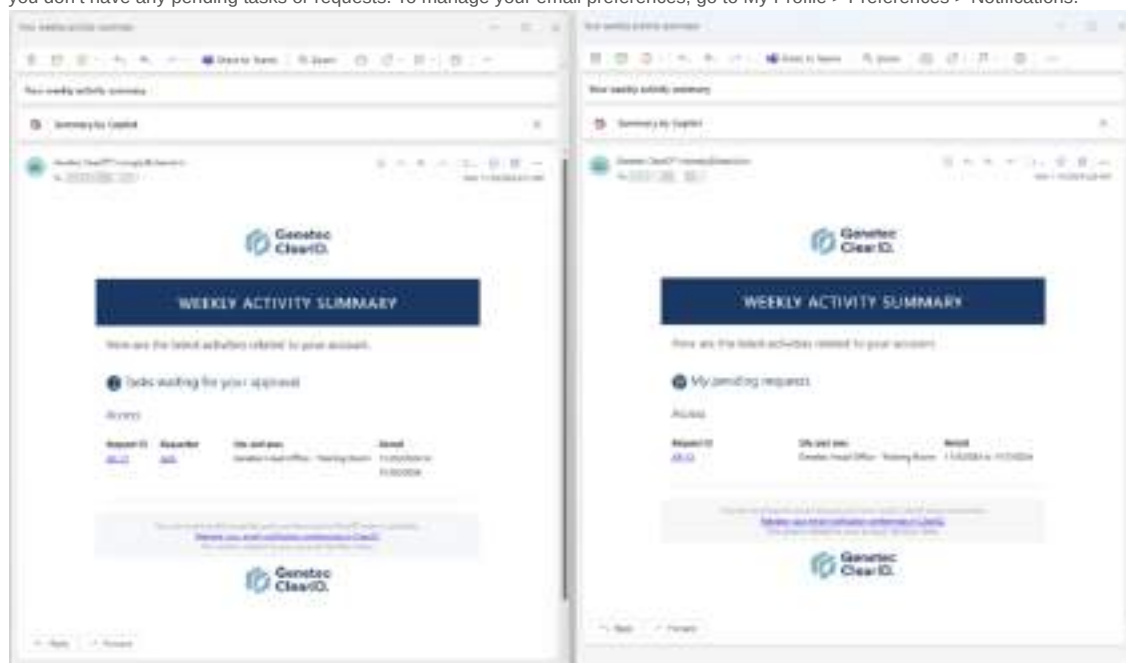
Site owners can now deactivate photo-taking during visitor check-in at the Self-Service Kiosk.

For more information, see [Disabling visitor photo during check-in](#).

What's New: December 2024

Keep track of your pending tasks

You can now receive Weekly Activity Summary emails every Monday detailing pending tasks or requests that require approval. You won't receive these emails if you don't have any pending tasks or requests. To manage your email preferences, go to [My Profile > Preferences > Notifications](#).



For more information, see [About email notifications](#) and [Configuring your email notification preferences](#).

What's New: October 2024

Synchronize ClearID identity pictures with Security Center

Account administrators can now set ClearID as the preferred data source for all cardholder pictures in Security Center. You can activate identity picture synchronization to automatically replace cardholder pictures in Security Center with ClearID identity pictures.

NOTE: ClearID identity pictures have a maximum size of 5 megabytes.

For more information, see [Synchronizing identity pictures with Security Center](#).

Personalize notification email header and footer text

Account administrators and *Site owners* can now customize the header and footer text of email notifications. Use the custom text fields to communicate information to visitors such as equipment or documentation requirements for their visit or steps to complete before arrival.



For more information, see [Customizing email notifications for sites in ClearID](#).

ClearID Self-Service Kiosk mobile app version 2.2 is now available

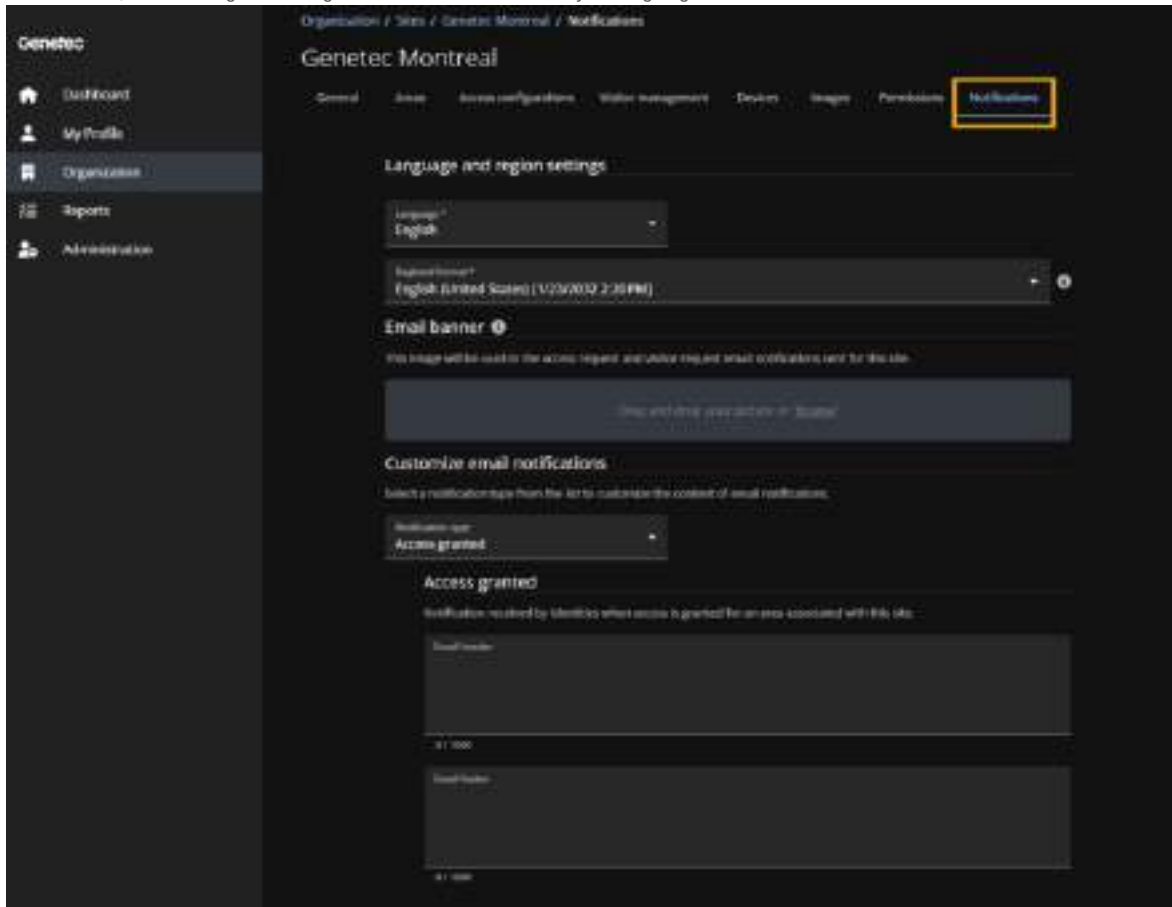
The latest update includes bug fixes and improved diagnostics for visit events. Core functionality of the kiosk remains the same.

To download the ClearID Self-Service Kiosk mobile app, visit the [App Store](#).

IMPORTANT: User interface changes

Language and region settings and notification settings have moved

Previously language and region settings and notification settings were configured by *Account administrators* or *Site owners* by clicking Organization > Sites > General. Now, these settings are configured in the Notifications tab by clicking Organization > Sites > Notifications.



For more information, see [Creating sites in ClearID](#) and [Modifying sites in ClearID](#).

What's New: September 2024

Cardholder credential synchronization

ClearID accounts connecting to multiple Security Center systems now have a new configuration setting. Administrators can now specify the Security Center system that is the source of credentials synchronized to other systems. This option makes credential synchronization automatic and predictable and can give employees access to multiple sites with a single access card.

For more information, see [Configuring credential replication in ClearID](#).

Simplified identity management

You can now use the System for Cross-domain Identity Management (SCIM) integration to synchronize system attributes from an external data source into ClearID. These identity attributes can then be used in ClearID to assign people to roles and automate role-based access control.

For more information, see [Synchronizing identities using the SCIM integration](#).

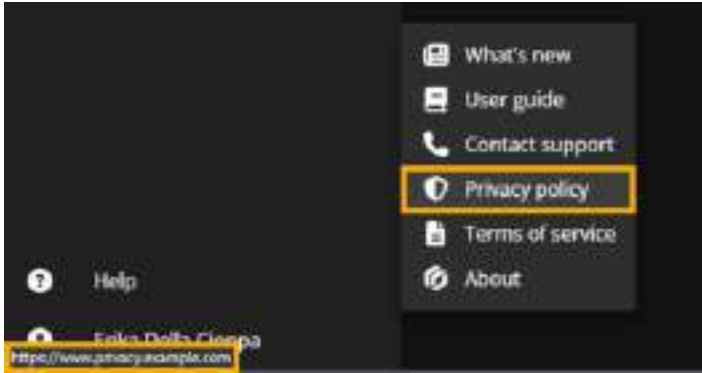
ClearID Self-Service Kiosk mobile app version 2.1.2 is now available

The latest update includes performance and scalability improvements, bug fixes, and some minor changes to the user interface. Core functionality of the kiosk remains the same.

To download the ClearID Self-Service Kiosk mobile app, visit the [App Store](#).

Help menu link customization

Account administrators can now customize the ClearID Help menu links, directing portal users to your company's support pages and resources.

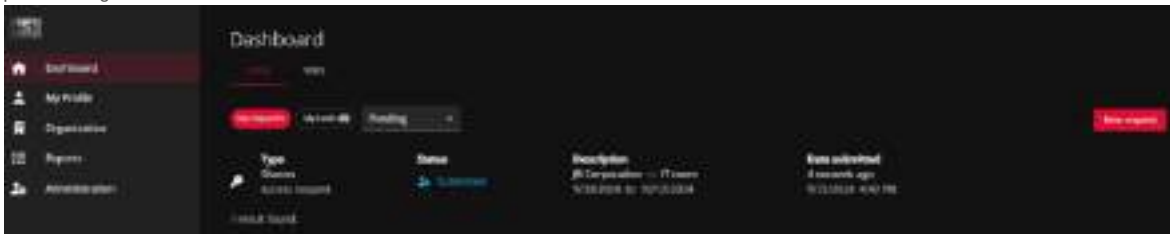


For more information, see [Customizing help menu links](#).

What's New: June 2024

Portal branding customization

Account administrators can now customize the ClearID portal logo and accent color to align with your company's branding. Portal users can choose to view the portal in a light or dark theme.



For more information, see [Customizing portal branding in ClearID](#).

Geo-specific data centers

You can now store your data in a region that applies to the geographical location of your system or where you want data stored. You can choose between more regional data center options to meet regulatory requirements or other geo-specific data storage needs.

Canadian data centers

All data is stored in data centers located within Canada.

- Primary data center: Azure Central Canada (Ontario)
- Secondary data center: Azure East Canada (Quebec)

Australian data centers

All data is stored in data centers located within Australia.

- Primary data center: Azure East Australia (New South Wales)
- Secondary data center: Azure Central Australia (Canberra)

For more information, see [About ClearID architecture](#).

User activity report

Account administrators can now review activity related to identities and supervisors in the User activity report. It's now possible to filter results in the Activity type column to display activities for these action types:

- Supervisor added or removed
- Identity created, updated, or deleted

For more information, see [About user activity report](#) and [Viewing a user activity report](#).

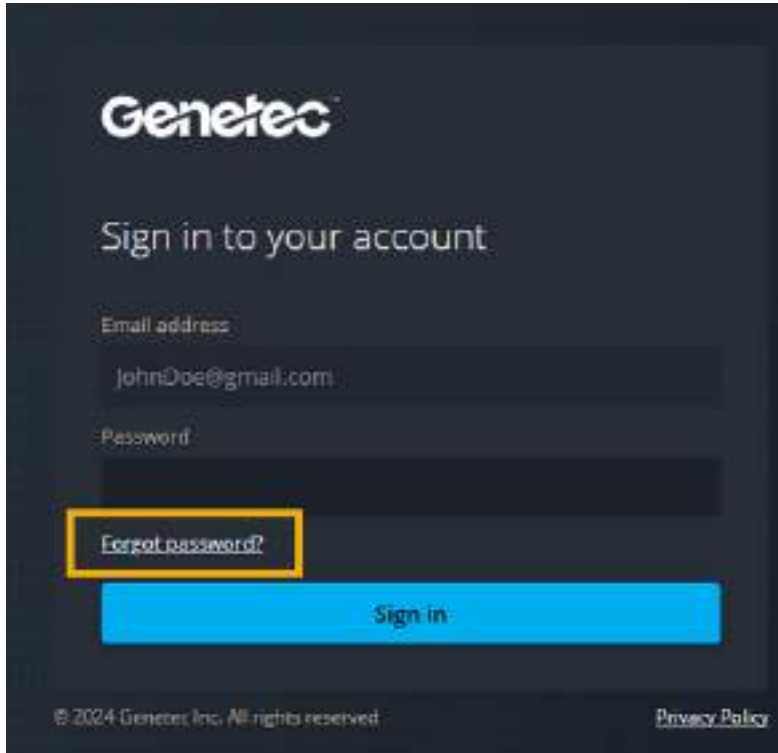
What's New: April 2024

Updates to the ClearID sign in system

An update has been made to the ClearID sign in system that might affect your organization. Users who don't use a single sign-on (SSO) integration might need to reset their passwords the first time they sign in to ClearID. As part of the transition:

- Multifactor authentication (MFA) is mandatory for all users that sign into Genetec™ applications.
- A code is sent to the email address associated with the user's account to act as a second factor for authentication.

NOTE: This change doesn't affect users in organizations that integrate their corporate identity system with ClearID. These users can continue to use the SSO functionality that their organization provides.



For more information, see [Resetting user passwords](#).

What's New: February 2024

Tracking entities managed by ClearID in Synergis™

You can now track entities managed by ClearID in Config Tool and Security Desk. These entities are highlighted with a blue dot in the bottom-right corner of the entity icon. For example:

Access rules ()

For more information, see [How the ClearID plugin works with Security Center](#).

Zebra DS 9300 QR code scanner support

ClearID now supports the Zebra DS 9300 QR code scanner.

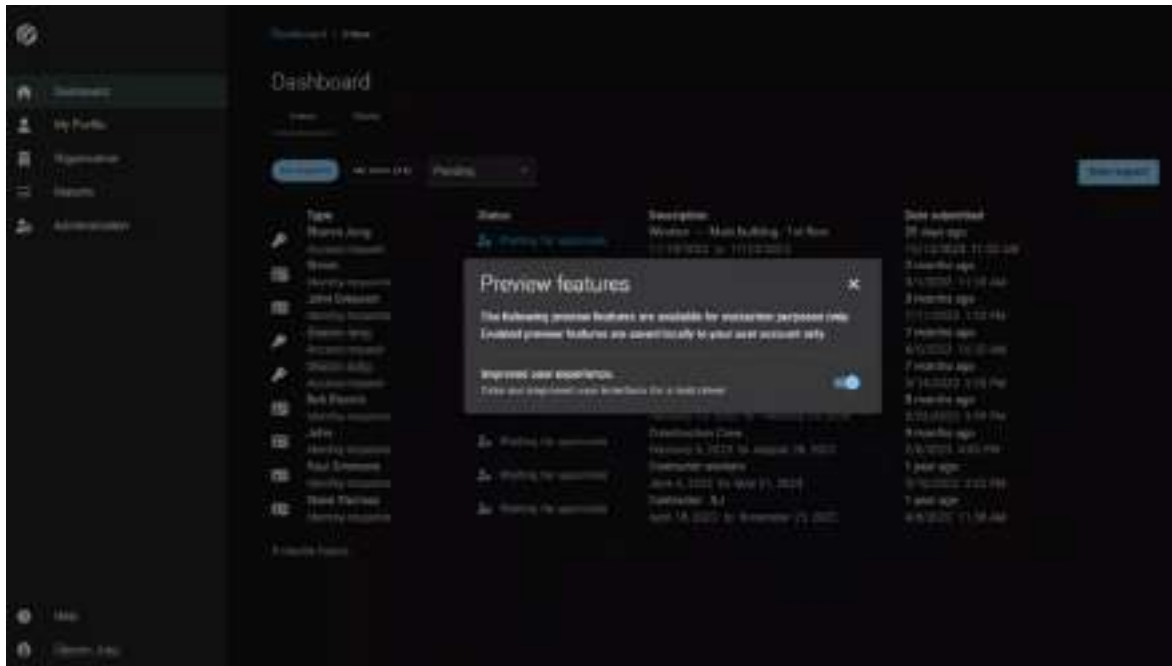


For more information, see [Supported devices for ClearID](#), [Enabling visitor management for sites in ClearID](#), or refer to the manufacturer documentation.

What's New: December 2023

Preview features

ClearID now includes a preview features option. Users can enable one or more preview features (when available) to get early access to new functions before they are released.

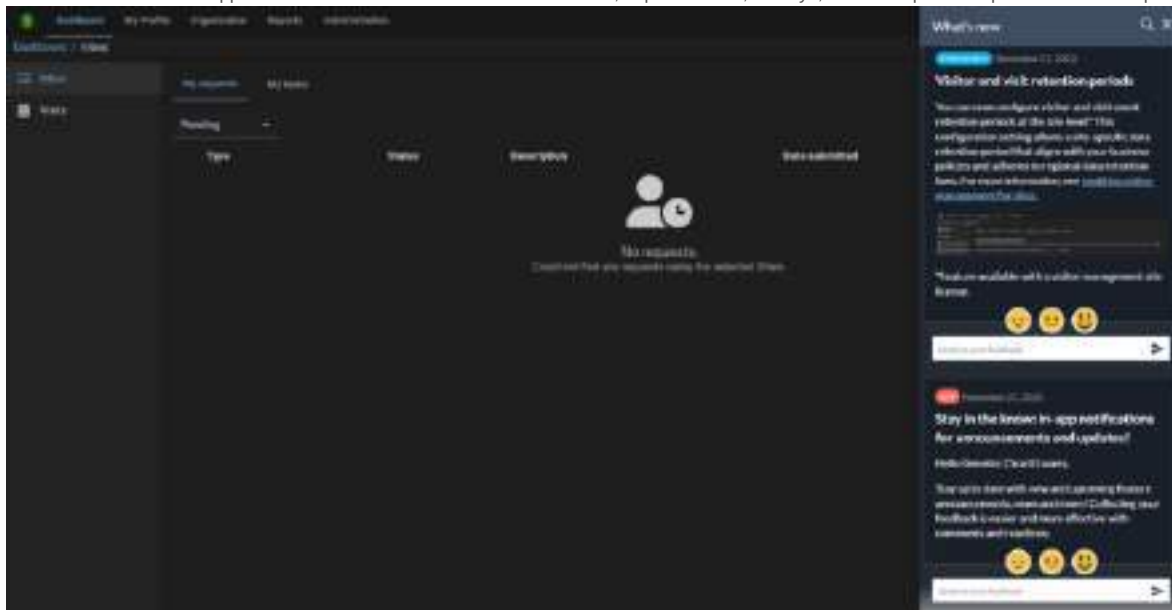


NOTE: Preview features are for evaluation purposes only. Enabled preview features are saved locally to your user account only.

For more information, see [Enabling preview features in ClearID](#) and [Disabling preview features in ClearID](#).

In-app notifications

ClearID now includes in-app notifications for new feature announcements, improvements, surveys, and other product updates in the web portal.



Stay up to date with new and upcoming feature announcements, news, and more. Collecting your feedback is now even easier. You can submit emoji reactions or send feedback for each announcement or notification directly to the product team.

ClearID architecture update

Identity data processing has changed.

For more information about which data centers are used in the Global deployment, see the *Microsoft Corporation* entry in the ClearID section of the [Genetec Subprocessors](#) list.

Genetec ClearID™ Self-Service Kiosk 1.13.9

ClearID Self-Service Kiosk mobile app version 1.13.9 is now available.

This maintenance update includes the following:

- Performance improvements
- iOS 17.1.1 compatibility update

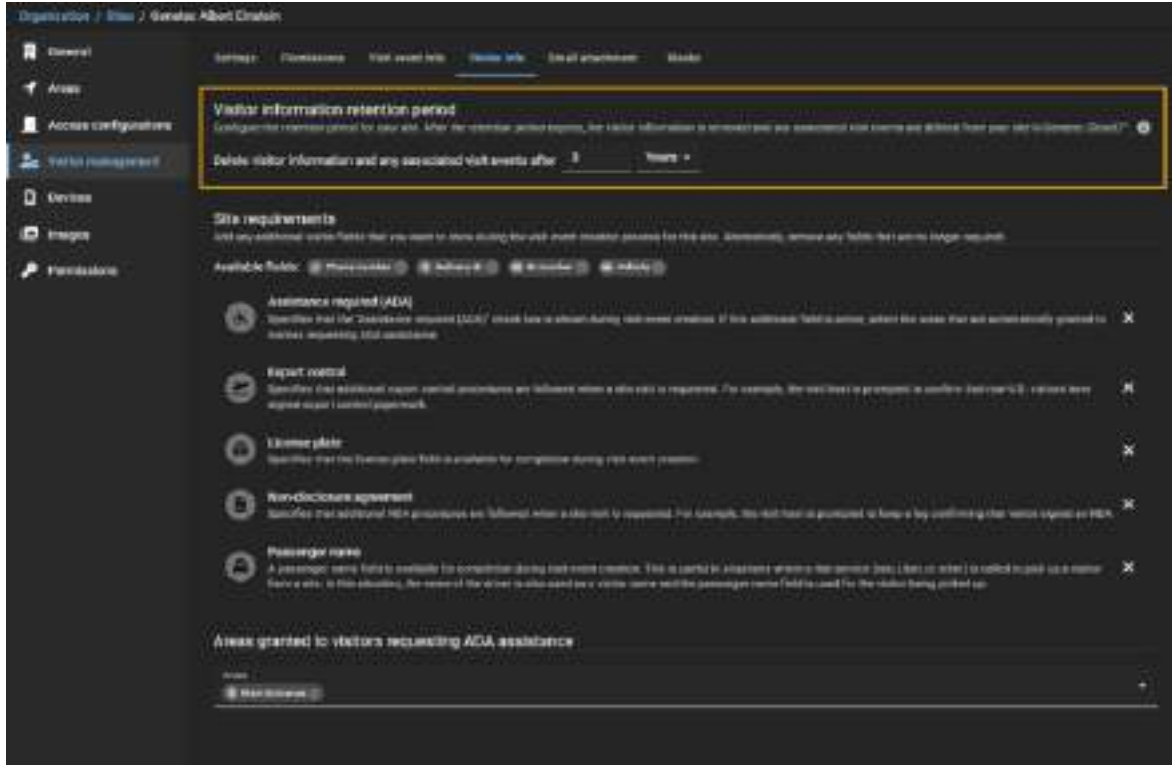
To download the ClearID Self-Service Kiosk mobile app, visit the [App Store](#).

What's New: November 2023

Data retention for visitors

You can now configure a retention period for visitor information. After the retention period expires, the visitor information is removed and any associated visit events are deleted from your site in ClearID.

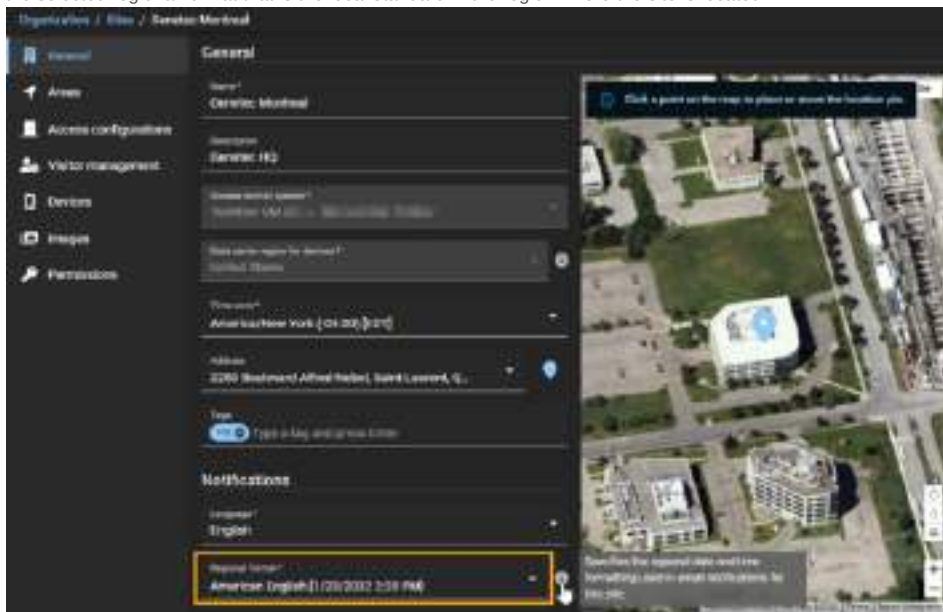
NOTE: The retention period is configurable by site to comply with the different data laws that might apply in your region.



For more information, see [Enabling visitor management for sites in ClearID](#).

Email notifications

You can now configure your email notifications to specify a Regional format that is relevant for your sites. The email notifications display the date and time using the selected regional format that is the local standard in the region where the site is located.

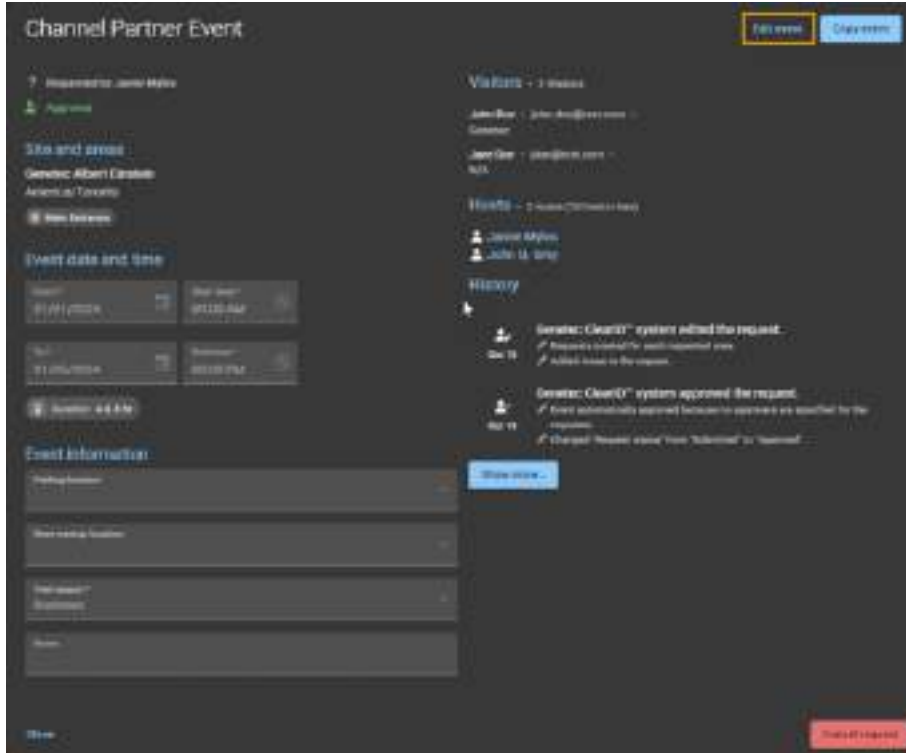


For more information, see [Creating sites in ClearID](#) and [Modifying sites in ClearID](#).

Updating scheduled visit events

You can now modify visit events to change the event details, or to add or remove visitors or hosts. Updating the visit event details ensures that your visitors are always kept up to date following any changes to an upcoming event.

NOTE: Events can only be modified before the start of the visit event.



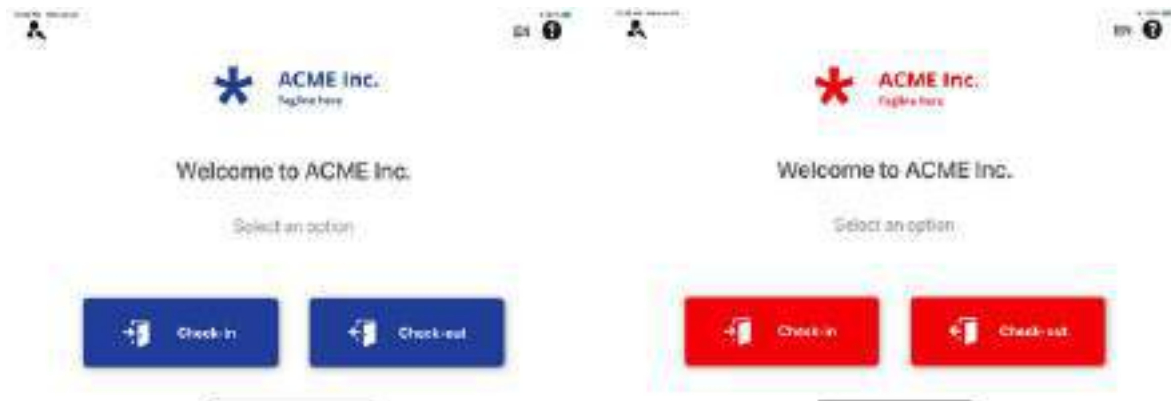
For more information, see [Modifying visit events in ClearID](#).

What's New: October 2023

Kiosk customization

The Genetec ClearID™ Self-Service Kiosk has been enhanced to include kiosk theme customization.

The following examples show the white kiosk theme with an accent color.



You can choose a white kiosk theme. When you choose the white kiosk theme, you can also choose one of ten accent colors. Alternatively you can enter a specific HEX color code value to align with your corporate branding.



For more information, see [Customizing the ClearID Self-Service Kiosk configuration](#) or [Enabling visitor management for sites in ClearID](#).

Genetec ClearID Self-Service Kiosk 1.13.8

ClearID Self-Service Kiosk mobile app version 1.13.8 is now available.

The Kiosk mobile app now supports the following:

- Kiosk Theme customization
- Translation updates for check-in, check-out, and welcome screen or assistance messages.

For more information, see [Customizing the ClearID Self-Service Kiosk configuration](#) or [Enabling visitor management for sites in ClearID](#).

To download the Genetec ClearID™ Self-Service Kiosk mobile app, visit the [App Store](#).

What's New: August 2023

Reports

ClearID now includes two more reports for audit trail and activity tracking purposes:

Identity requests report

Account administrators can now use the Identity requests report to review all activities related to identity requests.

Request date	Requested by	Name	Identity template	Status	Reviewers
From Aug 23, 2023 to Aug 23, 2023			Template A		
February 2, 2023 at 9:07 AM	Supervisor1	Anna Smith	Template A	Completed 0 - 0 - 1	1 reviewers
November 22, 2022 at 8:18 AM	Supervisor1	Charlie Brown	Template	Completed 0 - 0 - 1	1 reviewers
November 11, 2022 at 8:03 AM	Contractor Manager	Deborah S	Template	Completed 0 - 0 - 1	1 reviewers

Showing 1 to 3 of 3 total identity requests.

For more information, see [About reports in ClearID](#), [About identity requests report in ClearID](#), and [Checking the status of identity requests in ClearID](#).

Direct reports report

Supervisors or account administrators can now use the Direct reports report to check their direct reports access control status and general identity information.

Name	Job title	Company	Access control status
John Doe	IT Engineering	Service	Active
Charlie	Engineering	Service	Active
John Doe	Information Technology	Self	Active
Jane Smith	IT Support / Network	Service	Active
John Doe			Active reports as of 8/23/2023
John Doe	Research Scientist (Computer)	Spiky Spiky Chemical	Active reports as of 8/23/2023
John	Marketing Specialist	Service	Active

For more information, see [About reports in ClearID](#), [About direct reports report in ClearID](#), and [Viewing direct reports in ClearID](#).

Kiosk kit update

The ClearID Self-Service Kiosk kits now include and support the 10th generation 10.9 inch Apple iPad.

For more information, see [ClearID Self-Service Kiosk options](#) and [Supported devices for ClearID](#).

What's New: July 2023

One Identity Synchronization Tool

The Genetec ClearID™ One Identity Synchronization Tool has been updated to simplify synchronization and also to resolve the End of Life (EOL) of the Microsoft Azure AD Graph.

IMPORTANT: The Microsoft Graph library replaces the now End of Life (EOL) Azure Active Directory Graph library (EOL since June 30, 2023 - [Azure AD Graph API end of life](#)). The new library supports all previous mappings.

Who is affected? ClearID customers who are using Azure AD as the data source to synchronize their identities in ClearID with the One Identity Synchronization Tool.

For more information, see the official documentation from Microsoft: [Migrate your apps from Azure AD Graph to Microsoft Graph](#).

Next steps? Get in touch with your ClearID team deployment contact to upgrade the One Identity Synchronization Tool.

NOTE: If you are not using Azure AD as a data source, these events do not affect you and you do not require an upgrade.

For more information about the synchronization tool, see [Synchronizing identities using One Identity Synchronization Tool in ClearID](#).

For more information about Azure AD API permissions, see [About the Azure web app for ClearID One Identity Synchronization Tool](#).

What's New: June 2023

Genetec ClearID Self-Service Kiosk 1.13.7

ClearID Self-Service Kiosk mobile app version 1.13.7 is now available.

The Kiosk mobile app now supports the following:

- Brother QL-820NWBc label printer
- iOS 16
- 135 new or updated Identity Document (ID) types

For more information, see [Supported devices for ClearID](#), [ClearID Self-Service Kiosk options](#), [Configuring the ClearID Self-Service Kiosk label printer \(Brother QL-820NWBc, QL-820NWB, or QL-810W\)](#), and [Identity document types in ClearID](#).

To download the Genetec ClearID™ Self-Service Kiosk mobile app, visit the [App Store](#).

What's New: May 2023

Custom fields updates

ClearID custom fields information has been updated to help you understand the relationship between ClearID identity field names and Security Center entity type fields.

The screenshot displays the 'Custom Fields' configuration interface. The left sidebar contains navigation options: Events, Actions, Logical ID, User account settings, Activity tasks, Audio, Visual tools, Included Loggings, Features, Updates, and Maintenance - mobile features. The main area is titled 'Custom Fields' and contains a table of field configurations.

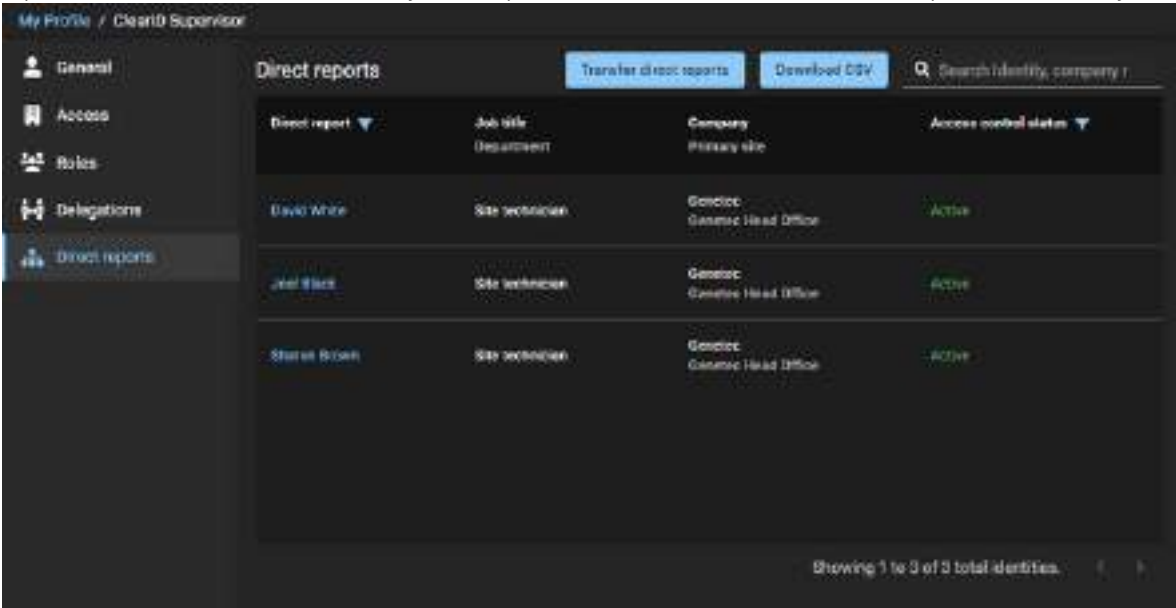
Field Name	Data Type	Default Value	Group Name / Priority	Mandatory	Maximal to attach	Indexed	Theme
Company	Text		Company (0)				Cardboard
Company Name	Text		Company (0)				White
Company Email	Text		Company (0)				Cardboard
Company Type	Dropdown (external type) (external type)	Unknown	Company (0)				Cardboard
Department	Text		Company (0)				Cardboard
Employee Number	Text		Company (0)				Cardboard
Signed Name	Text/Free	1/1/2004 0:00:00 PM	Company (0)				White
Signed Signature	Text/Free	1/1/2004 0:00:00 PM	Company (0)				White
Signed Control	Text		Company (0)				White
Internal ID	Text		Company (0)				Cardboard
Home Site	Text		Company (0)				Cardboard
User Home Address	Text		Company (0)				White
Identity ID	Text		Company (0)				Cardboard
Identity Management Index	Dropdown (Management) (User Center) Type	Maximum 64	Company (0)				Cardboard
Job Title	Text		Company (0)				Cardboard
Working Location	Text		Company (0)				White
Mobile Phone	Text		Company (0)				Cardboard
Mail (Business Agreement)	Text		Company (0)				White
Role	Text		Company (0)				White
Working Location	Text		Company (0)				White
Phone Number	Text		Company (0)				Cardboard
Residential Code	Text		Company (0)				White
Secondary Email	Text		Company (0)				Cardboard
Site ID	Text		Company (0)				White
Site Name	Text		Company (0)				White
Supervisor	Text		Company (0)				Cardboard

For more information, see [About custom fields in ClearID](#), [Modifying ClearID custom fields in Config Tool](#), and [Custom fields relationships](#).

What's New: March 2023

Transfer direct reports

Supervisors, account administrators, or an identity with write permissions for identities can now transfer direct reports to another identity.



IMPORTANT: This function is intended for identities that are locally managed in ClearID. If identities are managed using an external data source, the transfer of direct reports will be overwritten.
For more information, see [Transferring direct reports](#).

Synergis™ licensing changes

Synergis licensing has changed. For Security Center 5.11 or later (Synergis Base Enterprise or Synergis Base Professional) the Synergis visitor management module is now included by default.
NOTE: The Synergis visitor management module is required if the ClearID customer has the CD-SITE-VM-1Y ClearID license.
For more information, see [License options for ClearID system integration](#).

What's New: February 2023

Genetec ClearID Self-Service Kiosk 1.13.6

Genetec ClearID Self-Service Kiosk mobile app version 1.13.6 is now available.
The Genetec ClearID Self-Service Kiosk mobile app version 1.13.6 now supports the following:

- Brother TD-4550DNWB thermal printer (with pre-cut labels).

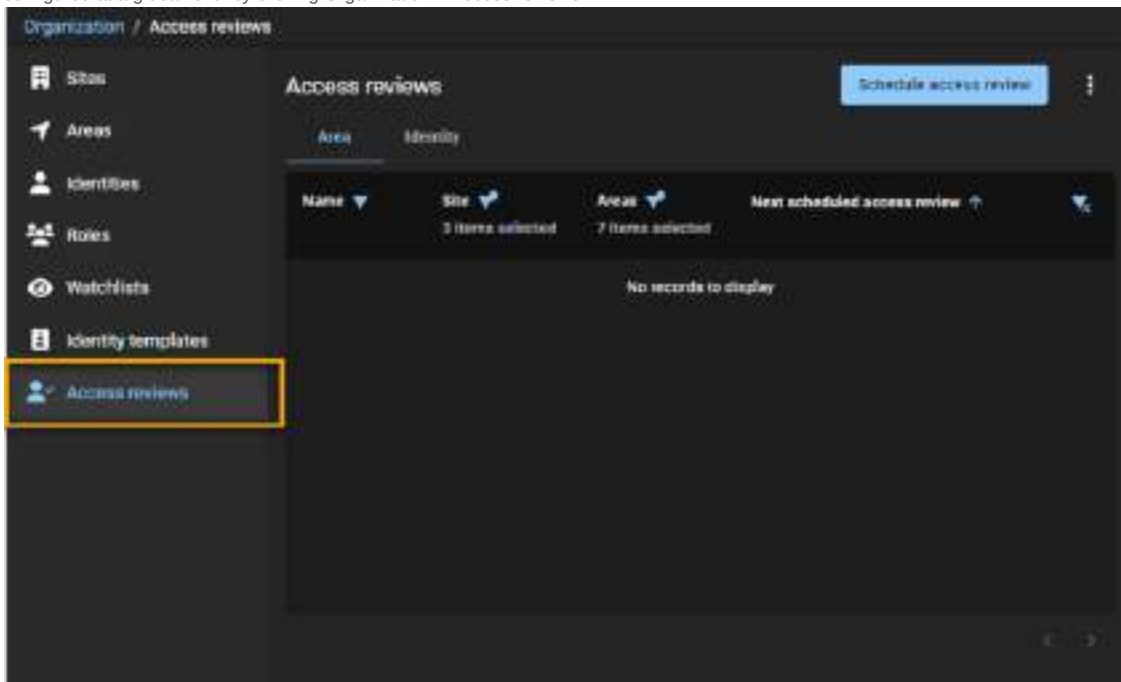
For more information, see [Supported devices for ClearID](#), [ClearID Self-Service Kiosk options](#), and [Configuring the ClearID Self-Service Kiosk label printer \(Brother TD-4550DNWB\)](#).

To download the Genetec ClearID™ Self-Service Kiosk mobile app, visit the [App Store](#).

IMPORTANT: User interface changes

Access reviews have moved

Previously access reviews were created and scheduled at a site level by clicking Organization > Sites > Access reviews. Access reviews settings are now configured at a global level by clicking Organization > Access reviews.

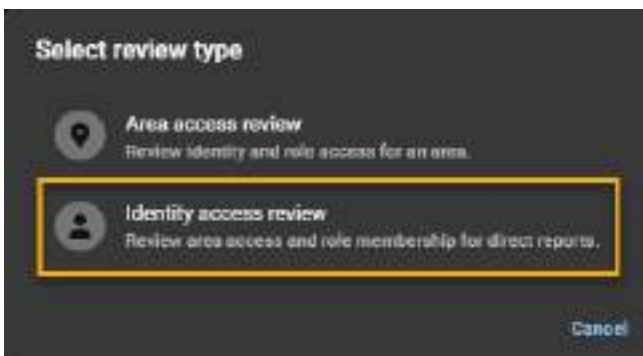


Access reviews enhancements

Access reviews

Access reviews now include a new Identity access review option.

An identity access review is the process where a supervisor reviews their direct reports access. This review includes confirming or updating area access, access control date range, or role membership for their direct reports to ensure security compliance and audit readiness.

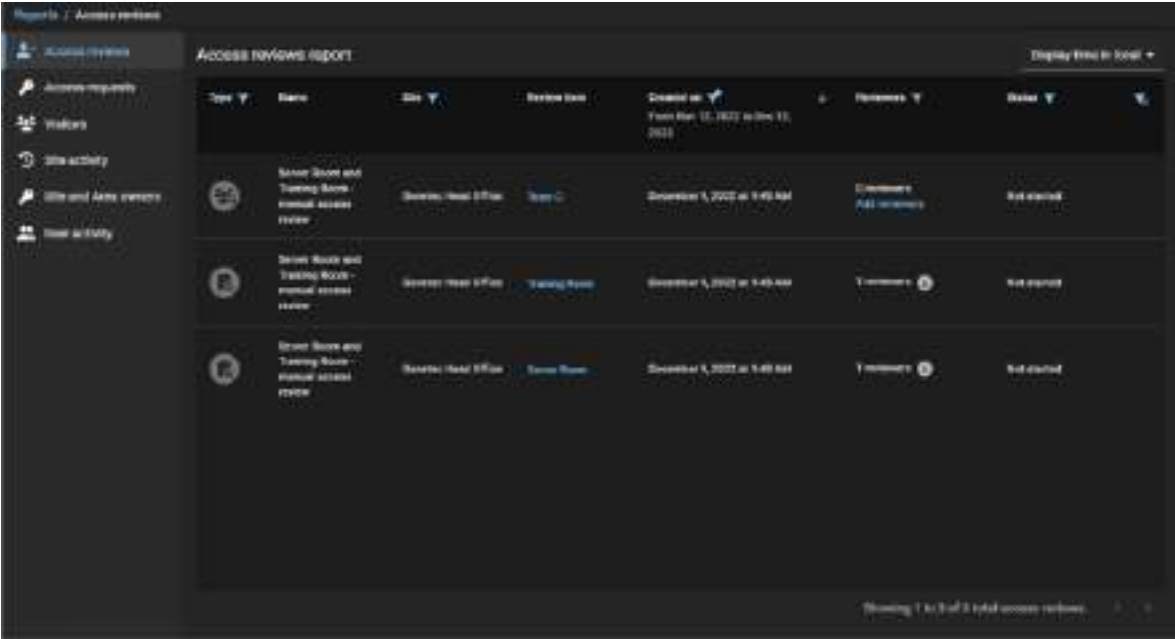


Access reviews also include updates to the Site access review schedule dialog.

For more information, see [Setting up area access reviews in ClearID](#) and [Setting up identity access reviews in ClearID](#).

Access reviews report updates

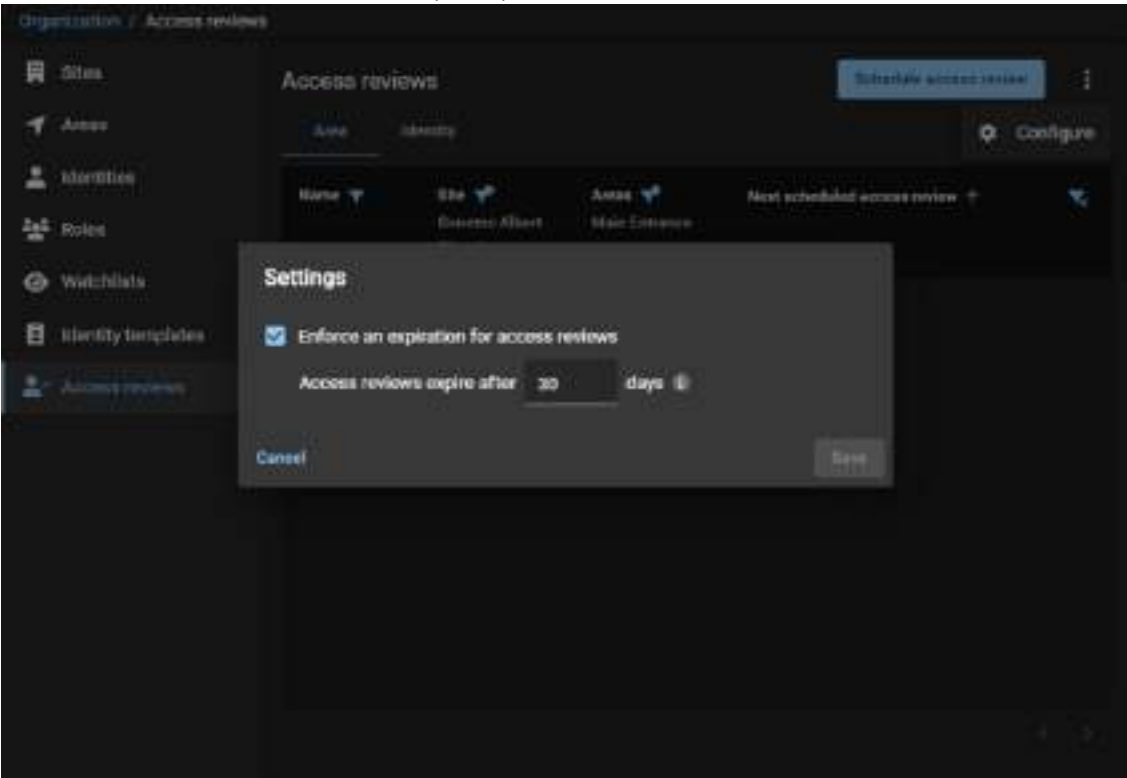
Access reviews report now includes updates to report data and filtering.



For more information, see [About access reviews report in ClearID](#) and [Checking the status of access reviews in ClearID](#).

Automatic expiration for access reviews

Account administrators can now set an automatic expiration period for all access reviews.



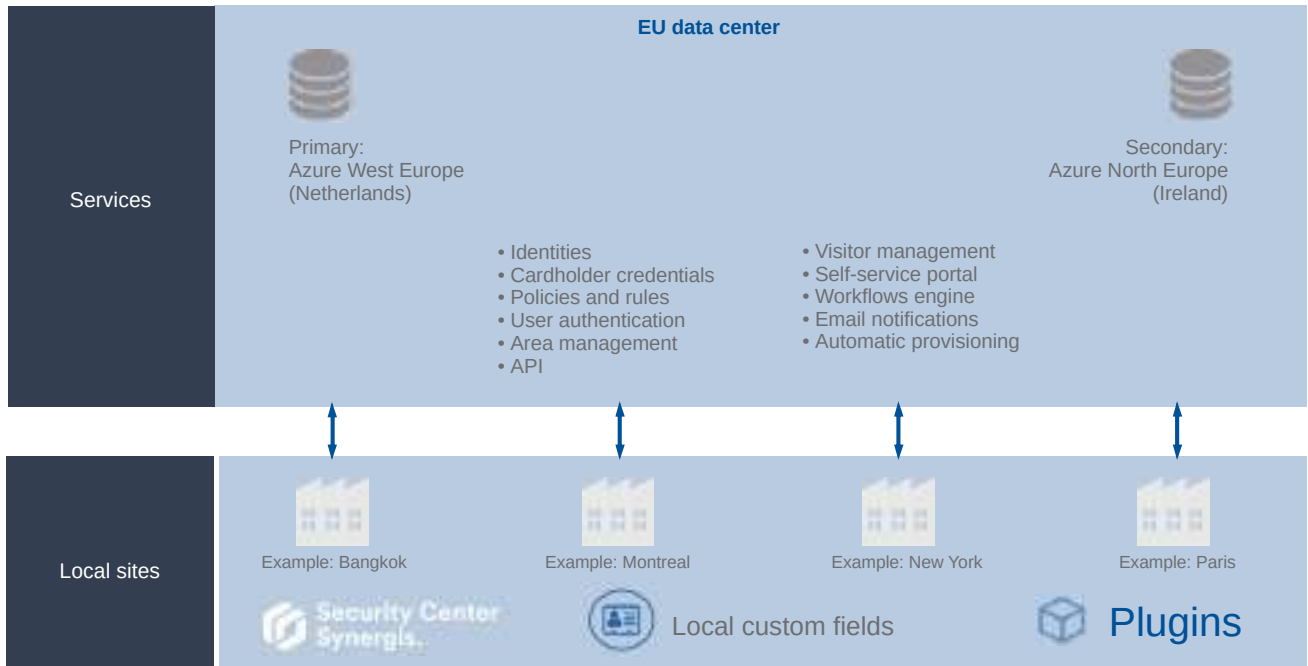
For more information, see [Setting up automatic expiration for access reviews](#).

What's New: January 2023

Europe only architecture (NOW AVAILABLE)

ClearID now includes a Europe only solution for customers who require all their data to be stored in Europe.

Genetec ClearID™ Europe only architecture



For more information, see [About ClearID architecture](#).

What's New: November 2022

Supervisor permissions enhanced

Administrators can now grant supervisors more control to manage their direct reports. Supervisors can now modify General identity information fields and Access control settings.



This option is useful for any organization that wants to decentralize some administration functions by allowing supervisors to manage their direct reports.

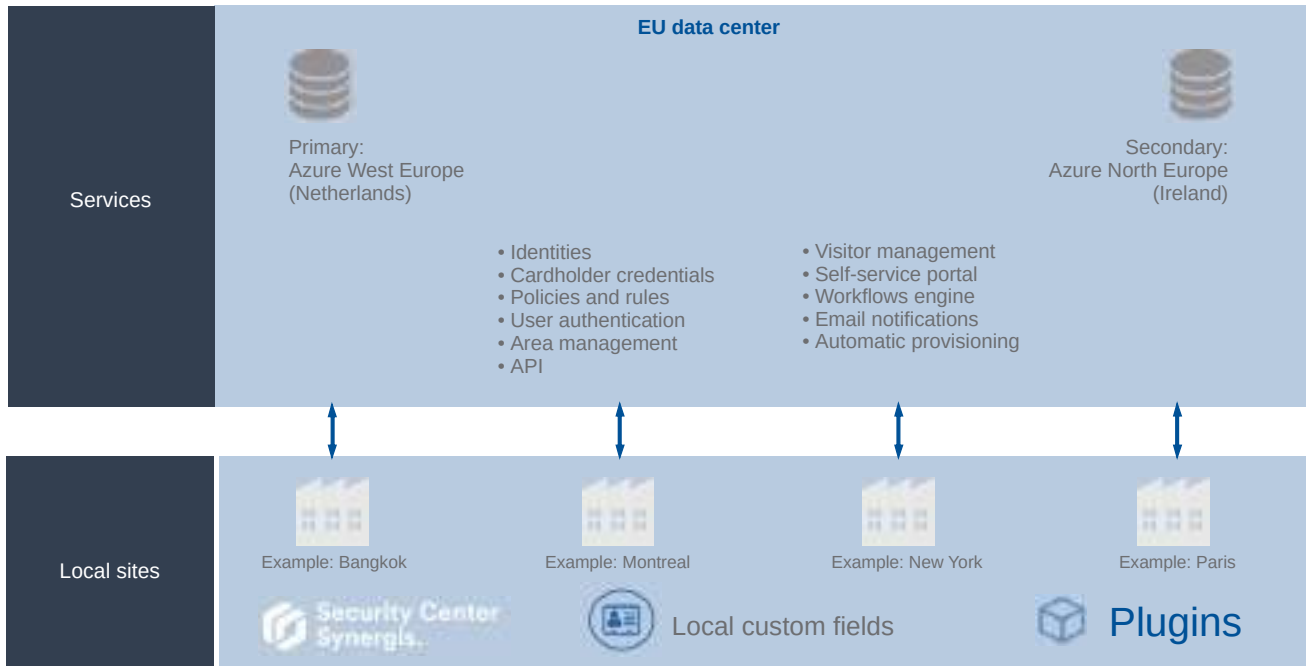
For more information, see [Managing direct reports in ClearID](#).

What's New: Coming soon

Europe only architecture (coming soon)

ClearID now includes a Europe only solution for customers who require all their data to be stored in Europe.

Genetec ClearID™ Europe only architecture



For more information, see [About ClearID architecture](#).

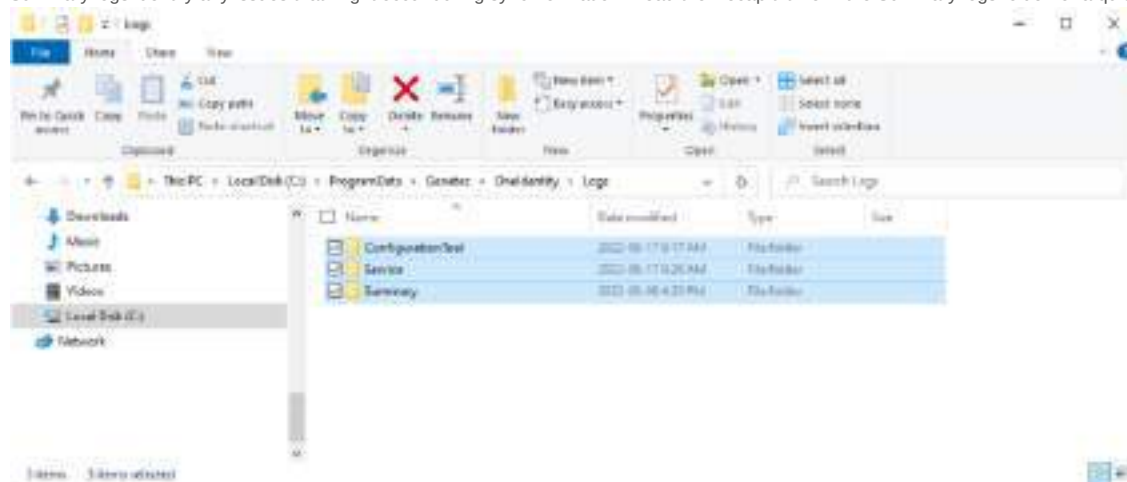
What's New: September 2022

Genetec ClearID One Identity Synchronization Tool

The Genetec ClearID One Identity Synchronization Tool has been updated and now supports the following:

Improved logging

Summary logs identify any issues that might occur during synchronization. Read the Recap.txt file in the Summary logs folder for a quick synchronization overview.



For more information, see [Viewing the ClearID One Identity Synchronization Tool logs](#).

Microsoft Graph library replaces Azure Active Directory Graph library

The Microsoft Graph library replaces the now deprecated Azure Active Directory Graph library. The new library supports all previous mappings.

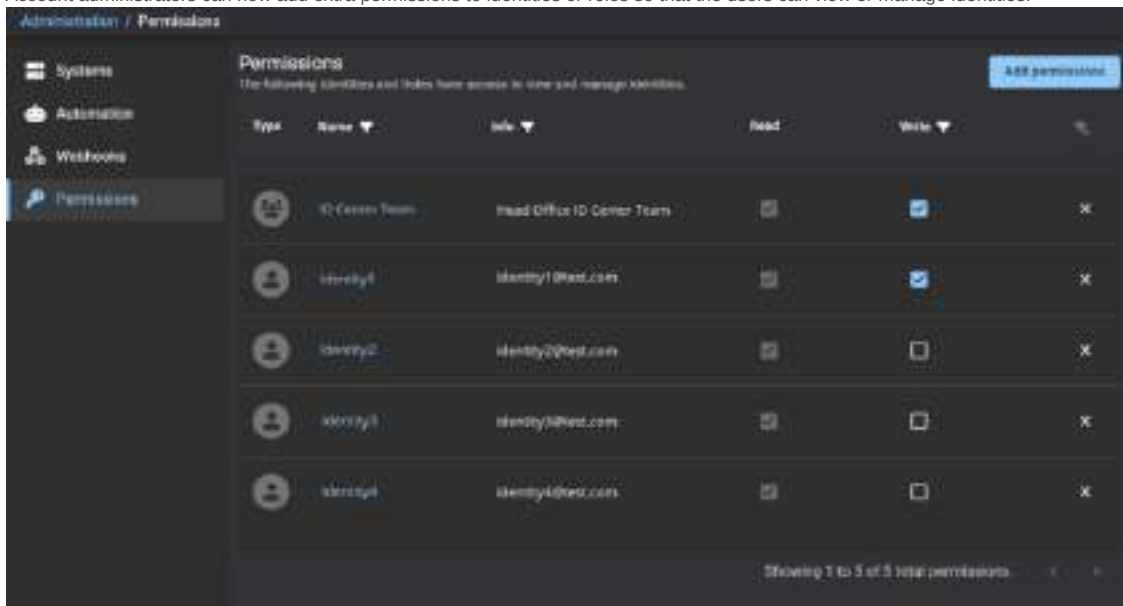
For more information, see [About the Azure web app for ClearID One Identity Synchronization Tool](#).

For more information about the synchronization tool, see [Synchronizing identities using One Identity Synchronization Tool in ClearID](#).

What's New: August 2022

Identity permissions

Account administrators can now add extra permissions to identities or roles so that the users can view or manage identities.



For more information, see [Granting additional permissions](#).

What's New: July 2022

Genetec ClearID Self-Service Kiosk 1.13.3

Genetec ClearID Self-Service Kiosk mobile app version 1.13.3 is now available.

The Genetec ClearID Self-Service Kiosk mobile app version 1.13.3 now supports the following Identity Document (ID) types:

- UAE - Driving License
- UAE - ID card
- UAE - Resident ID

For more information, see [Identity document types in ClearID](#).

To download the Genetec ClearID™ Self-Service Kiosk mobile app, visit the [App Store](#).

What's New: May 2022

ClearID best practices

ClearID User Guide now includes best practices information for the following:

- Setting up ClearID for a new Synergis system.
- Setting up ClearID with an existing Synergis system.

You can use the best practices to help plan your ClearID system deployments.

For more information, see [ClearID Best practices](#).

Requesting identities

An identity request wizard is now available to submit either an individual identity request or multiple identities request (CSV import) for different types of employees or contractors. Individual identity requests or multiple identities requests can be repeated using a template for specific employees who require the same access to a specific site, area, or building.

The following example shows an individual identity request:

The screenshot shows the 'identity request' wizard with four steps: 1. Identity template (checked), 2. General information (active), 3. Work details, and 4. Review. The 'General information' section contains the following fields: First name (John), Last name (Doe), Email (johndoe@test.com), Middle name (empty), Mobile phone number (123-456-7899), Preferred name* (John Doe), and External ID (empty). Below this is the 'Web portal access' section with a toggle for 'Grant user access to the web portal' (checked) and a status of 'N/A'. At the bottom are buttons for 'Save as draft', 'Back', and 'Next'.

The following example shows an identities request (CSV import):

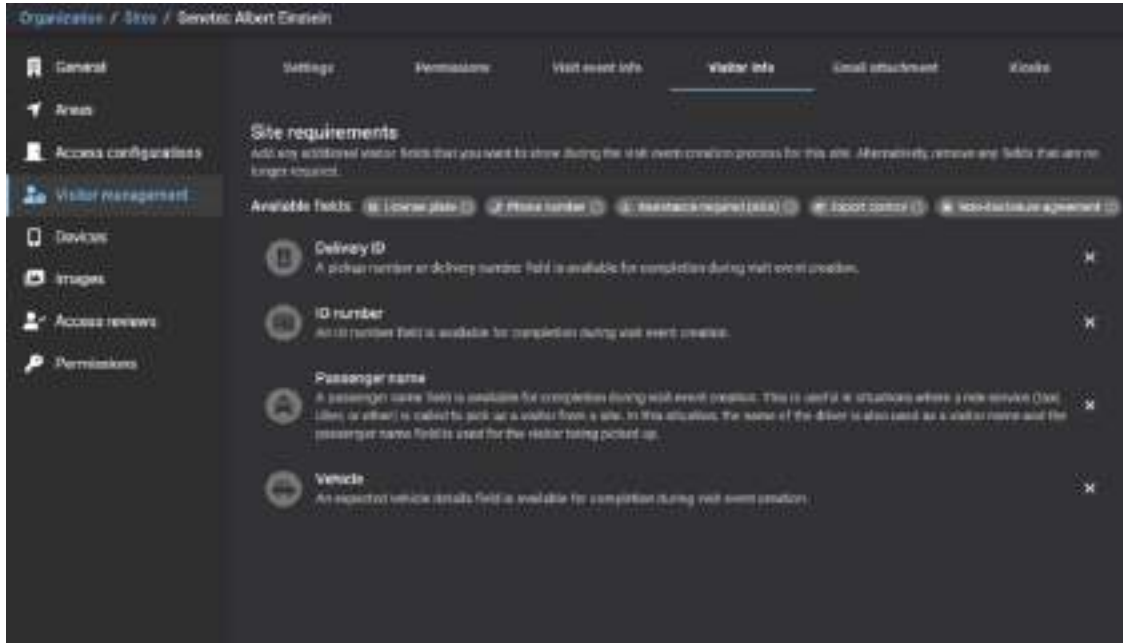
The screenshot shows the 'Request identities' wizard with three steps: 1. Basic information (checked), 2. Import (active), and 3. Review. The 'Import identities' section includes instructions: 'Import your identities for this request below. If any data errors are encountered during the identities import, fix the issues in the CSV file then import the file again. CAUTION: Importing the file again overwrites any data already imported into the grid.' There is an 'Import from CSV' button. Below the instructions, it says 'No records to display' and shows an empty table. At the bottom right, it says '0 total results'. At the bottom left is a 'Cancel' button, and at the bottom right are 'Back' and 'Next' buttons.

For more information, see About workflows in ClearID, Creating an identity template in ClearID, Requesting an identity in ClearID, and Requesting multiple identities using a CSV import in ClearID.

Visitor management enhancements

Visitor management for sites now includes more optional visitor information fields for the following:

- Delivery ID
- ID number
- Passenger name
- Vehicle



For more information, see the Visitor info tab in [Enabling visitor management for sites in ClearID](#).

What's New: March 2022

Genetec ClearID Self-Service Kiosk 1.13.1

Genetec ClearID Self-Service Kiosk mobile app version 1.13.1 is now available.

The ClearID Self-Service Kiosk mobile app version 1.13.1 now supports 78 additional Identity Document (ID) types and includes some additional countries.

For more information, see [Identity document types in ClearID](#).

To download the Genetec ClearID™ Self-Service Kiosk mobile app, visit the [App Store](#).

What's New: January 2022

Reports

ClearID now provides three more reports for audit trail and activity tracking purposes:

Genetec ClearID® User Guide
Displayed in the header

Site and area owners report

Account Administrators can now use the Site and area owners report to get a global view of all identities and their permissions. When the report is used by a site owner, only information about their own sites is shown.

Genetec

Dashboard

My Profile

Organization

Plans & Billing

Administration

Reports

[Access Events](#)
[Access Records](#)
[Visitor Records](#)
[Video](#)
[Get a Quote](#)
[Get a Demo](#)
[Admin Panel](#)

Day 1

Day 2

Day 3

Timeline 1

Assignment 1

Activity view 1

My profile view 1

Access Events

Access Records

Visitor Records

Video

Get a Quote

Get a Demo

Admin Panel

For more information, see [About reports in ClearID](#) and [Viewing a site and area owners report in ClearID](#).

User activity report

Account administrators can now use the User activity report to review all activities related to users.

The screenshot displays the 'Reports' section of a system, specifically the 'Total activity' tab. It shows a table of user activities over a period from February 23, 2020, to May 23, 2020. The table includes columns for the time stamp, activity type, the user who performed the activity, and details of the action.

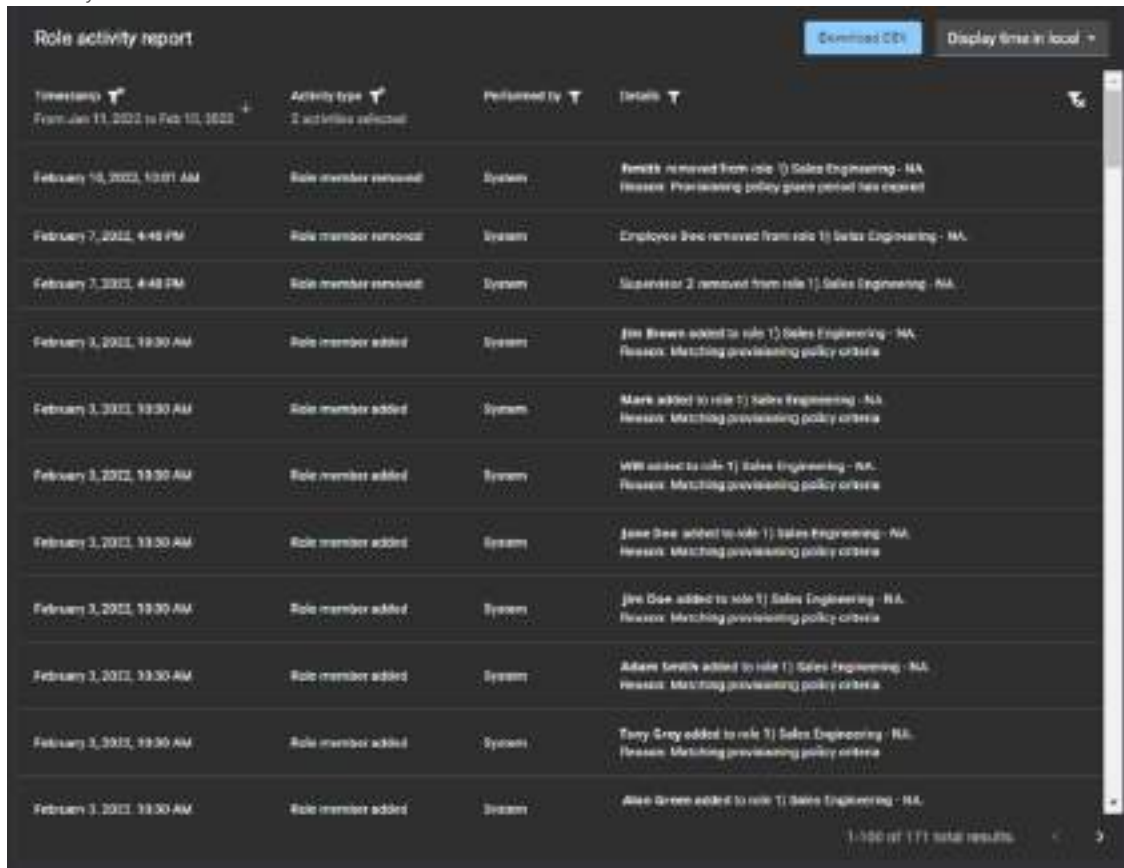
Time stamp	Activity type	Performed by	Details
April 2, 2020 at 1:52 PM	Area manager added	Erikka Della Cappa	Erikka Della Cappa added as area approver for Main Endowment
April 2, 2020 at 11:16 AM	Area member added	jack	Erikka Della Cappa added as area member for Main Endowment
April 2, 2020 at 11:16 AM	Area manager removed	jack	Erikka Della Cappa removed as area approver from Main Endowment
April 2, 2020 at 11:06 AM	Role member added	Erikka Della Cappa	Erikka Della Cappa added to user Identity Requests Decision: Unable to approve Identity Requests
April 2, 2020 at 11:07 AM	Role member added	Erikka Della Cappa	Erikka Della Cappa added to role Coordinator Manager Function: Erikka Della Cappa Coordinator Manager
April 2, 2020 at 11:07 AM	Role member added	Erikka Della Cappa	Erikka Della Cappa added to role Certified Function: Erikka Della Cappa Certified

Showing 1 to 5 of 13 total user activities.

For more information, see [About reports in ClearID](#) and [Viewing a user activity report in ClearID](#).

Role activity report

Account administrators can now use the Role activity report to review all activities related to roles. When the report is used by role managers or role owners, only the activity for their roles is shown.



Timestamp	Activity type	Performed by	Details
From Jan 11, 2022, to Feb 10, 2022	2 activities selected		
February 10, 2022, 10:01 AM	Role member removed	System	Remita removed from role 1) Sales Engineering - NA. Reason: Provisioning policy grace period has expired
February 7, 2022, 4:48 PM	Role member removed	System	Employee Dev removed from role 1) Sales Engineering - NA.
February 7, 2022, 4:48 PM	Role member removed	System	Supervisor 2 removed from role 1) Sales Engineering - NA.
February 3, 2022, 10:30 AM	Role member added	System	Joe Brown added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Mark added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Will added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Jane Doe added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Jim Doe added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Adam Smith added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Tony Grey added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Alice Green added to role 1) Sales Engineering - NA.

1-100 of 171 total results

For more information, see [About reports in ClearID](#) and [Viewing a role activity report in ClearID](#).

ClearID plugin

The ClearID plugin is a new integration for Security Center 5.7 SR6 or later.

3 | Deployment preparation

3.1 | License options for ClearID system integration

Use the following information to understand the licenses that are available for Genetec ClearID™ or the Genetec ClearID™ Self-Service Kiosk. To update your license, contact us and provide the part numbers listed in this topic.

ClearID license options

Part number	Description	Requirements
CID-DELIVERY	Remote support services for initial account setup of ClearID cloud-based service. These services include a block of eight hours of support. Services are rendered during local business days and normal business hours.	All services must be used within twelve months of your first support call. At the end of this twelve-month period, the full service fee is billed, and any unused support hours expire.
- CID-IDENTITY-1Y - CID-IDENTITY-3Y - CID-IDENTITY-5Y	One ClearID Identity license for one, three, or five years. An identity is a unique individual that is managed, governed, or authenticated by the system. The license includes two hours of ClearID deployment consultation.	This part is mandatory to use ClearID.
- CID-MULTI-SYSTEM-1Y - CID-MULTI-SYSTEM-3Y - CID-MULTI-SYSTEM-5Y	One ClearID multi-system license for one, three, or five years. Enables management and synchronization across multiple systems.	This part is mandatory to connect ClearID to two or more Security Center systems. NOTE: Only one system is required to support a ClearID account.

Part number	Description	Requirements
- CID-KIOSK-LIC-1Y - CID-KIOSK-LIC-3Y - CID-KIOSK-LIC-5Y	One ClearID kiosk license for one, three, or five year.	Each kiosk must be licensed. NOTE: The ClearID Self Service Kiosk app on an iPhone doesn't need to be licensed.

Synergis license options

To synchronize data between ClearID and Synergis™, one of the following part numbers is required:

NOTE: The following Synergis license options all include the CD-SC-PLUGIN by default. This package provides a license for one connection to ClearID cloud services. You need one license per Directory.

Part number	Description	Requirements
GSC-BASE-E 5.11 or later	The Synergis Base Enterprise package. NOTE: The base package includes the Synergis visitor management module by default.	
GSC-BASE-P 5.11 or later	The Synergis Base Professional package. NOTE: The base package includes the Synergis visitor management module by default.	
SCS-Base	Security Center SaaS Edition (Classic) - Base Package NOTE: The base package includes the Synergis visitor management module by default.	

Does your Security Center license include all the options you need?

In addition to a certificate for your plugin, ensure that your Security Center license includes all the options you expect to use in Security Center. For example, if you've integrated a system that has visitors, you need the Visitors option in Security Center. If an option is missing, an error message is displayed when the server tries to create or modify the entity related to that option.

For a list of available license options, see [License options in Security Center](#).

Browse

- Integration overview for the ClearID plugin
- ClearID Self-Service Kiosk options

3.2 | Compatibility for ClearID

The Genetec ClearID™ web portal and the ClearID plugin are compatible with Security Center 5.11 or later.

The web portal and plugin support Security Center versions for a maximum of 3 years after the first GA release date.

Supported Security Center versionsUse the following information to help you understand when each Security Center version will no longer be supported for use with ClearID:

Security Center version	Security Center first GA release date	Security Center end of support in ClearID
5.11	September 2022	September 2025
5.12	December 2023	December 2026
5.13	December 2024	December 2027

IMPORTANT: You must have Synergis™ Professional or Enterprise to use ClearID. For more information, see [License options for ClearID system integration](#).

3.3 | System requirements for ClearID

For the Genetec ClearID™ system to run efficiently in your web browser, the computer or mobile device that you use must meet certain software and hardware requirements.

The requirements for ClearID web application are as follows:

Desktop requirements

- Cookies and JavaScript are enabled in your web browser.

The ClearID web application is compatible with the following web browsers:

- Google Chrome (latest version)
- Microsoft® Edge (latest version)

ClearID plugin requirements

The following system requirements must be met to run the ClearID plugin:

Synergis Professional or Omnicast Professional is required for plugins support in Security Center.

Hardware

The ClearID plugin must be installed on a server that meets the recommended specifications, as described in the [Security Center system requirements](#).

Networking

The server that the plugin is installed on requires internet access to communicate between Synergis™ and ClearID cloud services. All communications use TCP port 443.

IMPORTANT: All data uploaded to the ClearID web application remains encrypted in transit and at rest.

3.4 | Firewall ports used in ClearID

To ensure that Genetec ClearID™ works as designed, the following ports, URLs, and network requirements must be met.

ClearID web portal

The following network configuration is required for the web portal:

- TCP Port 443 outbound
- *.clearid.io - Allow all outbound traffic for this domain
- *.core.windows.net - Allow all outbound traffic for this domain
- *.launchdarkly.com - Allow all outbound traffic for this domain

ClearID plugin

The following network configuration is required for the plugin:

- TCP Port 443 outbound
- *.clearid.io - Allow all outbound traffic for this domain
- *.servicebus.windows.net - Allow all outbound traffic for this domain
- *.core.windows.net - Allow all outbound traffic for this domain

NOTE: The server that the plugin is installed on requires internet access to communicate between Synergis™ and ClearID cloud services.

Genetec ClearID™ One Identity Synchronization Tool

The following network configuration is required for the One Identity Synchronization Tool:

- TCP Port 443 outbound
- *.clearid.io - Allow all outbound traffic for this domain

Genetec ClearID™ LDAP Synchronization Agent

The following network configuration is required for the LDAP Synchronization Agent:

- TCP Port 443 outbound
- *.clearid.io - Allow all outbound traffic for this domain

Genetec ClearID™ Self-Service Kiosk

The following features or network configuration are required for the Self-Service Kiosk:

- TCP Port 443 outbound
- *.clearid.io - Allow all outbound traffic for this domain
- Label Printer (Wi-Fi mode only) Bonjour - used for device search
- Label Printer (Wi-Fi mode only) SNMP - used for checking printer status information
- Label Printer (Wi-Fi mode only) UDP or TCP Port 9100 - used for sending print data

Other requirements

The following resources are used by ClearID to enhance the user experience, but they are not mandatory.

Google Maps:

- <https://www.google.com/>
- <https://maps.googleapis.com>
- <https://fonts.googleapis.com/>
- <https://maps.gstatic.com/>

Microsoft Application Insights:

- <https://dc.services.visualstudio.com/>
- <https://dc.applicationinsights.azure.com/>
- <https://dc.applicationinsights.microsoft.com/>

NOTE: These resources do not prevent you from using the ClearID portal, but some elements of the user interface might not format correctly unless these resources are available.

3.5 | Supported devices for ClearID

To help you understand the hardware devices that are supported for use with Genetec ClearID™ or the Genetec ClearID™ Self-Service Kiosk, use this supported devices list.

For each device, the corresponding firmware and certification level is listed.

Certified

Genetec Inc. has tested and validated the device.

Supported by design

The device has the same design characteristics as a certified device, but Genetec Inc. has not tested or validated the device.

Kiosk devices

The following iPad devices are supported for use with the ClearID Self-Service Kiosk.

Manufacturer	Model	Device type ¹	Version
Apple	Not applicable	• iPad 11.0 inches • iPad 10.9 inches • iPad 10.2 inches	Certified: iOS 16.1 or later

NOTE:

- ¹ Other iPad devices might also be supported (without kiosk stand) if they are running the Minimum iOS version required for the Kiosk mobile app. For example, the iPad Pro could be used. However, due to the iPad Pro physical dimensions it is not compatible with the Kiosk stand. For information about iPad power adapter requirements, see *ClearID Self-Service Kiosk options*.

Kiosk label printer

The following label printer devices are supported for use with the ClearID Self-Service Kiosk.

Manufacturer	Model	Device type	Version
Brother	QL-820NWBc (Network, Wi-Fi, Bluetooth) NOTE: Only DK-2205 or DK2251 (62mm Black or Red and Black) labels are supported for this printer.	Thermal Label Printer	Supported by design
Brother	QL-820NWB (Network, Wi-Fi, Bluetooth)	Thermal Label Printer	Supported by design (DEPRECATED) NOTE: The QL-820NWBc replaces the discontinued QL-820NWB printer.
Brother	QL-810W	Thermal Label Printer	Supported by design

Genetec ClearID®; User Guide

Displayed in the header

Manufacturer	Model	Device type	Version
	(Wi-Fi only)		
Brother	TD-4550DNWB (Network, Wi-Fi, Bluetooth) NOTE: Only RD001U1S (57mm Black) labels are supported for this printer.	Thermal Label Printer	Supported by design

QR code (2d barcode reader) devices

The following devices are supported for use with ClearID when using QR codes as a credential for visitors.

Manufacturer	Series	Model	Device type	Version
IBC	Qscan	Qscan (for parking lots)	Barcode scanner	Supported by design: Firmware qswie26m.bin
IBC	Qscan	QscanT (for turnstiles)	Barcode scanner	Supported by design
IBC	Qscan	QscanI (indoor version)	Barcode scanner	Supported by design
Zebra	DS9300	DS9308	Barcode scanner	Supported by design

STid OSDP devices

The following STid OSDP devices are supported for use with ClearID when using QR codes as a credential for visitors.

Manufacturer	Series	Model	Part Number	Device type	Version
STid	Architect®	ARC-AQ	SY-ARC-W33-AQPH5-7OS1	QR code reader - Classic Reader - QR Code Module	Supported by design All STid readers Firmware version 10 or later ¹
STid	Architect®	ARC-BQ	SY-ARC-W33-BQPH5-7OS1	QR code reader - Keypad Reader - QR module	Supported by design All STid readers Firmware version 10 or later ¹
STid	Architect® Blue	ARCS-AQ/BT	SY-ARCS-W33-AQBT1-7OS1	QR code reader - Classic reader - Crypto processor - QR Code module - Bluetooth	Supported by design All STid readers Firmware version 10 or later ¹
STid	Architect® Blue	ARCS-BQ/BT	SY-ARCS-W33-BQBT1-7OS1	QR code reader - Keypad reader - Crypto processor - QR Code module - Bluetooth	Supported by design All STid readers Firmware version 10 or later ¹

Manufacturer	Series	Model	Part Number	Device type	Version
STid	SECard ² - High security programming kit (Configuration software for the QR code reader)	Not applicable	KIT-SECARD-BT-V3.X	• STid ARC-G USB encoder • USB key containing SECard software	Supported by design Software version 3.5 or later.

STid model codes explained:

- ARCS = Crypto Processor
- AQ = reader + QR code
- BQ = Keypad reader + QR code
- BT = Bluetooth

¹ If you are re-using existing readers, refer to *STid documentation* about how to upgrade your reader to firmware version 10 or later.

IMPORTANT: ² Genetec Inc. does not provide support for the STid SECard solution. Customers require the stand-alone STid SECard software to configure the STid OSDP readers to work with the ClearID ACS panel solution.

Browse

- [ClearID Self-Service Kiosk options](#)
- [System requirements for ClearID](#)

3.6 | ClearID Best practices

Use the provided best practices to help you successfully plan, design, and configure your Genetec ClearID™ system deployments.

This information is intended for end users, integrators, or deployment contacts who are responsible for planning, designing, and configuring a ClearID system.

Review the following best practices before planning your deployments:

- [Best practices for setting up ClearID for a new Synergis system](#)
- [Best practices for setting up ClearID with an existing Synergis system](#)

3.6.1 | Best practices for setting up ClearID for a new Synergis system

Consider the following best practices when building a new Synergis™ system to align with Genetec ClearID™ for an eventual ClearID implementation.

This information is intended for end users, integrators, or deployment contacts who are responsible for planning, designing, and configuring a ClearID system.

IMPORTANT: Because every system has different requirements, these best practices alone cannot be used to deploy your system. The deployment steps vary depending on your organizations architecture and current setup.

- Use this information as a starting point only for basic planning purposes.
- If you require help with your deployment, contact your deployment contact.

Best Practice: Ensure that you always test your new deployment implementation in a demo environment before applying to your production environment.

Pre-ClearID deployment tasks

1. Plan your Sites and Areas to suit your access requirements.

Tip: Think about meaningful names that relate to the sites or areas that end users will request.

- a. Plan out the *Sites* and *Areas* that require access control.
 - Example sites: Main building, Satellite office 1, Satellite office 2 and so on.
 - Example areas: 1st floor, 2nd floor, server room, auditorium, and so on.

NOTE: A site is typically one physical building or a cluster of buildings in close proximity. The site configuration applies to the entire site so it should be controlled by the same sets of policies (access configurations and visitor management configurations).

- b. Plan out the *Roles* that you require for your access and identity grouping.
 - Example roles: Sales, Marketing, Executives, Faculty, Students, Production crew, Contractors, All permanent employees, All part-time employees.

- c. (Optional) Consider [attribute-based provisioning to automate role memberships](#).

NOTE: Make a note of these sites, areas, and roles for use during the deployment tasks (steps 3 and 4) detailed later in this procedure.

2. (Optional) Test your setup and configuration in a ClearID demo environment.

- a. Connect your ClearID demo account to a Synergis demo system.
- b. Contact your Genetec Inc. representative to request a ClearID DEMO account and a Synergis demo system.

IMPORTANT: The configuration performed in a demo environment cannot be migrated to a production system.

Deployment tasks

1. Connect your new production Synergis system with your ClearID production account.
 - a. Install the ClearID plugin.
 - b. Connect Security Center to ClearID.
2. Synchronize identities with your data source.

Depending on your specific requirements, do one of the following:

 - o Synchronize your identities using the Genetec ClearID™ One Identity Synchronization Tool.
 - o Synchronize your identities using the API.
3. In the ClearID web portal, create the sites and areas that you planned earlier.
 - a. Create your sites.
 - b. Create your areas.
4. In the ClearID web portal, create the roles and attribute provisioning policies that you planned earlier.
 - a. Create your roles.
 - b. (Optional) Create attribute-based provisioning policies to automate role memberships.

Parent topic: [ClearID Best practices](#)

Browse

- [About cardholder and identity relationships](#)
- [About custom fields in ClearID](#)
- [About ClearID One Identity Synchronization Tool attribute fields](#)

3.6.2 | Best practices for setting up ClearID with an existing Synergis system

Consider the following best practices when setting up Genetec ClearID™ with an existing Synergis™ system.

This information is intended for end users, integrators, or deployment contacts who are responsible for planning, designing, and configuring a ClearID system.

IMPORTANT: Because every system has different requirements, these best practices alone cannot be used to deploy your system. The deployment steps vary depending on your organizations architecture and current setup.

- Use this information as a starting point only for basic planning purposes.
- If you require help with your deployment, contact your deployment contact.

Best Practice: Ensure that you always test your new deployment implementation in a demo environment before applying to your production environment.

Pre-ClearID deployment tasks

1. [Prepare your cardholder information.](#)
 - a. In Security Center, make sure that the existing cardholders have the required information to link with ClearID identities.

IMPORTANT: Cardholder Email field or External ID custom field must be populated.

 - This check ensures that existing identities and future identities are linked with pre-existing cardholders.
 - Future cardholders created by ClearID will already be linked correctly.
2. Plan your Sites and Areas to suit your access requirements.

Tip: Refer to your existing Synergis system when planning out your requirements. Think about meaningful names that relate to the sites or areas that end users will request.

 - a. Plan out the *Sites* and *Areas* that require access control.
 - Example sites: Main building, Satellite office 1, Satellite office 2 and so on.
 - Example areas: 1st floor, 2nd floor, server room, auditorium, and so on.

NOTE: A site is typically one physical building or a cluster of buildings in close proximity. The site configuration applies to the entire site so it should be controlled by the same sets of policies (access configurations and visitor management configurations).
 - b. Plan out the *Roles* that you require for your access and identity grouping.
 - c. (Optional) Consider attribute-based provisioning to automate role memberships.

NOTE: Make a note of these sites, areas, and roles for use during the deployment tasks (steps 3 and 4) detailed later in this procedure.
3. (Optional) Test your setup and configuration in a ClearID demo environment.
 - a. Connect your ClearID demo account to a Synergis demo system.
 - b. Contact your Genetec Inc. representative to request a ClearID DEMO account and a Synergis demo system.

IMPORTANT: The configuration performed in a demo environment cannot be migrated to a production system.

Deployment tasks

1. Connect your existing production Synergis system with your ClearID production account.
 - a. Install the ClearID plugin.
 - b. Connect Security Center to ClearID.
2. Synchronize identities with your data source.

Depending on your specific requirements, do one of the following:

 - o Synchronize your identities using the API.
 - o Synchronize your identities using the Genetec ClearID™ One Identity Synchronization Tool.
3. In the ClearID web portal, create the sites and areas that you planned earlier.
 - a. Create your sites.

- b. [Create your areas.](#)
- 4. In the ClearID web portal, create the roles and attribute provisioning policies that you planned earlier.
 - a. [Create your roles.](#)
 - b. (Optional) Create attribute-based provisioning policies to automate role memberships.

Parent topic: [ClearID Best practices](#)

Browse

- [About cardholder and identity relationships](#)
- [About custom fields in ClearID](#)
- [About ClearID One Identity Synchronization Tool attribute fields](#)

4 | ClearID plugin

4.1 | About ClearID plugin for Security Center

The Genetec ClearID™ Plugin integrates Genetec ClearID™ with Security Center and connects Synergis™ and ClearID cloud services. Any actions performed in ClearID are automatically synchronized with Synergis.

NOTE: Genetec ClearID™ was designed with a focus on the API. This API focus means that an Account administrator can create an API integration and use their own tools or services to communicate with our API.

You can download the ClearID plugin for Security Center [here](#).

Browse

- [ClearID API](#)

4.2 | About cardholder and identity relationships

Depending on the type of systems you want to integrate in Genetec ClearID™, you can choose to manage your cardholders and credentials manually or use ClearID to manage them automatically.

For cardholders that aren't created by ClearID, ClearID doesn't initially know which *identity* the *cardholder* belongs to. In this situation, ClearID finds different cardholder fields, identifies relationships, and associates them with the correct corresponding identities in the ClearID system.

ClearID compares the following information before creating a relationship between a cardholder and an identity:

Global unique identifier (GUID)

When our system creates a cardholder, we use the same GUID as the identity to create it.

Tip: You can find the GUID in the identity record URL for a ClearID user.

Code

```
https://demo.clearid.io/techdoc/organization/identities/139e92cd-44b9-427e-8727-bf7681ef0a8d
```



Where 139e92cd-44b9-427e-8727-bf7681ef0a8d is the GUID.

Email address

If the business email is the same as the cardholder email.

External ID

This field is an external identifier for creating identities in ClearID using the identity service API. The ClearID plugin creates this field in Security Center as a custom field for cardholders.

Best Practice: In Config Tool, check that all your cardholders have a valid business email address or external ID before adding your systems in ClearID. This check ensures that cardholders are correctly associated with the corresponding identities. For more information, see [Best practices for setting up ClearID with an existing Synergis system](#).

Scenario 1: Automatically manage cardholders and credentials

Select the Genetec ClearID: Cardholder and credential changes are synchronized back to Security Center radio button when you have a Security Center system and you want ClearID to create and manage your cardholders and credentials.

For example, a customer has a new Security Center system that is deployed without any cardholders or credentials already defined. By installing the ClearID plugin and adding access to identities, the corresponding cardholders and credentials are populated in the Security Center system and are automatically synchronized.

Tip: Use the Credentials configuration in the ClearID portal to synchronize your credentials.

For more information about credentials synchronization, see [Configuring credential replication in ClearID](#).

Scenario 2: Manually manage cardholders and credentials

Select the Security Center: Cardholders and credentials in ClearID are read-only radio button when you want ClearID to use existing cardholders and credentials without managing their state. In this situation, ClearID has access to Security Center cardholders and credentials in read-only mode because you want ClearID to know about your cardholders and credentials, but you never want ClearID to modify them.

For example, a customer has Security Center set up with 1000 cardholders and they use the ClearID plugin to connect the system to ClearID:

- If the Genetec ClearID: Cardholder and credential changes are synchronized back to Security Center radio button isn't selected when they add their systems, none of the cardholders or credentials information is modified or synchronized. Cardholders and credentials must be created and synchronized using other solutions. For example, Lightweight Directory Access Protocol (LDAP), Global Cardholder Synchronizer role, import plugins, and so on.
- If the Security Center system is already synchronized with an LDAP, they should synchronize ClearID with the same LDAP source.

Tip: Use LDAP or the *Global Cardholder Synchronizer* role in Security Center to create and synchronize cardholders and credentials.

For more information about global cardholder synchronization, see [Global cardholder management](#).

Browse

- [Reviewing cardholders and identities information in ClearID](#)
- [Adding a system to ClearID](#)
- [Synchronizing ClearID identity pictures with Security Center](#)

4.3 | Downloading and installing the ClearID plugin

To integrate the Genetec ClearID™ web application into Security Center, you must install the ClearID plugin on a Security Center server.

Before you begin

Ensure the following:

- Your server meets the [recommended system requirements](#).
- A [compatible version](#) of Security Center is installed.

What you should know

Best Practice: Although it's possible to host the ClearID role on any server, for best system performance host that role on a dedicated expansion server.

- To install or configure the plugin in Security Center, you must be a Site administrator. For example, local security, system integrator, or Security Center administrator.
- Synergis Professional or Omnicast Professional is required for plugins support in Security Center.
- Failover or Federation™ are not supported.

Procedure

1. Open the GTAP Product Download page.
2. From the Download Finder list, select your version of Security Center.
3. Search for your package by name and download it.
4. Download the plugin .exe file [here](#).
5. Follow your browser prompts to download the .exe file.
6. Stop the Genetec Server, and close Security Desk and Config Tool.
7. Open the extracted folder, right-click the setup.exe file, and click Run as administrator.
8. Open the downloaded file folder location, right-click the setup.exe file, and click Run as administrator.
9. Follow the installation instructions.

The plugin is installed to C:\Program Files (x86)\Genetec Inc\Genetec Security Center Plugins - ClearID\ by default.

10. On the Installation Wizard Completed page, click Finish.

After you finish

Return to Config Tool, and connect the ClearID plugin to ClearID cloud services account.

Best Practice: Use the Genetec™ Update Service (GUS) to keep the ClearID plugin up to date. For more information, see [About the Genetec Update Service](#).

Browse

- [How the ClearID plugin works with Security Center](#)

4.4 | Creating the ClearID plugin role

Before you can configure and use the Genetec ClearID™ plugin, you must create the plugin role in Config Tool.

Before you begin

[Download and install the plugin.](#)

What you should know

- To install or configure the plugin in Security Center, you must be a Site administrator. For example, local security, system integrator, or Security Center administrator.
- Each plugin role can only connect to or communicate with one unique ClearID system name at a time. For environments with multiple systems, you must create a plugin role for each system.

Procedure

1. From the Config Tool homepage, open the Plugins task.
2. In the Plugins task, click Add an entity () , and select Plugin.
The plugin creation wizard opens.
3. On the Specific info page, select the server on which the plugin role is hosted, the plugin type, and the database for the plugin role, and then click Next.
If you do not use expansion servers in your system, the Server option is not displayed.
IMPORTANT: The entry in the Database server field might default to the (local)\SQLEXPRESS setting. If this is not the correct server, choose the correct server from the Database server list.
4. On the Basic information page, specify the role information:
 - a. Enter the Entity name.
 - b. Enter the Entity description.
 - c. Select the Partition for the plugin role.
If you do not use partitions in your system, the Partition option is not displayed. Partitions are logical groupings used to control the visibility of entities. Only users who are members of that partition can view or modify the role.
 - d. Click Next.
5. On the Creation summary page, review the information, and then click Create, or Back to make changes.
After the plugin role is created, the following message is displayed: The operation was successful.
6. Click Close.
7. If you require multiple systems in your ClearID environment, repeat this procedure for each additional role that you require.

Results

The plugin role appears in the entity browser.

After you finish

You can now [connect Security Center to ClearID](#).

4.5 | Connecting Security Center to ClearID

Before you can connect the Genetec ClearID™ plugin role to your ClearID account, you must add your ClearID system and download an activation file. This activation file is then used to connect your Security Center system to the ClearID web application.

Before you begin

[Create the plugin role.](#)

What you should know

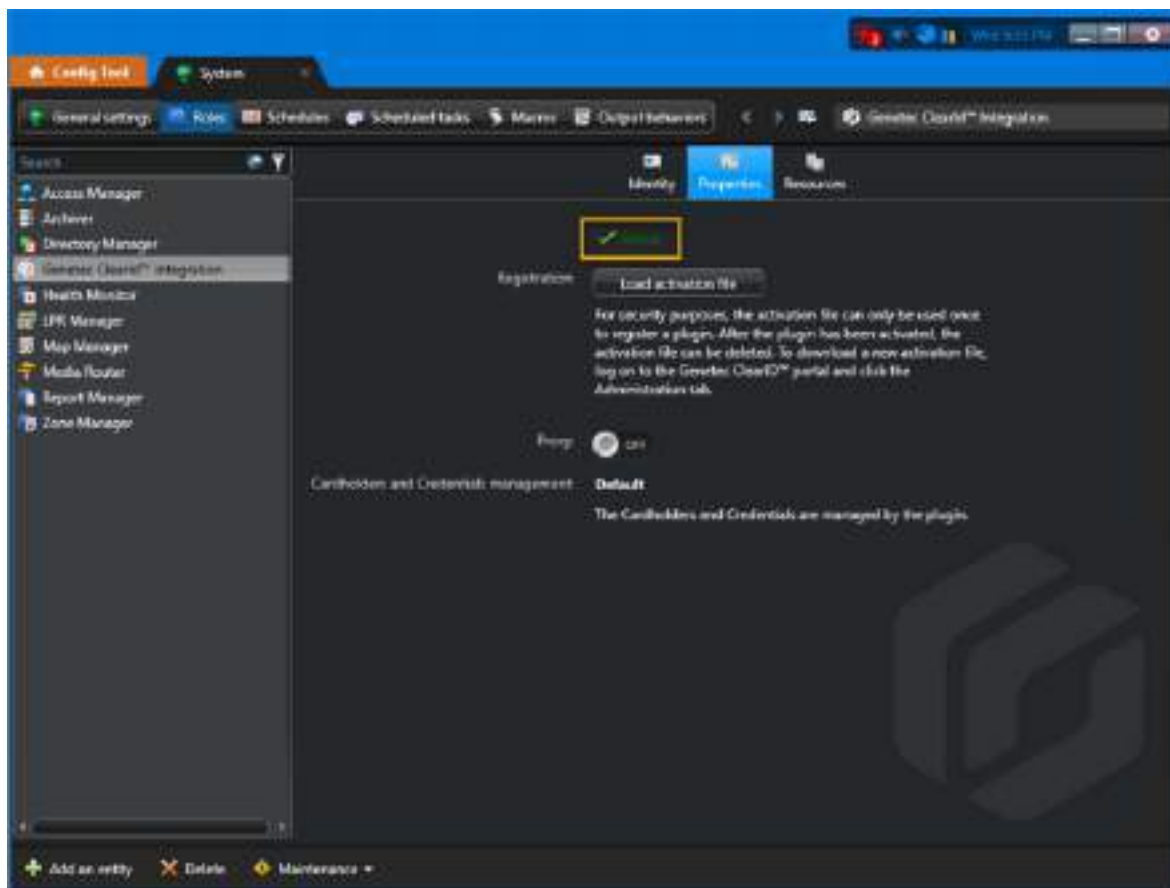
- To create systems in ClearID, you must be a Global administrator.
- To install or configure the plugin in Security Center, you must be a Site administrator. For example, local security, system integrator, or Security Center administrator.
- An activation file is used to authenticate the communication between your Security Center system and the ClearID web application.

Procedure

1. (Optional) If you have pre-existing Synergis™ cardholders, [review your cardholders and identities information](#).
2. [Add a system to ClearID](#).
3. [Download the activation file for the system you just created](#).
4. [Configure the connection settings using the activation file you just downloaded](#).
5. If you require multiple systems in your ClearID environment, repeat these steps for each additional system name that you require.

Results

The ClearID plugin is now connected to Security Center.



Browse

- Synchronizing ClearID identity pictures with Security Center

4.5.1 | Reviewing cardholders and identities information in ClearID

To ensure that cardholders are correctly associated with their corresponding identities in Genetec ClearID™ when systems are added, check that all cardholders have a valid business email address.

Before you begin

Learn about cardholder and identity relationships.

What you should know

This procedure is only applicable when you are setting up ClearID with an existing Synergis™ system that contains cardholders.

- All existing cardholders in Security Center require a valid business email address before they can be associated with their corresponding identities in ClearID.
- If all cardholders are created by ClearID, then the GUID is used to associate the cardholders with their corresponding identities automatically.

Procedure

To review identities in ClearID:

1. From the Home page, click Organization > Identities.
2. Click an identity in the list to see the identity details.

The following example shows a ClearID identity:

Organization / Identities / Test Cloud Employee

Test Cloud Employee

General Access Roles Delegations Device reports Access control User permissions Risk management Credentials

General **Active**

First name: Test **Last name:** Cloud Employee **Phone number:** **Mobile phone number:**

Middle name: **Business email:** cloudemployee@test.com **Personal email:**

Preferred name: Test Cloud Employee **Social link:** **Social ID:**

Country: Canada **State or Province:** **Street:**

City: **Zip or Post code:**

Company

Company: Genetec **Primary role:** Type to search... **Worker type description:** **Worker type code:**

Department: **Supervisor name:** **Job title:** **Employee number:**

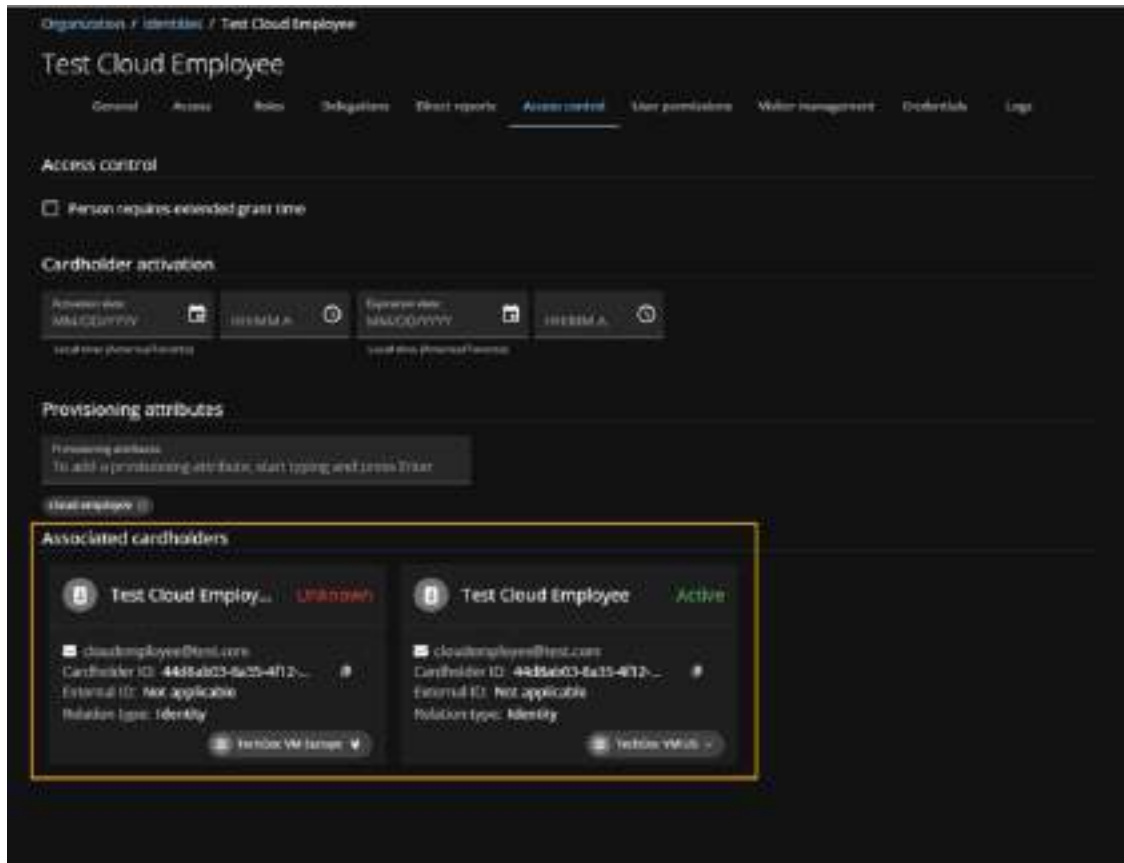
Supervisors

Name	Email
No supervisors	

Requests from this user do not require supervisor approval.

To review cardholders associated with a ClearID identity:

1. From the Home page, click Organization > Identities.
2. Click an identity in the list to see the identity details.
3. Click Access control.
A list of Security Center cardholders associated with a ClearID identity is displayed in the Associated cardholders section.



After you finish

Add your systems.

Parent topic: Connecting Security Center to ClearID

Browse

- About cardholder and identity relationships
- Synchronizing ClearID identity pictures with Security Center

4.5.2 | Adding a system to ClearID

Before you can connect the Genetec ClearID™ plugin role to your ClearID account, you must add your Security Center systems to ClearID.

Before you begin

- Create the plugin role.
- (Optional) If you have pre-existing Synergis™ cardholders, follow the best practices for Setting up Genetec ClearID™ with an existing Synergis™ system.
 - In Config Tool, check that all your cardholders have a valid business email address or external ID before adding your systems in ClearID. This check ensures that cardholders are correctly associated with the corresponding identities.
- Connect Security Center to ClearID.

What you should know

- To create systems in ClearID, you must be a Global administrator.

Procedure

1. Log on to your ClearID account.
2. From the Dashboard, click Administration > Add system.

← BACK

Add system

System name *

A descriptive name to identify your system. This can be changed later.

Data center region *

The region where your system information will be stored. This choice is permanent and cannot be changed.

Cardholder and credential management

The source of truth for cardholders and credentials.

☒ Genetec ClearID™: Cardholder and credential changes are synchronized back to Security Center.

☐ Security Center: Cardholders and credentials in ClearID are read-only.

Terms of service

☐ I accept the [Genetec Cloud Services - Subscriber terms of service](#) *

Cancel Save

NOTE: The Data center region option is not available for accounts deployed in regional architectures, such as Europe-only, Canada-only, or Australia-only data centers.

3. In the Add system dialog box, complete all the fields:
 - a. Enter a system name.

Tip: Use a system name that represents the name of the account and the associated data center region. For example, GenetecEuropeSC.
 - b. From the Data center region list, select a region that applies to the geographical location of your system or where you want data stored.
 - c. If you want ClearID to populate cardholder and credential fields automatically, select Genetec ClearID™: Cardholder and credential changes are synchronized back to Security Center.

This is the default option.
 - d. If you want to manage cardholder and credential fields manually, select Security Center: Cardholders and credentials in ClearID are read-only.
 - e. Select the checkbox to accept the terms of service, and click Save.

← BACK

Add system

System name *

Montreal HQ

A descriptive name to identify your system. This can be changed later.

Data center region *

Canada

The region where your system information will be stored. This choice is permanent and cannot be changed.

Cardholder and credential management

The source of truth for cardholders and credentials.

☒ Genetec ClearID™: Cardholder and credential changes are synchronized back to Security Center.

☐ Security Center: Cardholders and credentials in ClearID are read-only.

Terms of service

☒ I accept the [Genetec Cloud Services - Subscriber terms of service](#) *

Cancel Save

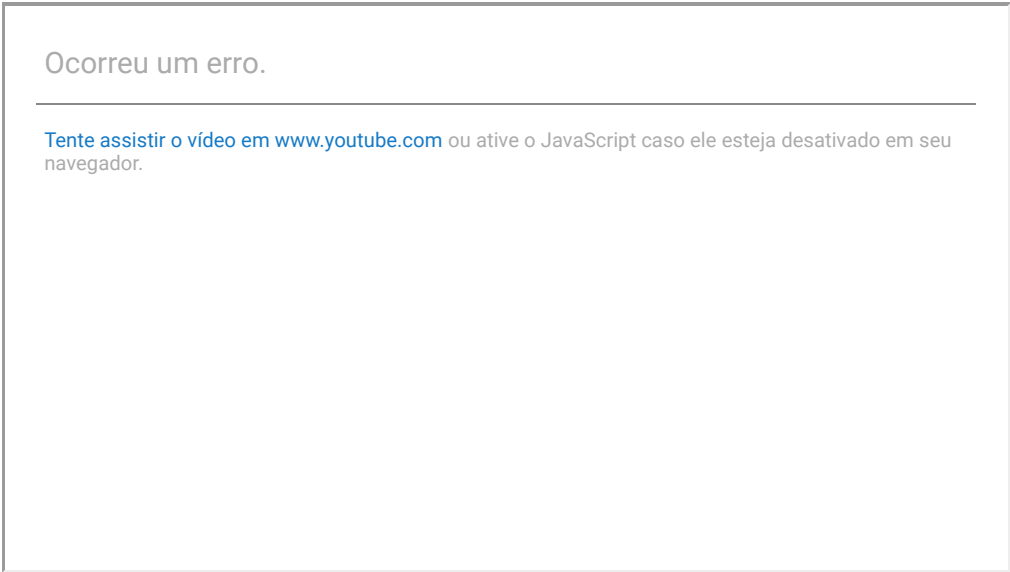
Results

Your new system is created. The system remains inactive until you download an activation file and register the ClearID plugin.



Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.



After you finish

- Download the activation file.
Parent topic: Connecting Security Center to ClearID
Browse
- About ClearID system states
 - About cardholder and identity relationships

4.5.3 | Downloading an activation file for ClearID

Before you can connect the Genetec ClearID™ plugin role to your ClearID account, you must download an activation file. This activation file is then used to connect your Security Center system to the ClearID web application.

Before you begin

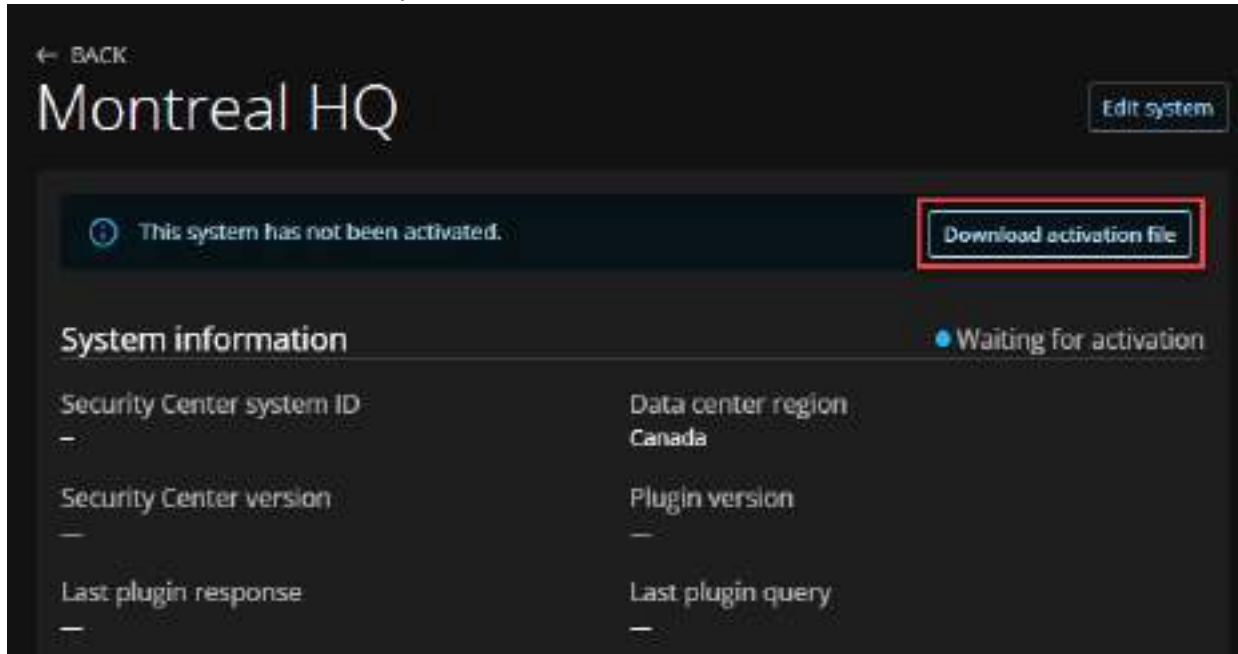
Add a system to ClearID.

What you should know

- To install or configure the plugin in Security Center, you must be a Site administrator. For example, local security, system integrator, or Security Center administrator.

Procedure

1. From the Dashboard, click the Administration tab.
2. On the Systems page, select a system.
3. Click Download activation file to save the file in json format.



Tip: Note the location of the activation file for later use. By default, the activation files are named systemname-systemID-activation-file.json.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.



After you finish

Configure the connection settings.

Parent topic: Connecting Security Center to ClearID

4.5.4 | Configuring connection settings for ClearID

To configure connection settings, you must load a previously downloaded activation file. This activation file is then used to connect your Security Center system to the Genetec ClearID™ web application.

Before you begin

[Download an activation file for ClearID.](#)

What you should know

- To install or configure the plugin in Security Center, you must be a Site administrator. For example, local security, system integrator, or Security Center administrator.
- An activation file is used to authenticate the communication between your Security Center system and the ClearID web application.
- For security purposes, the activation file can only be used once to register a plugin. After the plugin is activated, the activation file can be deleted.

Procedure

1. From the Config Tool homepage, open the Plugins task.
2. Select ClearID Integration from the entity browser, and click the Properties tab.
3. Click Load activation file and select the activation file that you previously downloaded.
4. (Optional) Configure the proxy server settings:

A proxy server is a server that verifies and forwards incoming client requests to other servers for further communication. For example, when a client is unable to meet the security authentication requirements of the server but should be permitted access to some services.

ON

Specifies that a proxy server is required to access the Internet. This option is typically used by customers behind a firewall or where network access to the Internet is restricted.

OFF

Specifies that a proxy server is not required. This is the default.

Proxy URL

If Proxy is enabled, enter the proxy URL supplied by your organization. For example, <https://proxy:8080/outgoing>. This information is typically supplied by the network administration team.

5. (Optional) Configure the proxy authentication settings:
Proxy authentication is the process of validating user credentials for access to a proxy server. This authentication typically includes a username and can also include a password.

ON

Specifies that proxy authentication is required.

OFF

Specifies that proxy authentication is not required.

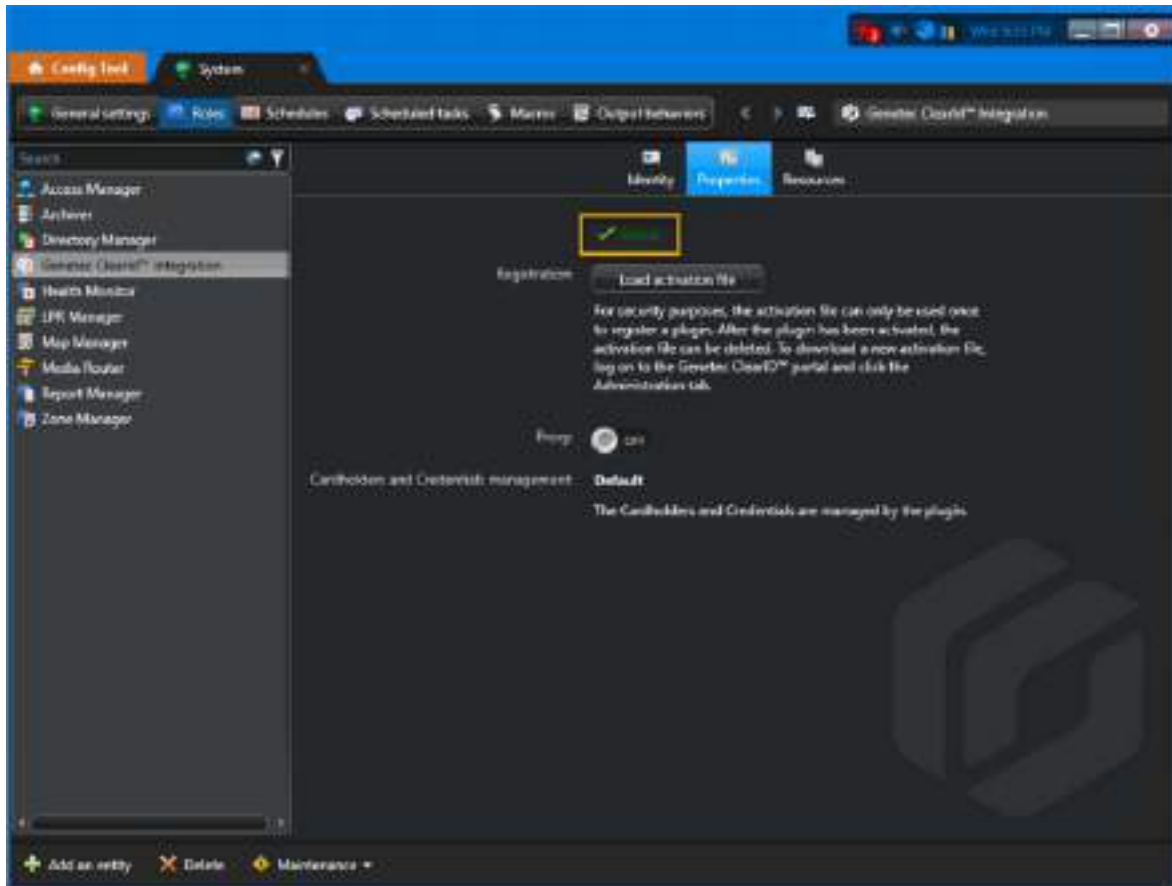
Proxy username

If proxy authentication ON was enabled, enter the proxy username supplied by your organization.

6. If proxy authentication ON is specified, set a proxy authentication password:
 - a. Click Set password.
 - b. Enter a New Password and then confirm the password.
NOTE: Use industry best practices for creating strong passwords.
 - c. Click Apply to save your password.
7. Click Apply to save all changes.

Results

The ClearID plugin is now connected to Security Center.



Parent topic: Connecting Security Center to ClearID

4.6 | Granting user privileges for the ClearID plugin

To allow users to access the Genetec ClearID™ plugin features and tasks, you must grant them the correct user privileges in Security Center.

What you should know

For administrators to install and configure the plugin in Config Tool, and for operators to use Security Desk functions, the correct user privileges must be granted to their user accounts.

This topic lists the minimum user privileges required.

NOTE: You might require more privileges, depending on the tasks you want to perform in Config Tool and Security Desk. For more information, see the [Security Center privileges spreadsheet](#) for your version.

Procedure

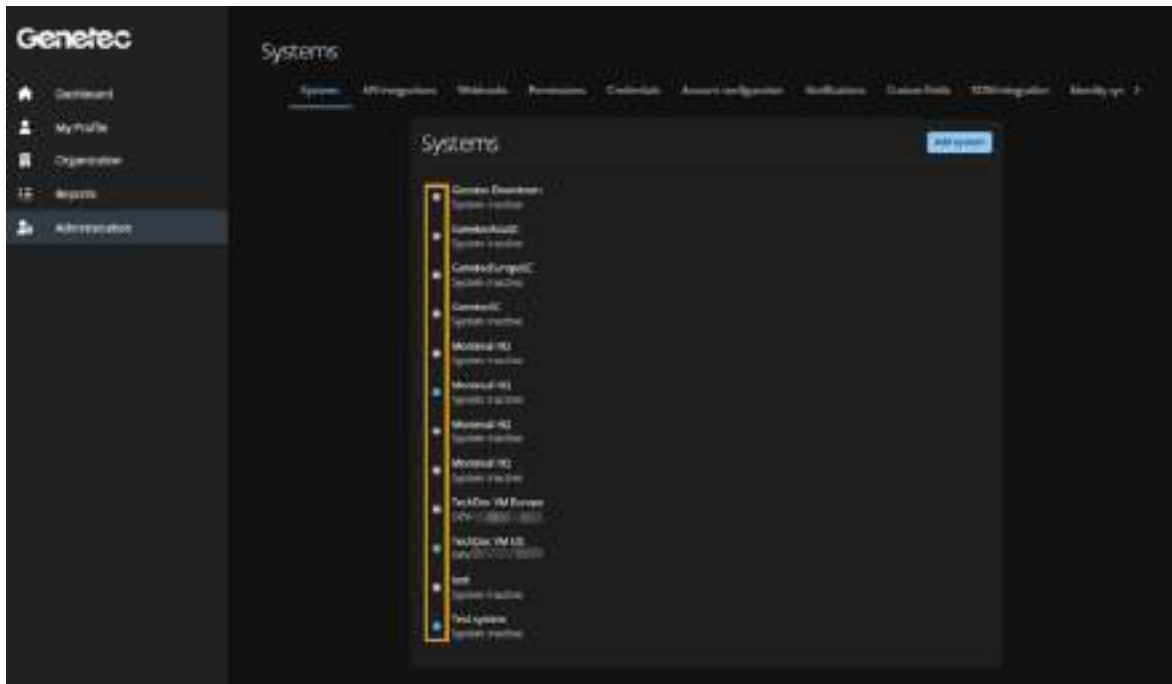
1. From the Config Tool homepage, open the User management task.
2. Select the relevant user, and click the Privileges tab.
3. Set the following privileges to Allow:
 - Application privileges > Security Desk
 - Application privileges > Config Tool
 - Administrative privileges > System management > View role properties
 - Administrative privileges > System management > View server properties
 - Task privileges > Administration > Plugins
4. (Optional) Set the custom field privileges that you require to Allow.
 - Administrative privileges > Access control management > View cardholder group properties > Modify cardholder group properties > Modify custom fields
 - Administrative privileges > Access control management > View cardholder properties > Modify cardholder properties > Modify custom fields
 - Administrative privileges > Access control management > View credential properties > Modify credential properties > Modify custom fields
 - Administrative privileges > Access control management > View visitor properties > Modify visitor properties > Modify custom fields
 - Administrative privileges > System management > View general settings > Modify custom field definitions
5. Click Apply.

Browse

- [About custom fields in ClearID](#)

4.7 | About ClearID system states

When you create or configure a Genetec ClearID™ system, the system goes through different states before being online or active. You can see the real-time status of ClearID systems on the Systems page.



Hover over the dot beside each ClearID system name to view its status:

Creating

Indicates that a new *system name* is being created.

New

Indicates that the *system name* has been successfully created. The activation file can now be downloaded to register the system.

Not available

Indicates that the API is not available, or is unable to respond.

Offline

Indicates that the system is offline. This status is displayed when the plugin has not sent a *heartbeat* response within 10 - 15 minutes to ClearID.

Online

Indicates that the system is registered, online, and connected to the ClearID plugin.

Unknown

Indicates that the system status cannot be obtained.

Waiting for activation

Indicates that the activation file was downloaded and the system is waiting for activation.

Warning

Indicates that the ClearID cloud services or the ClearID plugin did not process a message request within 10 minutes.

Tip: Move your mouse over a system status in the Status column to display the status explanation in the user interface.

Browse

- Adding a system to ClearID

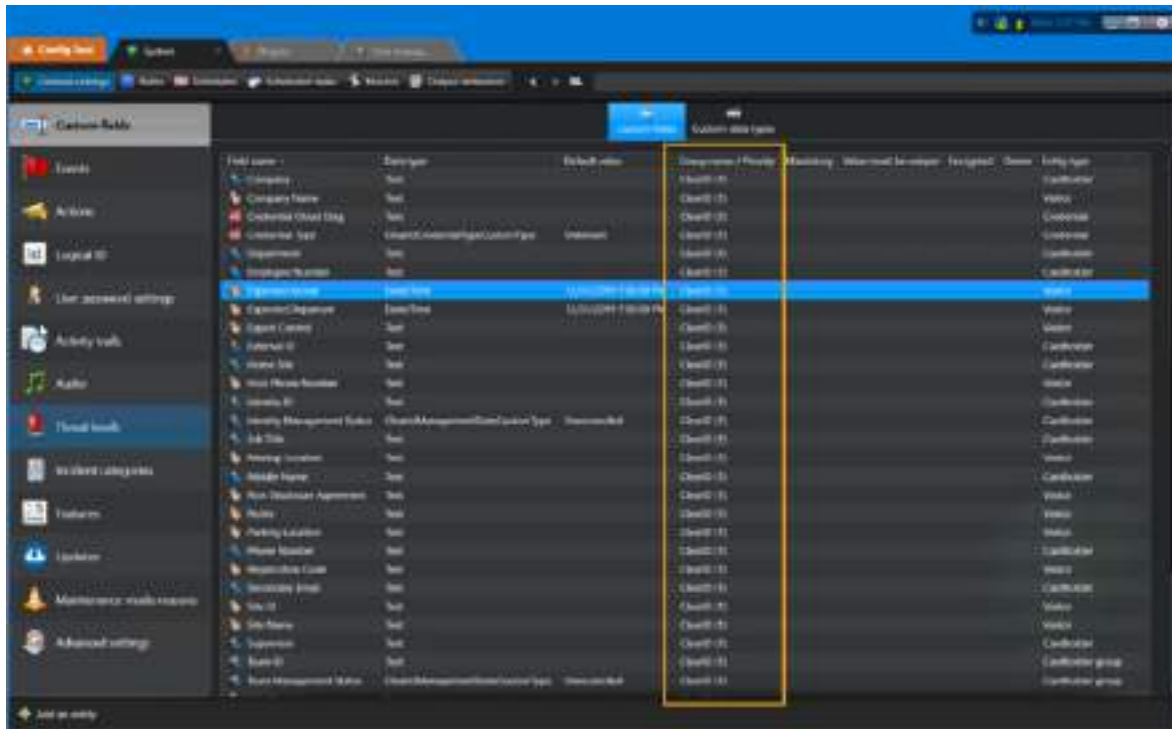
4.8 | About custom fields in ClearID

A custom field is a user-defined property associated with an entity type. Custom fields are useful for storing additional information.

In Security Center, Genetec ClearID™ uses custom fields for visitors, credentials, and cardholders functions. The group name ClearID is used to identify the custom fields associated with ClearID, and can be found in the Group name/Priority column.

IMPORTANT: ClearID custom fields should be used as read-only fields. These custom field values are populated and managed by ClearID. If you have existing custom fields, and the name and entity type matches the ClearID custom fields, ClearID will use the existing custom fields.

You can see the complete list for your organization in Config Tool. In the System task, click General settings > Custom fields.



NOTE: Only users with the privilege *Modify custom field definitions* can view custom fields.
Browse

- Granting user privileges for the ClearID plugin

4.8.1 | Modifying ClearID custom fields in Config Tool

You can modify Genetec ClearID™ custom fields in Config Tool so that they are displayed to specific groups or users. For example, you might display visit reason, registration code, expected arrival, and expected departure to a group that contains your security team or building reception team.

Before you begin

Make sure that the Genetec ClearID: Cardholder and credential changes are synchronized back to Security Center radio button is selected for the ClearID system, otherwise no custom fields are displayed.

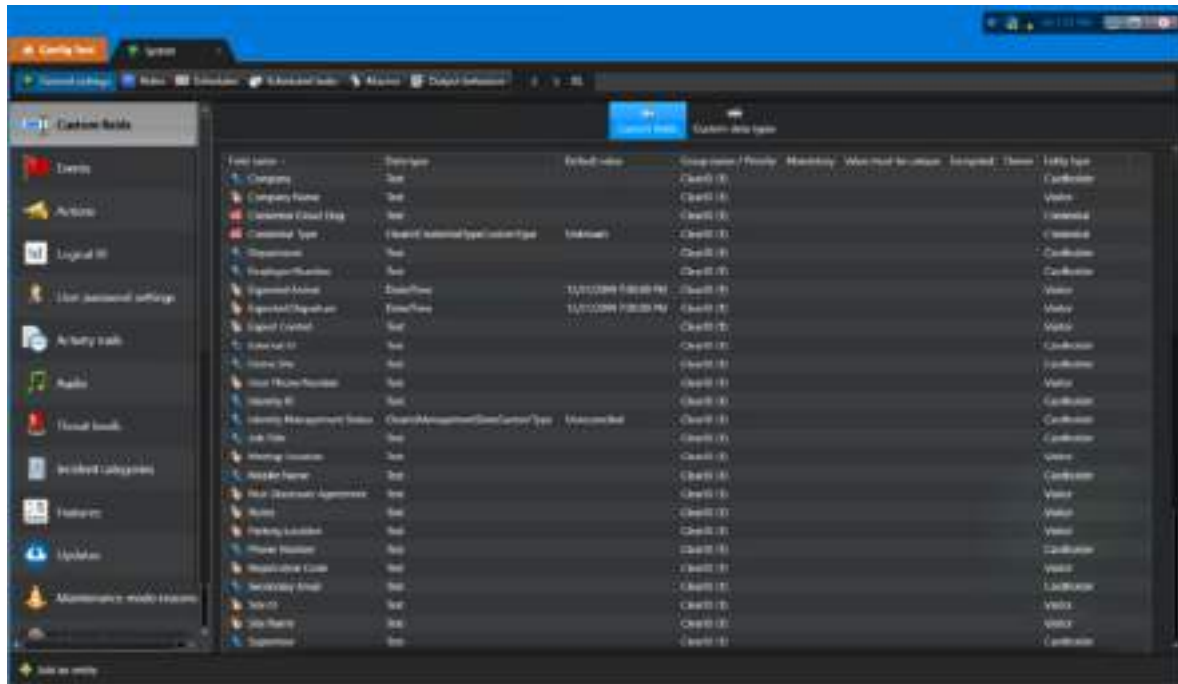
What you should know

Only users with the privilege to *Modify custom field definitions* can view custom fields.

- At least one identity must have been synchronized before any custom fields are displayed.

Procedure

1. In Config Tool, Open the System task.
2. Click Custom fields.



3. In the Custom fields tab, double-click a Field name to select the custom field that you want to modify.

4. In the Edit custom field dialog, make any changes that you require.

a. In the Definition section, make any changes that you require.

IMPORTANT: Do not select the Mandatory checkbox for custom fields. In ClearID, custom fields must not be mandatory or unique otherwise synchronization issues can occur.



b. In the Layout section, make any changes that you require.

For example, you could add a group name to categorize your custom fields, or you could remove a custom field from a group when a grouping is no longer applicable.

Genetec ClearID® User Guide
Displayed in the header

c. In the Security section, make any changes that you require.

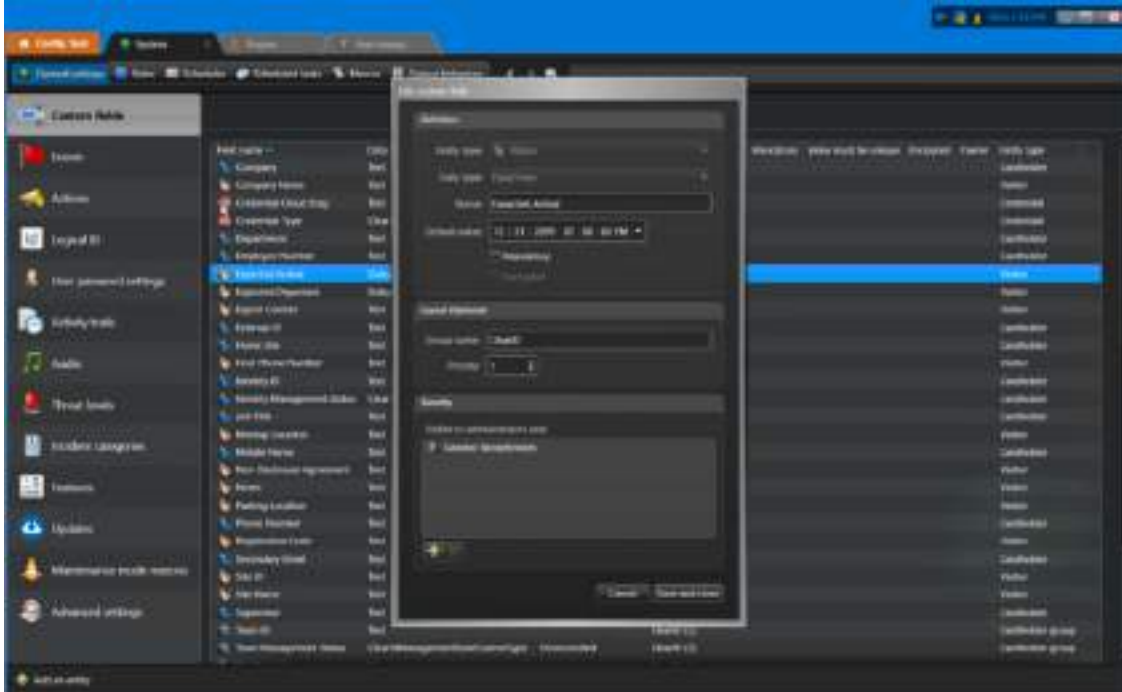
For example, you might add users or user groups in the Security section so that the custom field is displayed to them.

For information about user groups or custom fields, see [Creating user groups](#) or [About custom fields](#) on the TechDoc Hub.

d. Click Save and close.

Example

The following example shows the *Expected arrival* custom field. Using the Security section of the Edit custom field dialog, the Genetec Receptionists user group has been added so that the *Expected arrival* custom field can be displayed to members of the group.



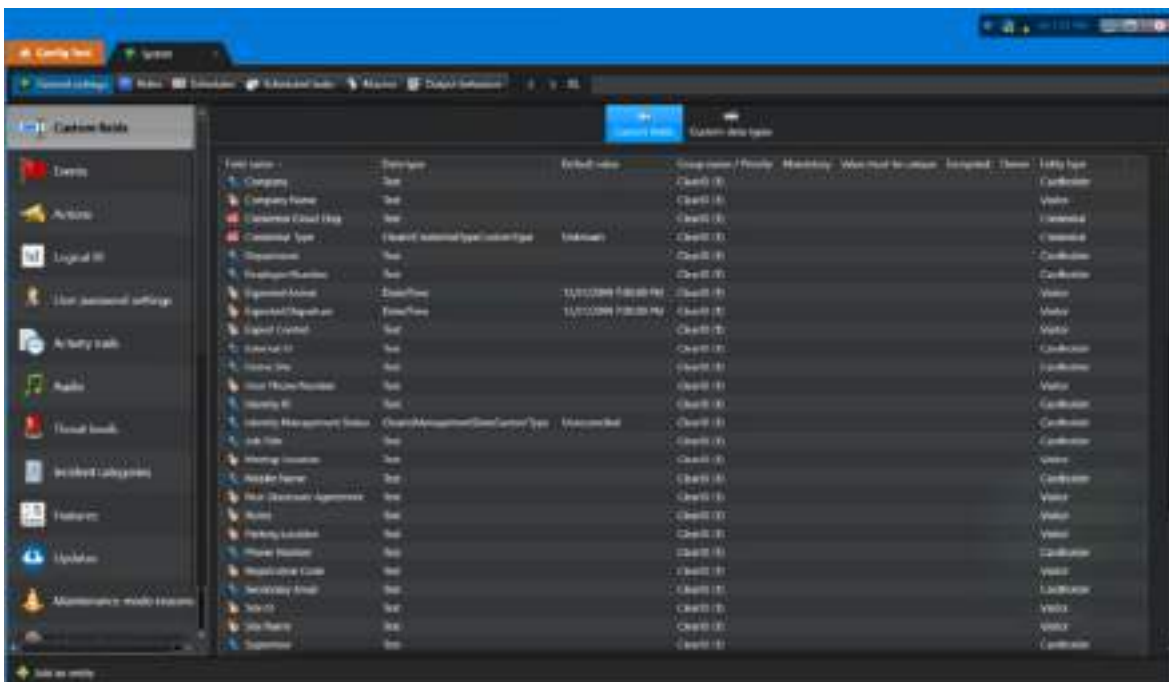
Parent topic: [About custom fields in ClearID](#)

Browse

- Custom fields not displayed in Security Desk
- Granting user privileges for the ClearID plugin

4.8.2 | Custom fields relationships

Use the following custom fields information to understand the relationship between Genetec ClearID™ identity field names and Security Center entity type fields.



Cardholder fields

Cardholder fields are used to synchronize cardholder information with an identity in ClearID.

Field name	Data type	Default value	Group name (And Priority)
Company	Text		ClearID (1)
Department	Text		ClearID (1)
Employee Number	Text		ClearID (1)
External ID	Text		ClearID (1)
Home Site	Text		ClearID (1)
Identity ID	Text		ClearID (1)
Identity Management Status	ClearIdManagementStateCustomType	Unreconciled	ClearID (1)
Job Title	Text		ClearID (1)
Middle Name	Text		ClearID (1)
Phone Number	Text		ClearID (1)
Secondary Email	Text		ClearID (1)
Supervisor	Text		ClearID (1)
Worker Type Code	Text		ClearID (1)
Worker Type Description	Text		ClearID (1)

Cardholder group fields

Cardholder group fields are used to synchronize cardholder group information with a role in ClearID.

- The Team ID represents the role ID in ClearID.
- The Team Management Status indicates whether ClearID is managing cardholders and credentials or not (managed by ClearID, not managed by ClearID, deleted by ClearID, or unreconciled).

Field name	Data type	Default value	Group name (And Priority)
Team ID	Text		ClearID (1)
Team Management Status	ClearIdManagementStateCustomType	Unreconciled	ClearID (1)

Credential fields

Credential fields are used by ClearID to keep the credentials up to date.

Field name	Data type	Default value	Group name (And Priority)
Credential Cloud Etag	Text		ClearID (1)
Credential Type	ClearIdCredentialTypeCustomType	Unknown	ClearID (1)

Visitor fields

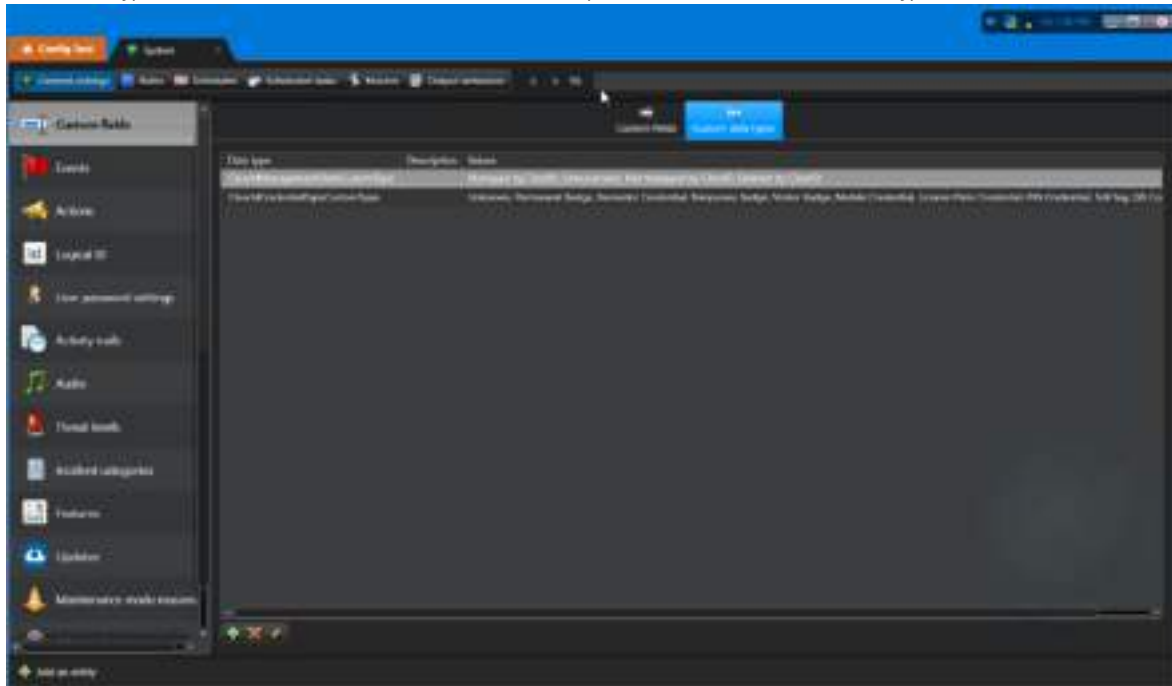
These visitor fields are used to synchronize visitor information.

Genetec ClearID™ User Guide Displayed in the header

Field name	Data type	Default value	Group name (And Priority)
Company Name	Text		ClearID (1)
Expected Arrival	Date and time	12/31/2099 7:00:00 PM	ClearID (1)
Expected Departure	Date and time	12/31/2099 7:00:00 PM	ClearID (1)
Export Control	Text		ClearID (1)
Host Phone Number	Text		
Meetup Location	Text		ClearID (1)
Non Disclosure Agreement	Text		ClearID (1)
Notes	Text		ClearID (1)
Parking Location	Text		ClearID (1)
Registration Code	Text		ClearID (1)
Site ID	Text		ClearID (1)
Site Name	Text		ClearID (1)
Visit Event Name	Text		ClearID (1)
Visit Reason	Text		ClearID (1)
Visitor ID	Text		ClearID (1)
Watchlist Status	Text		ClearID (1)

Custom data types

Custom data types are used for some custom fields to define the accepted values associated with the data types.



NOTE: All custom fields are labels used to define a property associated with a Security Center entity type that might be useful to an organization. The fields included in the description here are merely descriptive labels. All the custom data types might not be applicable to or used by ClearID.

Data type	Values
ClearIdManagementStateCustomType	Managed by ClearID, Unreconciled, Not managed by ClearID, Deleted by ClearID

Data type	Values
ClearIdCredentialTypeCustomType	Unknown, Permanent Badge, Biometric Credential, Temporary Badge, Visitor Badge, Mobile Credential, License Plate Credential, Pin Credential, Toll Tag, QR Code

Parent topic: [About custom fields in ClearID](#)

5 | Managing identities and users

5.1 | Creating identities in ClearID

From time to time, you might need to create an identity manually in Genetec ClearID™. For example, for an identity that isn't part of the usual mass import process or synchronization of identities using LDAP, One Identity, or API solutions.

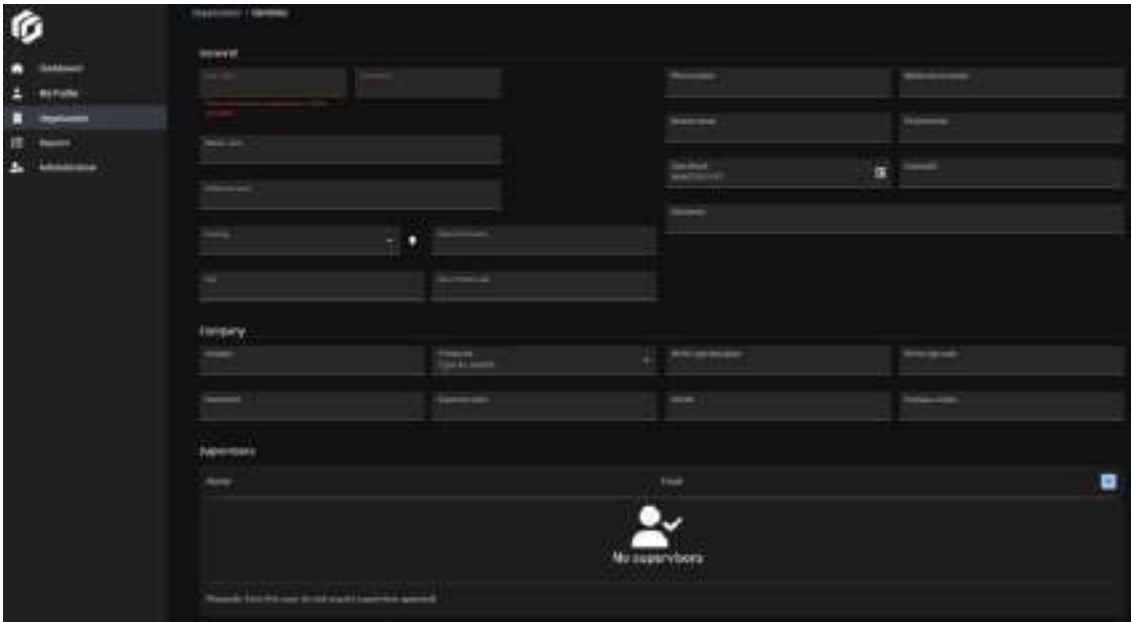
What you should know

Only an account administrator can create identities.

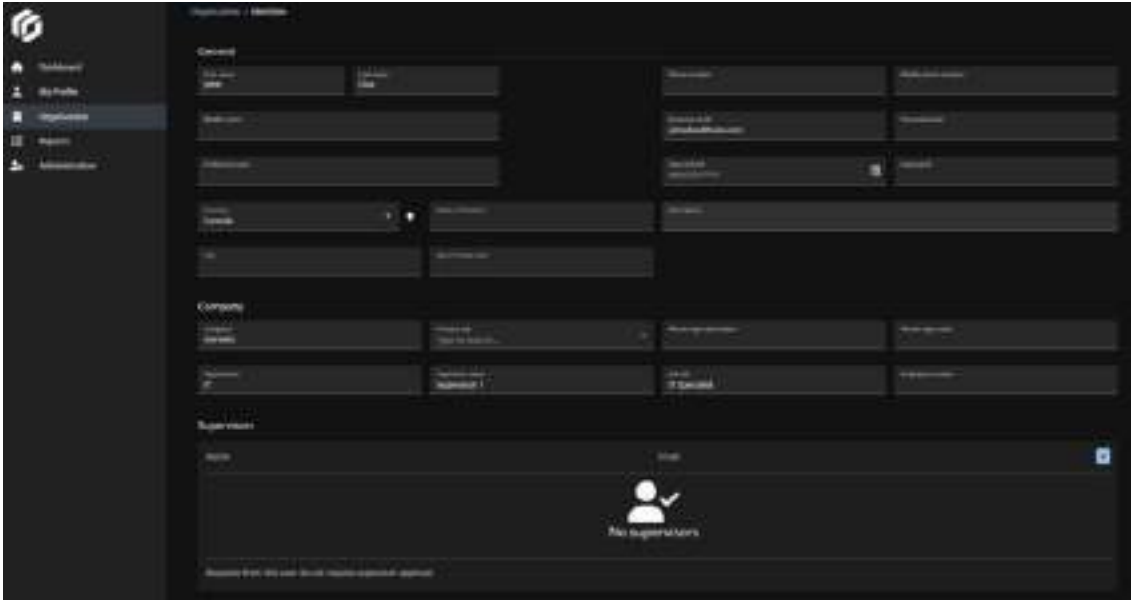
Account administrators can create an identity manually in the web portal when the identity isn't part of a mass import or synchronization of identities using LDAP, One Identity, or API solutions. For example, a *contractor*, *system integrator*, or other identities might be added manually.

Procedure

- 1. Click Organization > Identities.
- 2. Click Add an identity.



- 3. Complete the mandatory fields:
 - a. Enter a First name.
 - b. Enter a Last name.
 - c. Select a country from the list.
Tip: Enter the first letter of the country to jump to that part of the country list.
- 4. (Optional) Complete any additional fields that you require. For example:
 - a. Enter a Business email address.
 - b. Enter a Company name.
 - c. Enter a Department.
 - d. Enter a Supervisor name.
 - e. Enter a Job title.
 - f. Complete other fields as required.



5. Click Save to create the identity in Genetec ClearID™.

Example

Ocorreu um erro.

[Tente assistir o vídeo em \[www.youtube.com\]\(http://www.youtube.com\)](#) ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Grant the identity access to the web portal.
Browse

- Logging on to ClearID
- Viewing direct reports in ClearID

5.2 | Identity fields in ClearID

Use the following information to help you understand the identity fields that are used in Genetec ClearID™. The following table explains which fields are mandatory, which fields are used by Security Center, and which fields are available for use by provisioning rules.

ClearID identity fields	Type or format	Mandatory in ClearID	Pushed to Security Center	Security Center field name	Available in provisioning rules
Activation date	Date		✓	Activation	
Business email	Email		✓	Email address	
City	Text				
Company	Text		✓	Company	✓

Genetec ClearID®; User Guide

Displayed in the header

ClearID identity fields	Type or format	Mandatory in ClearID	Pushed to Security Center	Security Center field name	Available in provisioning rules
Country	ISO 3 Character	✓			✓
Date of birth	Date				
Department	Text		✓	Department	✓
Description	Text		✓	Description	✓
Display name	Text		✓	Entity name	
Employee number	Text		✓	Employee number	
Expiration date	Date		✓	Expiration	
Extended grant time required	True or False		✓	Use extended grant time	✓
External ID	Text		✓	External ID	✓
First name	Text	✓	✓	First name	
Home site	Unique ID		✓	Home site	✓
Identity ID	Unique ID		✓	Identity	
Job title	Text		✓	Job title	✓
Last name	Text		✓	Last name	
Middle name	Text		✓	Middle name	
Mobile phone number	Phone number				
Personal email	Email		✓	Secondary email	
Phone number	Phone number		✓	Phone number	
Provisioning attributes	List				✓
State/Province	Text				
Status	Active or Inactive	✓	✓	Status	✓
Supervisor name	Text		✓	Supervisor	✓
Supervisor(s)	List of identities				✓
Worker type code	Text			Worker type code	✓
Worker type description	Text		✓	Worker type description	✓
Zip code	Text		✓		

Browse

- [Configuring role-based access control policies in ClearID](#)
- [About custom identity fields in ClearID](#)

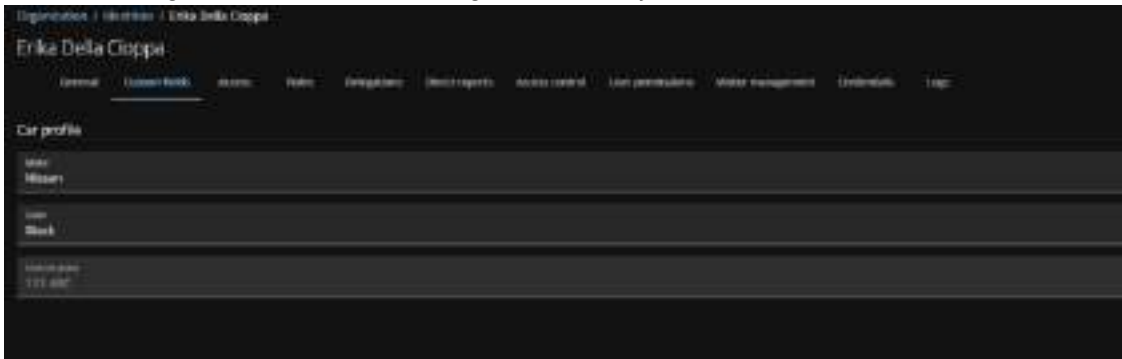
5.3 | About custom identity fields in ClearID

Custom fields are user-defined properties associated with identities in the Genetec ClearID™ web portal.

In Genetec ClearID™, custom identity fields add additional configurable information to identities, separate from the system's default identity fields. *Account administrators* create and manage these custom fields in the ClearID web portal. The custom fields can be manually populated in the identity profile or can be synchronized from an external data source. The custom fields can be synchronized to linked Security Center systems as needed.

NOTE: Select Synchronize custom field values with external systems to automatically synchronize the custom fields with Security Center. No prior setup is required, and custom fields can be populated by the *Account administrators* later.

Custom identity fields can include information such as vehicle profiles, employee types, worker schedules, and more for all identities in the ClearID portal. The custom fields are organized in sections and can be configured to be read-only.



Browse

- [Creating custom identity fields in ClearID](#)
- [Identity fields in ClearID](#)

5.4 | Creating custom identity fields in ClearID

To collect and store additional information about identities in the Genetec ClearID™ web portal, *Account administrators* can create custom fields and set them to synchronize with Security Center as needed.

Before you begin

Learn about custom identity fields.

What you should know

You must be an *Account administrator* to create custom identity fields.

Procedure

1. In the ClearID portal, click Administration > Custom fields.
2. Create a custom field section.
 - Custom field sections group related custom fields together to be displayed on identity profile pages.
 - a. Click Add custom field section.
 - b. On the New custom field section page, fill out the necessary fields.

Section ID

In the Section ID field, enter a unique ID for your custom field section.

IMPORTANT: The section ID is used for organization and troubleshooting purposes. This value cannot be changed later.

Display name

In the Display name field, enter a name for the custom field section. The name is displayed on identity profile pages.

- c. Click Save.

3. (Optional) Click  to edit a custom field section.
 - a. On the new page, edit the custom field section as needed:

Display name

Edit the selected section's display name.

Custom fields

Add, view, or edit custom fields within the selected custom field section.

Delete custom field section

Delete the selected custom field section.

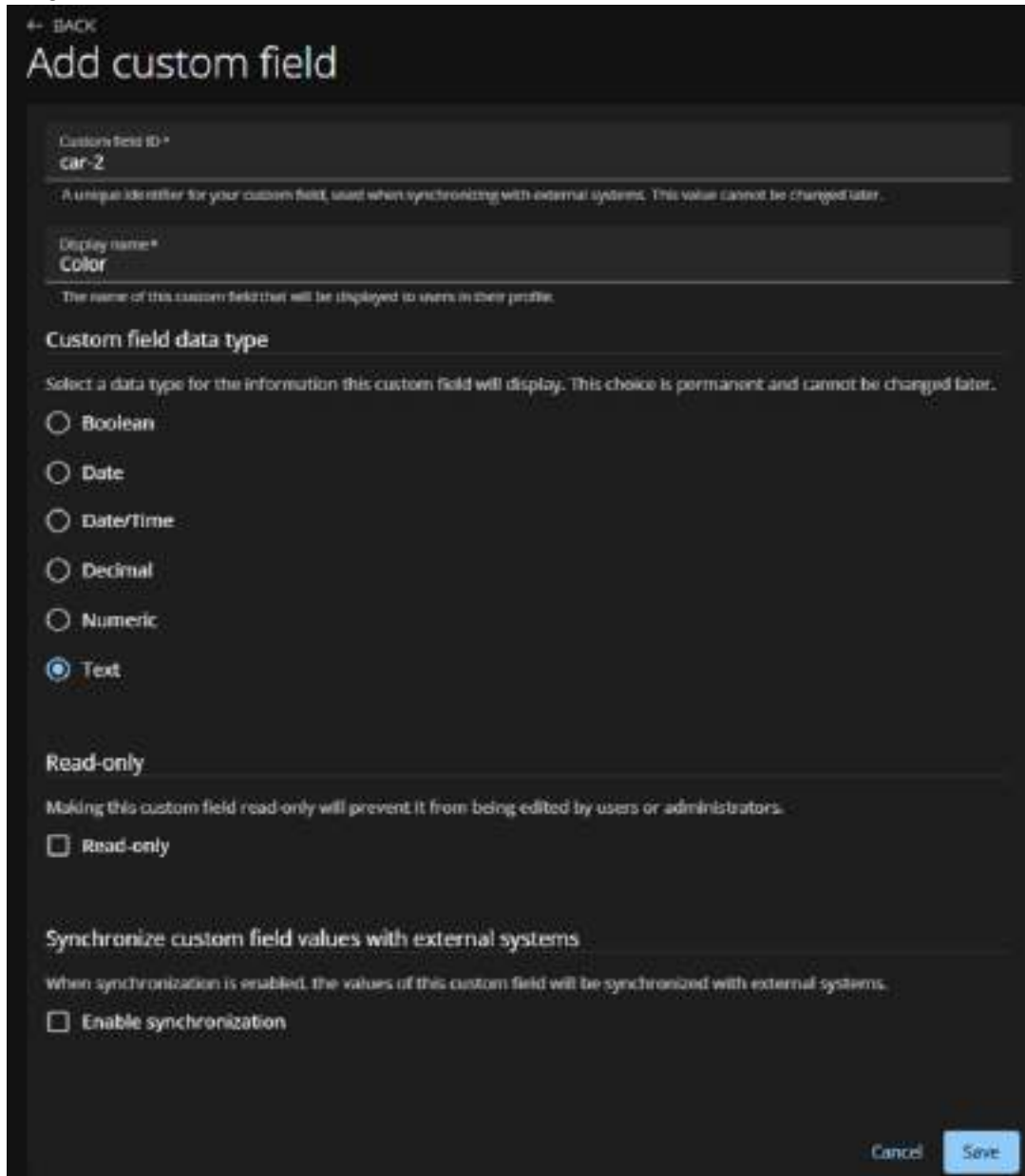
b. Click Save.

4. Add custom fields to the custom field section.

a. Click  to edit the custom field section.

b. Click Add custom field.

c. Configure the custom field as needed:



Custom field ID

In the Custom field ID field, enter a unique ID for the custom field.

Display name

In the Display name field, enter a name for the custom field.

Custom field data type

In the Custom field data type section, select the data type for the information displayed in the custom field.

Read-only

In the Read-only section, choose whether to restrict users and administrators from editing the custom field on the identity profile page.

NOTE: The read-only feature is intended to be used when synchronizing ClearID with an external source.

Synchronize custom field values with external systems

In the Synchronize custom field values with external systems section, choose whether to synchronize the custom field with Security Center.

d. Click Save.

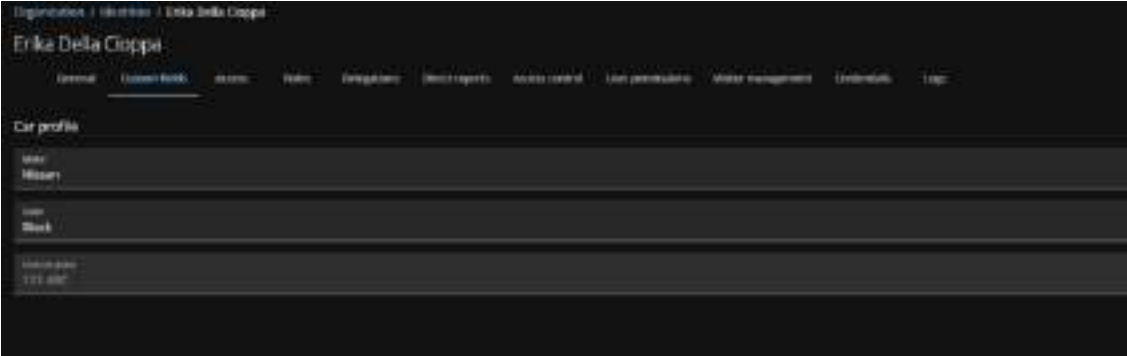
5. (Optional) Create a custom field that will not be displayed on the identity profile page.

NOTE: These custom fields will still synchronize with Security Center if Synchronize custom field values with external systems is selected.

- a. In the ClearID portal, click Administration > Custom fields.
- b. Click Add custom field.
- c. Repeat step 4 c.
- d. Click Save.

Results

You can view and fill custom fields by navigating to Organization > Identities > Identity > Custom fields.



Browse

- [About custom identity fields in ClearID](#)

5.5 | Granting additional permissions for identities and roles in ClearID

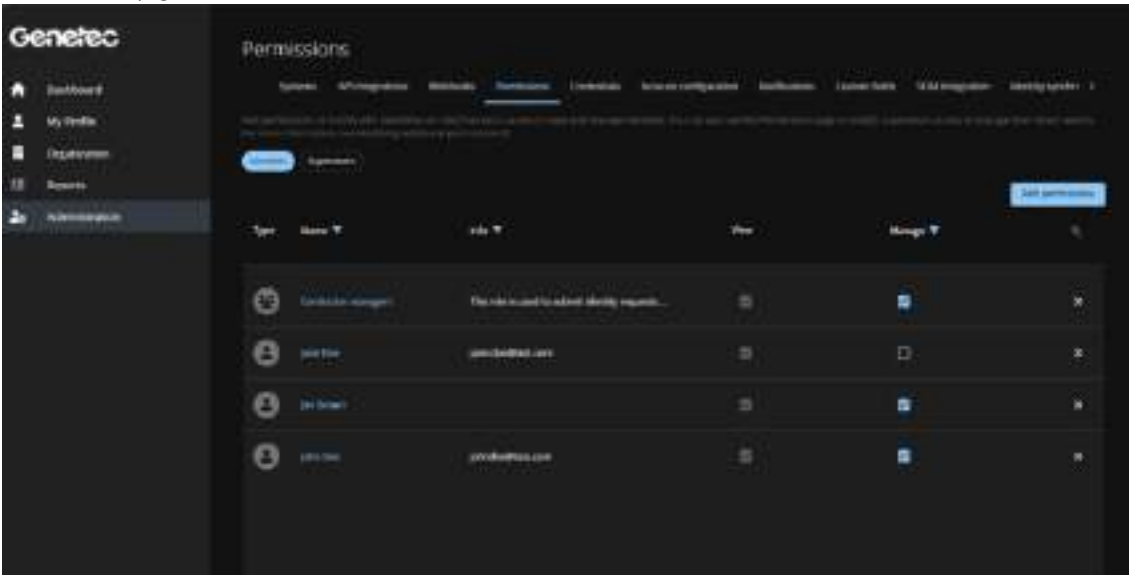
Some organizations require more access than the default permissions provided for a Genetec ClearID™ user. You can grant identities and roles additional permissions so that they can view or manage all identities in the system.

What you should know

Only an account administrator can add identity and role permissions.

Procedure

1. From the Home page, click Administration > Permissions.



2. Click Add permissions.

The screenshot shows the 'Permissions' dialog box with the 'Identities' tab selected. The 'Identities' field contains a search bar with 'jack' entered and a 'Type to search...' placeholder. Below the search bar, it shows '1 / 30'. The 'Permissions' section has two checkboxes: 'View' (checked) and 'Manage' (unchecked). Below this is a 'Reason' field with a placeholder 'Access required to view and manage identities'. At the bottom, there are 'Cancel' and 'Add identities' buttons.

3. In the Permissions dialog, select either Identities or Roles to add the permissions you require.

4. If you selected Identities, complete the following:

- In the Identities field, enter one or more identities that you want to grant extra access.
A maximum of 20 identities per request is supported.
- In the Permissions section, select the permissions you want to add to the identities selected earlier.

View

Access to view identities is granted by default.

Manage

Select the Manage checkbox to add permissions to modify identities.

NOTE: If you make updates to identities that are synchronized with an external data source, the synchronization can overwrite your manage permission changes. Manage permissions are useful for identities being manually entered into ClearID.

- In the Reason field, enter a reason why the access was added.

This screenshot is similar to the first one, but the 'Manage' checkbox is now checked. The 'Reason' field contains the text 'Access required to view and manage identities'. The 'Identities' field still shows '1 / 30'.

5. If you selected Roles, complete the following:

- In the Roles field, enter one or more roles that you want to grant extra access.
A maximum of 20 roles is supported.
- In the Permissions section, select the permissions you want to add to the roles selected earlier.

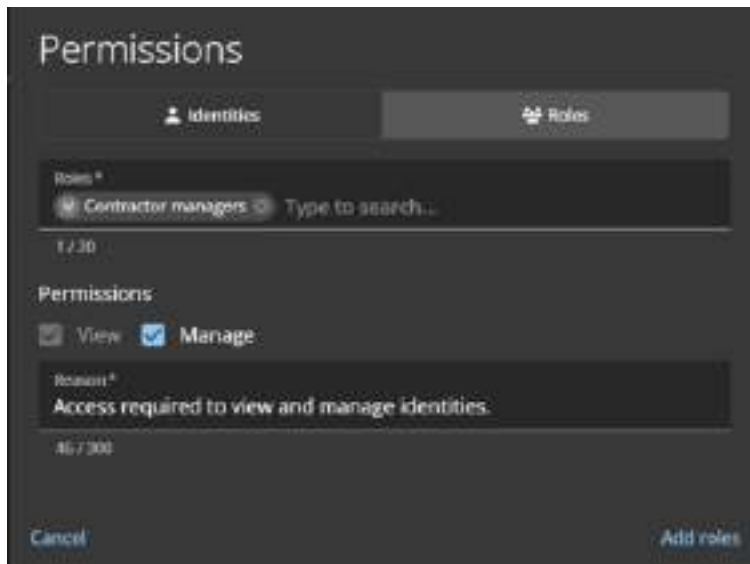
View

Access to view identities is granted by default.

Manage

Select the Manage checkbox to add permissions to modify identities.

- In the Reason field, enter a reason why the access was added.



6. Click Add identities or Add roles to submit your changes.

Results

The specified identities or roles now have the required permissions to view and manage identities.

After you finish

View identities or Modify identities.

Browse

- Transferring direct reports in ClearID

5.6 | Granting additional permissions for supervisors in ClearID

Some organizations require more access than the default permissions provided for a Genetec ClearID™ supervisor. You can grant supervisors additional permissions so that they can manage their direct reports.

What you should know

Only an account administrator can grant supervisors access to manage their direct reports.

Procedure

1. From the Home page, click Administration > Permissions.
2. Click the Supervisors tab.
3. Select the Grant supervisors access to manage their direct reports checkbox to grant supervisors the required permissions to update General identity profile information and Access Control settings.



4. Click Save to confirm the changes.

Results

Supervisors now have more control to manage their direct reports. They can now modify General identity information fields and Access control settings.

After you finish

Modify your direct reports information.

Browse

- Transferring direct reports in ClearID

5.7 | Viewing additional permissions in ClearID

You can use the Permissions page to review who (identities or roles) has extra access to view and manage identities. You can also use the Permissions page to verify if supervisors have extra access to manage their direct reports.

Before you begin

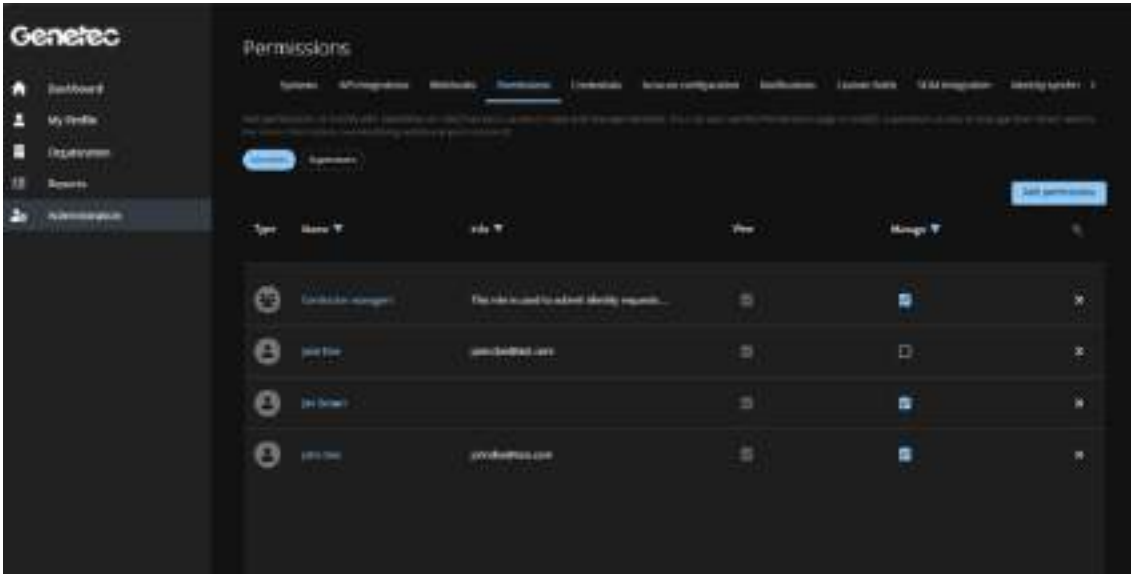
- Grant additional permissions for identities and roles.
- Grant additional permissions for supervisors.

What you should know

Only an account administrator can view identity and role permissions or supervisor permissions.

Procedure

1. From the Home page, click Administration > Permissions.



- In the Type column, each row has a visual identifier to signify the entry as either a role or an identity.
2. In the Name column, click  to filter results by identity or role name.
 3. In the Info column, click  to filter results by an email address, or enter words to search for in the permission information.
 4. In the Manage column, click  to filter results by permission. For example, to see which identities have View and Manage permissions.
 5. (Optional) Click Clear filters () to reset filters and restore the default page view.
 6. (Optional) Click the Supervisors tab to verify if supervisors have access to manage their direct reports.



After you finish

Modify additional permissions.

5.7.1 | Modifying additional permissions in ClearID

You can use the Permissions page to modify who (identities or roles) has extra access to view and manage identities. You can also use the Permissions page to modify supervisors access to manage their direct reports.

Before you begin

[View additional permissions.](#)

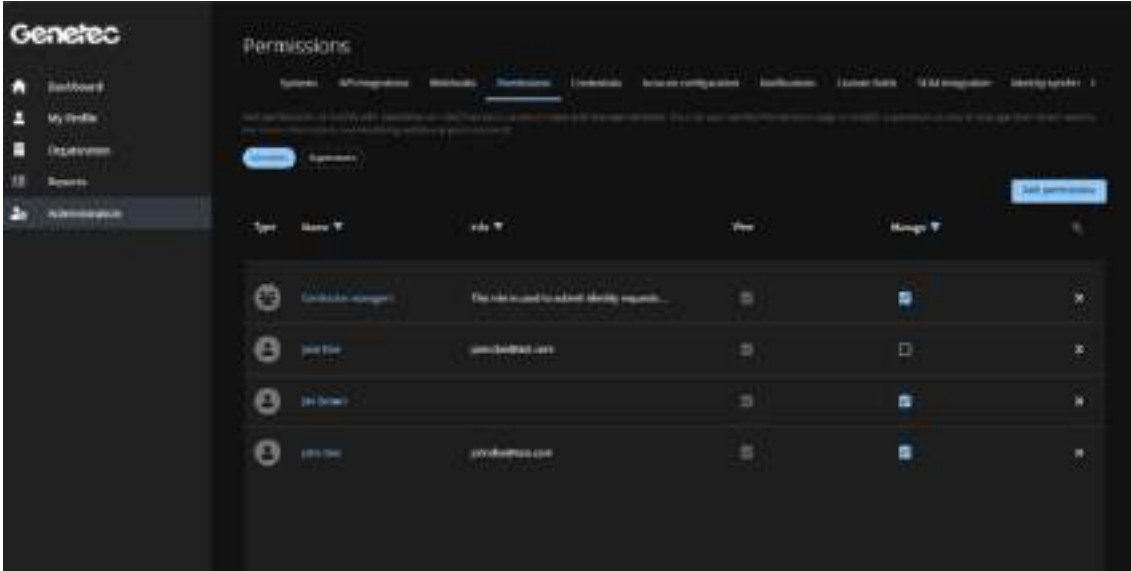
What you should know

Only an account administrator can modify identity and role permissions.

Procedure

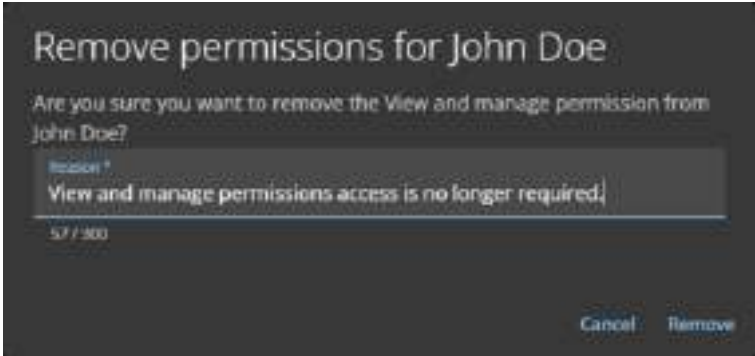
To modify identity and role permissions:

- 1. From the Home page, click Administration > Permissions.



In the Type column, each row has a visual identifier to signify the entry as either a role or an identity.

- 2. In the Name column, click to filter results by identity or role name.
- 3. In the Info column, click to filter results by an email address, or enter words to search for in the permission information.
- 4. In the Write column, click to filter results by permission. For example, to see which identities have Read and Write permissions.
- 5. (Optional) Click Clear filters () to reset filters and restore the default page view.
- 6. (Optional) In the Write column, select or clear the check box next to an identity or role to add or remove their Write access.
 - a. Click Save to submit your changes.
- 7. (Optional) Click the next to an identity or role to remove extra permissions (Read and Write) that are no longer required.



- a. Enter a Reason.
- b. Click Remove.

To modify supervisor permissions:

- 1. (Optional) Click the Supervisors tab to modify supervisor permissions.



- a. Make the changes that you require and click Save.

Parent topic: [Viewing additional permissions in ClearID](#)

5.8 | Viewing identities in ClearID

You can view identities in Genetec ClearID™ to check their access control status, general identity information, or verify if they have any supervisors specified.

Before you begin

[Create your identities.](#)

What you should know

Only account administrators or identities or roles with the required permissions can view identities.

Procedure

1. From the Home page, click Organization > Identities.
2. Select an option from the drop-down menu to display the identities that you require. Choose one of the following:
 - Active**
Displays active identities.
 - Inactive**
Displays inactive identities.
 - All**
Displays all active and inactive identities.
3. In the Search field, enter some search criteria and press enter.
4. Select an identity from the list to view the identity details.

The screenshot shows the 'Fred Smith' user profile page in the Genetec ClearID system. The page has a dark theme and a top navigation bar with tabs: General, Access, Roles, Delegations, Direct reports, Access control, User permissions, Visitor management, Credentials, and Logs. The 'General' tab is selected. The profile includes a profile picture, a status indicator (Active), and various fields for personal and professional information. A 'Deactivate this identity' button is visible in the top right. The 'Supervisors' section shows no supervisors are assigned.

Organization: P Identities: P Fred Smith

Fred Smith

General Access Roles Delegations Direct reports Access control User permissions Visitor management Credentials Logs

General Active

Personal Information

First name: Fred	Last name: Smith	Phone number:	Mobile phone number:
Middle name:		Business email: fred.smith@test.com	Personal email:
Preferred name: Fred Smith		Date of birth: MM/DD/YYYY	Personal ID:
Country: Canada	State or Province:	Description:	
City:	Zip or Postal code:		

Company

Company:	Primary title: Types to search...	Worker type description:	Worker type code:
Department:	Department name:	Job title: Contractors Manager	Employee number:

Supervisors

Name	Email
No supervisors	

Requests from this user do not require supervisor approval.

5. In the General tab, review the identity details including any associated supervisors, and the identity status (active or inactive).
6. (Optional) Additional tabs are also provided to review other details and options associated with the selected identity as follows:

Custom fields

Custom fields associated with the selected identity.

Access

Access associated with the selected identity.

Roles

Roles associated with the selected identity added by a provisioning policy or manually added.

Delegations

Delegations associated with the selected identity.

Direct reports

Reportees associated with the selected identity.

Access control

Access control associated with the selected identity including extended grant time, cardholder activation, provisioning attributes, and associated cardholders.

User permissions

Web portal user or administrator access permissions associated with the selected identity.

Visitor management

List of sites where selected identity can invite visitors.

Credentials

Synchronized credentials associated with the selected identity.

Tip: A credential synchronization can also be performed at the individual identity level. Select an identity then click the Credentials tab and click Synchronize.

Logs

Identity event logs for activities associated with the selected identity.

After you finish

[Modify your identities.](#)

5.9 | Modifying identities in ClearID

After you have added identities, you might need to modify the identity details. You can deactivate or activate an identity, or modify identity details after a change in job title, department, company, supervisors, personal information, and so on.

Before you begin

[Create your identities.](#)

What you should know

- Only account administrators, supervisors, or identities or roles with the required permissions can modify identities.
- Only account administrators can delete identities.

IMPORTANT: If you make updates to identities that are synchronized with an external data source, your changes can be overwritten by the synchronization.

Procedure

1. From the Home page, click Organization > Identities.
2. Select an option from the drop-down menu to display the identities that you require. Choose one of the following:

Active

Displays active identities.

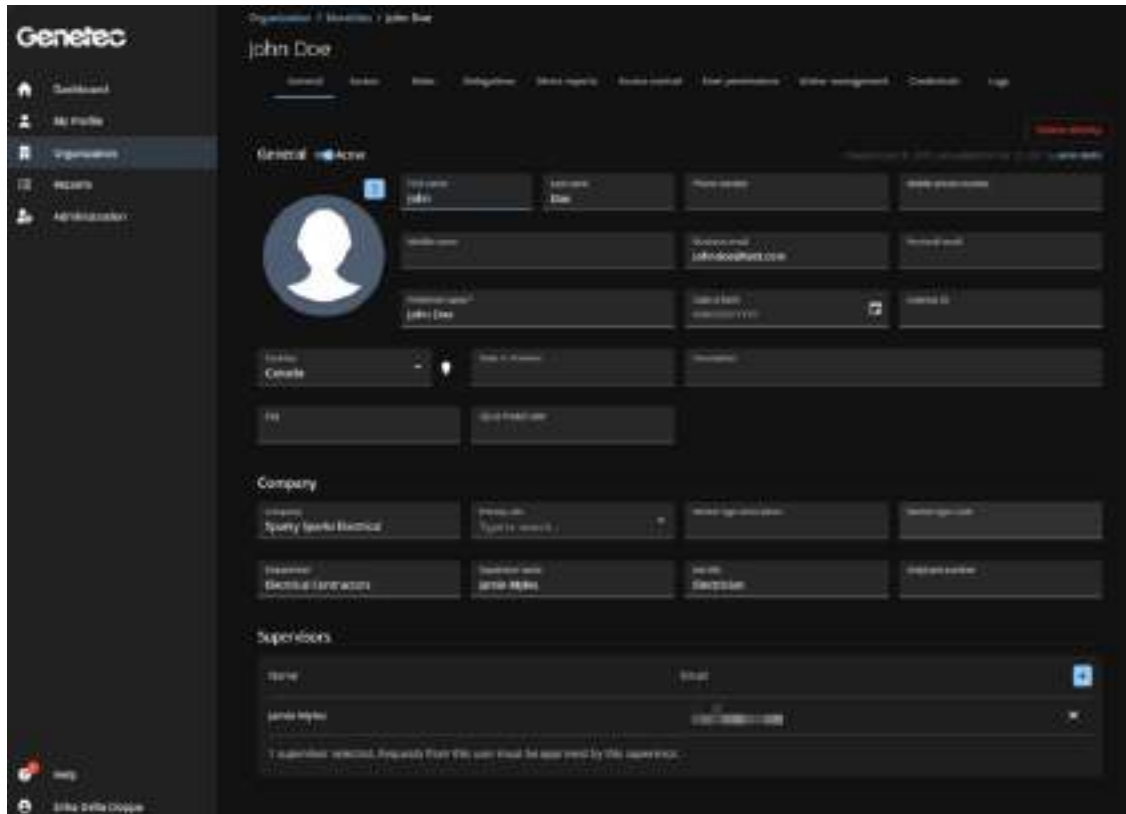
Inactive

Displays inactive identities.

All

Displays all active and inactive identities.

3. In the Search field, enter your search criteria and press enter.
4. Select an identity from the list to view the identity details.



5. Modify any settings, or deactivate or activate an identity as required.
For example, after a change in job title, department, company, supervisors, personal information, and so on.
6. Click Save to submit your changes.

After you finish

Delete Identities that are obsolete or no longer required.

Browse

- Synchronizing ClearID identity pictures with Security Center

5.10 | Deleting identities in ClearID

An administrator can delete identities that have become obsolete or are no longer required. For example, when a person leaves the organization, or when an identity was created in error.

Before you begin

You must have identities that were previously created, that are now ready for deletion.

What you should know

Only account administrators can delete identities.

- Search functions and audit trail information are retained after an identity is deleted so that you can check when the person had their access removed and the reason.
- The identity is also removed from all associated approver, owner, or manager lists or identity requests if applicable.

Procedure

1. From the Home page, click Organization > Identities.
2. Select an option from the drop-down menu to display the identities that you require. Choose one of the following:

Active

Displays active identities.

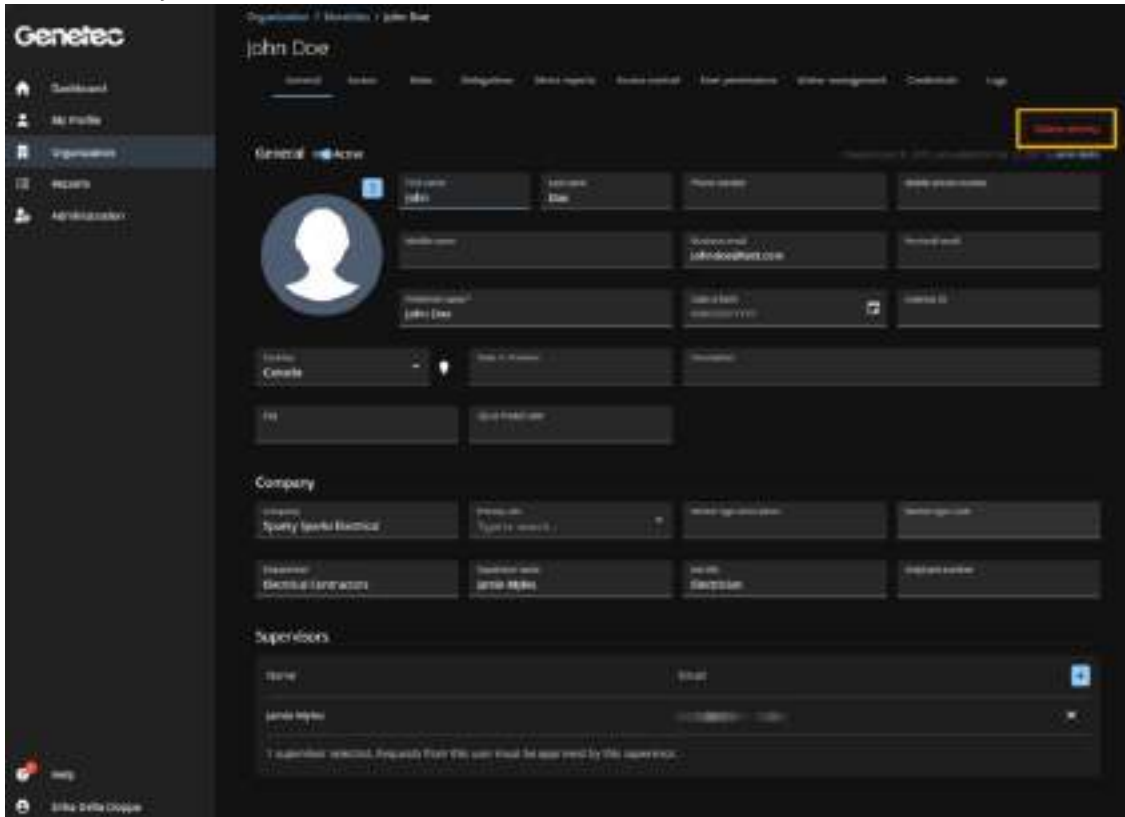
Inactive

Displays inactive identities.

All

Displays all active and inactive identities.

3. In the Search field, enter your search criteria and press enter.
4. Select an identity from the list to view the identity details.
5. Click Delete identity.



6. Click Remove to confirm the deletion.

5.11 | Synchronizing ClearID identity pictures with Security Center

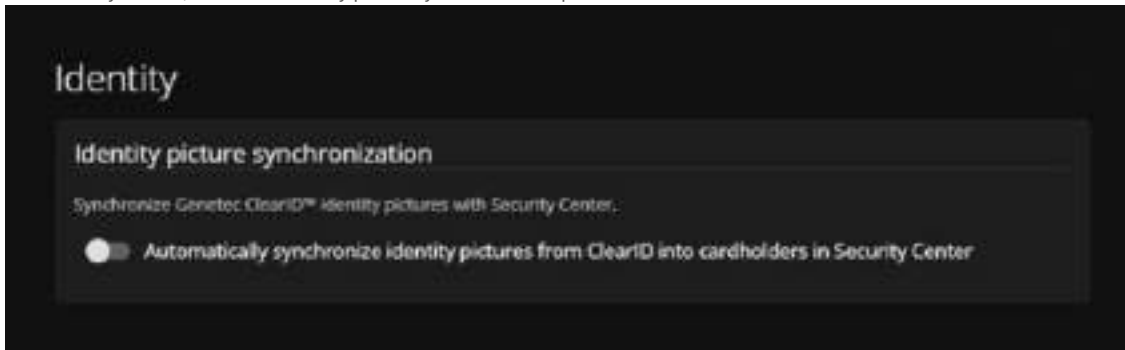
To manage identity and cardholder pictures in one place, *Account administrators* can set Genetec ClearID™ as the preferred data source for all cardholder pictures in Security Center.

Before you begin

Ensure that Security Center is connected to ClearID.

Procedure

1. In the ClearID web portal, click Administration > Account configuration.
2. In the Identity section, turn on the Identity picture synchronization option.



3. ClearID identity pictures are automatically synchronized with Security Center, replacing existing cardholder pictures. If updates to cardholder pictures are made directly through Security Center after Identity picture synchronization is turned on, ClearID overrides these updates.
NOTE: If no identity pictures are found in ClearID when identity picture synchronization is first turned on, cardholder pictures in Security Center aren't replaced.

Browse

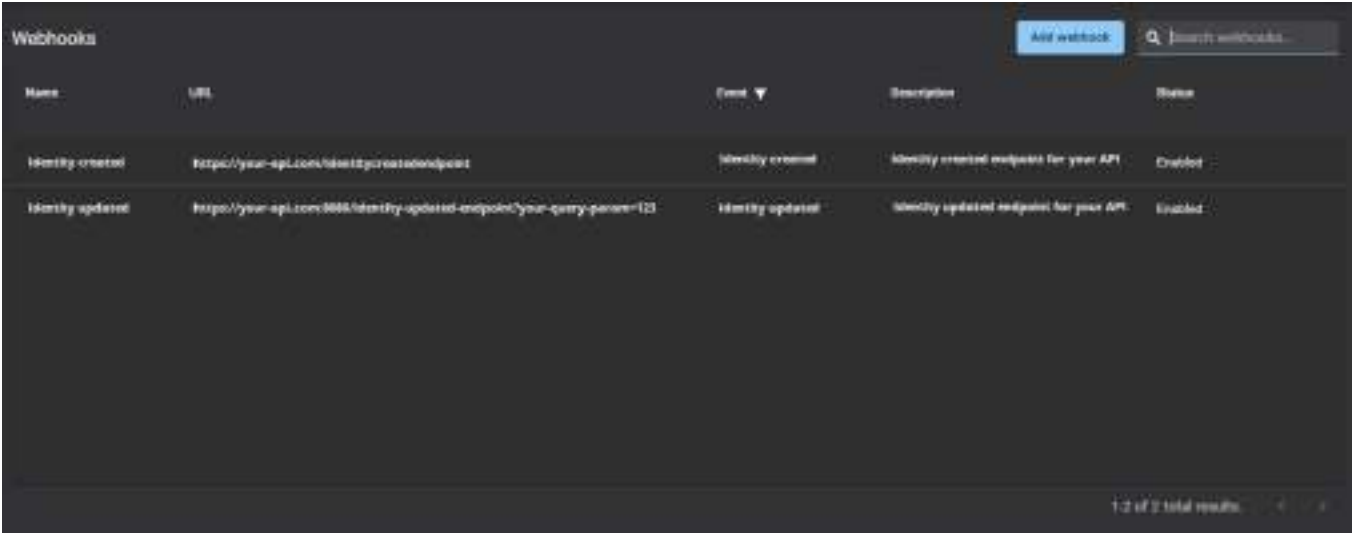
- Connecting Security Center to ClearID
- About cardholder and identity relationships
- Reviewing cardholders and identities information in ClearID
- Modifying identities in ClearID

5.12 | About webhooks in ClearID

A webhook is a user-defined HTTP callback. A webhook can be triggered by an event in a web application and can be used to send data or notifications to a third-party Application Programming Interface (API).

Webhooks in Genetec ClearID™

In ClearID, webhooks can be created and used to notify third-party APIs when specific events occur.



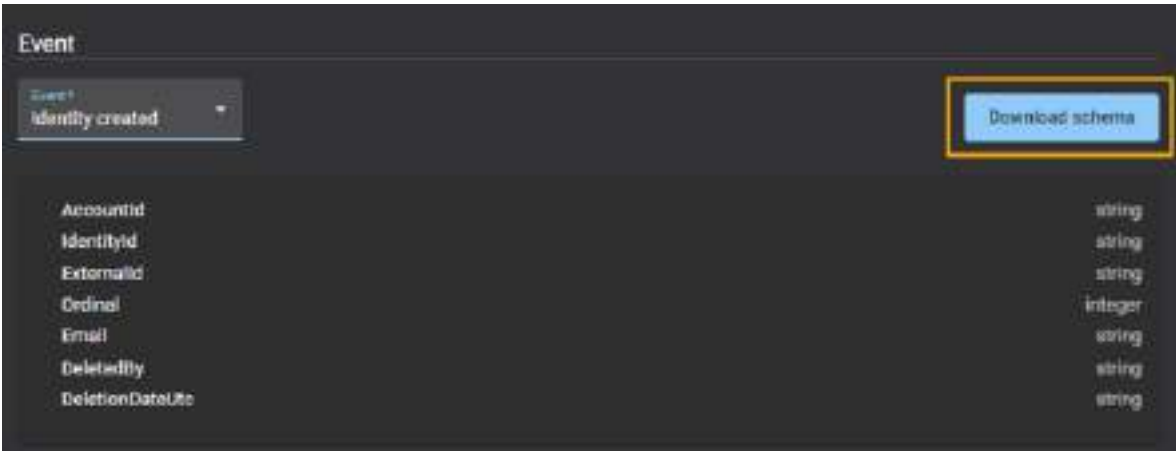
For example, an email notification with a link to detailed information about an identity could be sent when an Identity updated event occurs, or if you require other stakeholders to be notified after an Identity requests created or Identity requests updated event occurs.

Webhook processing

After the webhook is created, the webhook service listens for a subset of specified events coming from other ClearID services. When the specified event occurs the webhook service notifies the API specified in the Webhook details section URL field.

Webhook event schemas

The schema describes the object that is sent through the webhook and the contents of the schema vary depending on the event type specified. The webhook event schema can be downloaded from the Event section of the webhook to help understand the data structure of the events so that they can be retrieved and processed correctly on the user's side of the webhook integration.



For more information about downloading the schema, see [Creating webhooks in ClearID](#).

Webhook logs

Third-party API owners can use webhook logs to verify the status of every HTTP callback request sent to the third-party URL and to troubleshoot unreceived webhooks or other associated issues. For example, sender issues, receiver issues, and so on.

Webhook logs include the following:

Callback date

When the callback was sent (includes date range filters).

URL

The URL used to forward the webhook event notification to the relevant third-party API (program or application).

Response

The response state indicates whether the HTTP callback was successfully received by third-party API or not. For example, accepted, bad request, internal server error, and so on.



Callback date	URL	Response
Last 365 days		
March 14, 2022 at 1:07 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
March 4, 2022 at 9:06 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
March 4, 2022 at 1:10 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
March 3, 2022 at 10:17 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
March 2, 2022 at 3:57 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
March 2, 2022 at 10:06 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
February 28, 2022 at 4:13 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
February 24, 2022 at 1:16 PM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
February 21, 2022 at 3:36 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request
February 9, 2022 at 10:54 AM	https://your-api.com:8080/identity-updated-endpoint?your-query-param=123	Bad Request

NOTE: The webhook Logs section is only displayed at the end of the webhook details after the first callback has occurred.

5.13 | Creating webhooks in ClearID

You can create webhooks in Genetec ClearID™ to integrate with third-party solutions APIs so that you can notify interested parties when specific events occur.

Before you begin

[Learn about webhooks.](#)

What you should know

- Only an account administrator can create webhooks in ClearID.
- External organizations are responsible for developing their own third-party solution APIs (programs or applications) that consume ClearID webhook HTTP callback notifications.

Procedure

- From the Home page, click Administration > Webhooks.
- Click Add webhook.

← BACK

Add webhook

General

Name *

Description

☒ Enabled

Webhook details

URL *

Secret

Additional headers

Name	Value
No additional headers found	

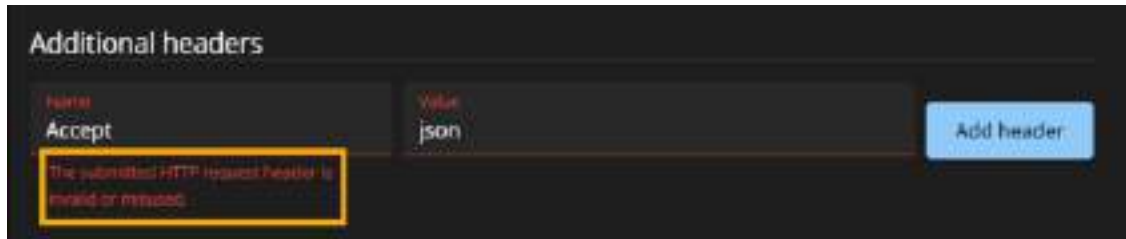
Add header

Event

Event *

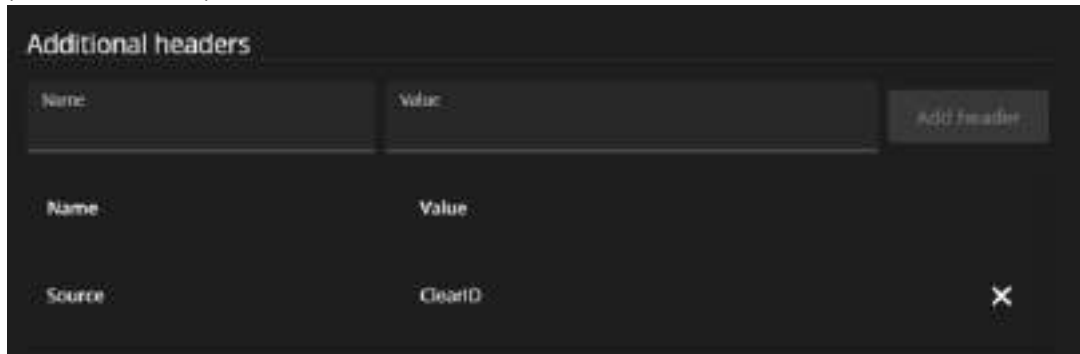
Download schema

3. In the General section, complete the fields:
 - a. (Optional) Select the Enabled checkbox to enable the webhook.
NOTE: When the webhook is *disabled*, the HTTP callback doesn't happen.
 - b. In the Name field, enter a meaningful Name so that you can easily identify your webhook later on.
For example, Identity updated or Identity requests created webhook and so on.
 - c. In the Description field, enter a Description that describes the purpose of the webhook.
For example, what the webhook is for, and what API (program or application) it notifies when events occur.
4. In the Webhook details section, complete the fields:
 - a. Enter a valid HTTPS:// URL for your API (program or application).
URLs can include ports and query parameters as follows:
 - Example 1: `https://my-api.com/identityupdatedendpoint`
 - Example 2: `https://my-api.com:8080/identity-updated-endpoint?my-query-param=123`This URL is used to forward the webhook event notification to the relevant third-party API (program or application).
NOTE: Your organization is responsible for providing the URL that you want the webhook event notifications forwarded to.
 - b. (Optional) Enter the Secret (App key) if required by the third-party API.
The secret (App key) is used to authenticate communications between the ClearID webhook and your organizations third-party API.
5. (Optional) In the Additional headers section, complete the fields:
Extra custom HTTP headers can be added in the HTTP callback request. These custom headers can be used by the third-party API on the user's side of the integration.
NOTE: If you enter an invalid or reserved header, the following message is displayed The submitted HTTP request header is invalid or misused.



- a. Enter the header parameter Name.

For example, if you had one event coming from multiple sources, extra HTTP request headers could be used to specify where event is coming from (ClearID or external API).



- b. Enter the header parameter Value.

- c. (Optional) Click Add header to add extra HTTP request headers as required.

For example, if your API is expecting or requires a specific set of headers (Host, Origin, Language, and so on).

- d. (Optional) Click  to remove any headers that are no longer required.

6. In the Event section, configure the settings you require:

- a. From the Event list, select an event that you want this webhook to listen for.

- b. Click Download schema and follow your browser prompts.

Best Practice: Use the downloaded schema information to understand the data structure of the events so that they can be retrieved and processed correctly on the user's side of the integration.

The following example shows an extract from a schema-identitycreated.json file:

Code

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "IdentityDeletedCallbackModel",
  "type": "object",
  "additionalProperties": false,
  "required": [
    "AccountId",
    "IdentityId",
    "DeletedBy",
    "DeletionDateUtc"
  ],
  "properties": {
    "AccountId": {
      "type": "string",
      "description": "The account id for which this identity is member of.",
      "minLength": 1
    },
    "IdentityId": {
      "type": "string",
      "description": "A unique id to identify the identity.",
      "minLength": 1
    },
    "ExternalId": {
      "type": [
        "null",
        "string"
      ],
      "description": "External ID"
    },
    "Ordinal": {
      "type": [
        "integer",
        "null"
      ],
      "description": "Commit ordinal in the storage.",
      "format": "int64"
    },
    "Email": {
      "type": [
```



```
"null",  
"string"  
],
```



7. Click Save.

Results

Your webhook is now configured to integrate with a third-party API (program or application) to notify interested parties when specific events occur.

After you finish

Using the downloaded schema, configure your third-party API to receive and process the webhook notifications.

5.13.1 | Modifying webhooks in ClearID

After you have created your webhooks, you might need to modify the webhook details. You can deactivate or activate a webhook, and modify the webhook details or event type if required.

Before you begin

[Create your webhooks.](#)

What you should know

Only an account administrator can modify webhooks in Genetec ClearID™.

Procedure

1. From the Home page, click Administration > Webhooks.
2. Select the webhook that you want to modify.
Tip: If the list is long, use the Search field to find the webhook that you require.
3. In the General section, modify the fields as required.
 - a. (Optional) Move the Enabled slider to enable or disable the webhook.

NOTE: When the webhook is *disabled*, the HTTP callback does not happen.
4. In the Webhook details section, modify the fields as required:
5. (Optional) In the Additional headers section, modify the fields as required:
6. In the Event section, modify the settings as required.
7. Click Save.

Parent topic: [Creating webhooks in ClearID](#)

5.14 | Viewing webhook logs in ClearID

To troubleshoot unreceived webhooks or other associated issues, third-party Application Programming Interface (API) owners can use the webhook logs to verify the status of every HTTP callback request sent to the third-party URL.

Before you begin

[Create your webhooks.](#)

What you should know

- Only an account administrator or third-party API owner can view webhook logs in Genetec ClearID™.
- The webhook Logs section is only displayed at the end of the webhook details after the first callback has occurred.

Procedure

1. From the Home page, click Administration > Webhooks.
2. Select the webhook that you want to troubleshoot.
Tip: If the Webhooks list is long, you can use the Search field to find the webhook that you require.
3. In the Logs section Callback date column, click  to select a specified range or use the Date range picker to specify your own range.
NOTE: The callback data range time period is limited to a maximum of 1 year and the callback information is displayed in reverse chronological order.
The following image shows callback logs containing *Accepted* responses.

Logs		
Callback date 	URL	Response
Last 365 days		
May 2, 2022 at 3:16 PM	https://your-api.com/identitycreatedendpoint	Accepted
April 26, 2022 at 5:40 PM	https://your-api.com/identitycreatedendpoint	Accepted
April 12, 2022 at 4:18 PM	https://your-api.com/identitycreatedendpoint	Accepted
March 28, 2022 at 3:23 PM	https://your-api.com/identitycreatedendpoint	Accepted
March 28, 2022 at 9:47 AM	https://your-api.com/identitycreatedendpoint	Accepted
March 25, 2022 at 10:22 AM	https://your-api.com/identitycreatedendpoint	Accepted
March 25, 2022 at 5:18 AM	https://your-api.com/identitycreatedendpoint	Accepted
March 25, 2022 at 4:49 AM	https://your-api.com/identitycreatedendpoint	Accepted
March 24, 2022 at 10:31 AM	https://your-api.com/identitycreatedendpoint	Accepted
March 24, 2022 at 9:28 AM	https://your-api.com/identitycreatedendpoint	Accepted
1-10 of 58 total results. < >		

The following image shows callback logs containing *BadRequest* responses.

Logs		
Callback date 	URL	Response
Last 365 days		
March 14, 2022 at 1:07 PM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
March 4, 2022 at 3:05 PM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
March 4, 2022 at 1:10 PM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
March 3, 2022 at 10:17 AM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
March 2, 2022 at 3:57 PM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
March 2, 2022 at 10:06 AM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
February 28, 2022 at 4:13 PM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
February 14, 2022 at 1:16 PM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
February 11, 2022 at 3:36 AM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
February 9, 2022 at 10:54 AM	https://your-api.com/666/identity-updated-endpoint?your-query-param=123	BadRequest
1-10 of 47 total results. < >		

4. Review the Logs information as follows:
 - a. In the Callback date column, check when the callback was sent (includes date range filters).
 - b. In the URL column, verify the URL used to forward the webhook event notification that a specified event occurred to the relevant third-party API (program or application).
 - c. In the Response column, review the states to verify whether the HTTP callback was received successfully by third-party API or not. For example, Accepted, BadRequest, InternalServerError, and so on.
 - d. (Optional) Navigate through the callback logs (forwards or backwards in time) by clicking the Next page or Previous page icons.

5.15 | Granting access to the ClearID web portal

Before a user can access the Genetec ClearID™ web portal, you must grant them the required *User* or *Administrator* permissions for the website.

Before you begin

The identity that you want to grant access to must exist in the system.

What you should know

- To grant *User* or *Administrator* permissions for the website, you must be an account administrator.

Procedure

Choose one of the following:

- Grant user access to the web portal
- Grant administrator access to the web portal

Results

The selected identity now has access to the web portal with either User or Administrator privileges.

After you finish

[Log on to the web portal.](#)

Browse

- Viewing sites where a user can invite visitors

5.15.1 | Granting user access to the ClearID web portal

Before a user can access the Genetec ClearID™ web portal, you must grant them the required permissions for the website.

Before you begin

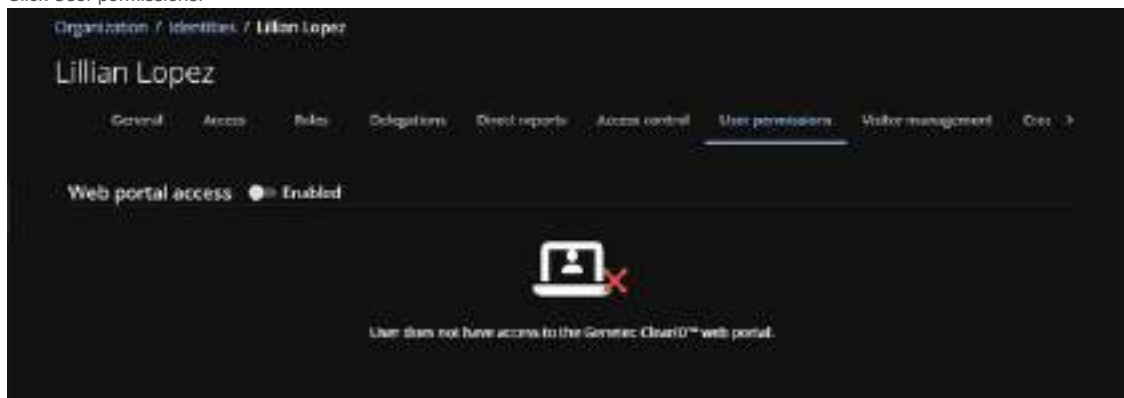
The identity that you want to grant access to must exist in the system.

What you should know

- To grant user permissions for the website, you must be an account administrator.

Procedure

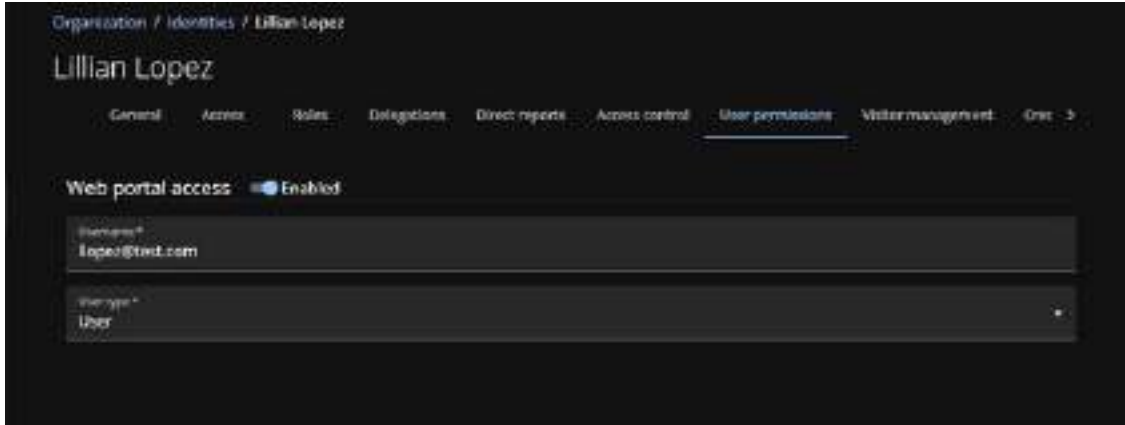
1. Click Organization > Identities.
2. Search for a user or select one from the Identities list.
3. Click User permissions.



4. In the User permissions section, click or move the Web portal access slider to Enabled to grant access to the web portal.
If the slider is disabled the identity cannot access the web portal.

NOTE: Some organizations do not enable web portal access for some or all of their identities because their organization does not require employee requests or web portal access.

5. In the Username field, enter a valid email address.
6. In the User type list, select User for default user access to the web portal.
7. Click Save to confirm your changes.



Results

The selected identity now has access to the web portal with the default User privileges.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.



After you finish

Log on to the web portal.

Parent topic: Granting access to the ClearID web portal

5.15.2 | Granting administrator access to the ClearID web portal

Before an administrator can access the Genetec ClearID™ web portal, you must grant them the required permissions for the website.

Before you begin

The identity that you want to grant access to must exist in the system.

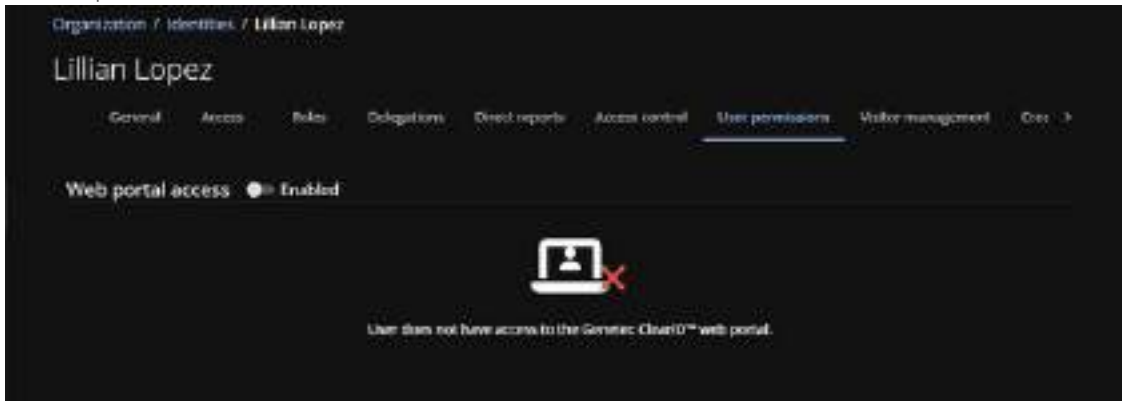
What you should know

- To grant administrator permissions for the website, you must be an account administrator.

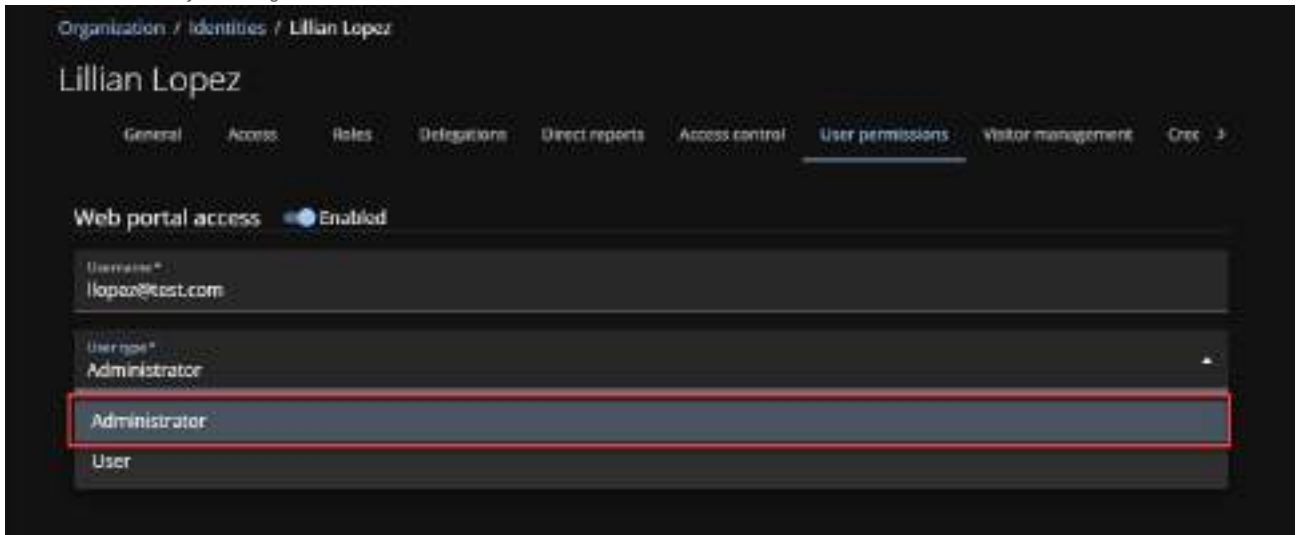
IMPORTANT: When a new account is created, an end user designated as the account administrator will receive a Welcome to Genetec ClearID™ and a New ClearID Account - ACCOUNTNAME email notification. By default, Administrator access is given to the end user that receives the email. If a system integrator or other identity also requires administrator access, their administrator access must be added by the end user (account administrator).

Procedure

1. Click Organization > Identities.
2. Search for a user or select one from the Identities list.
3. Click User permissions.



4. In the User permissions section, click or move the Web portal access slider to Enabled to grant access to the web portal.
If the slider is disabled the identity cannot access the web portal.
NOTE: Some organizations do not enable web portal access for some or all of their identities because their organization does not require employee requests or web portal access.
5. In the Username field, enter a valid email address.
6. In the User type list, select Administrator for Administrator access to the web portal.
7. Click Save to confirm your changes.



Results

The identity now has access to the web portal with Administrator privileges.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Log on to the web portal.

Parent topic: Granting access to the ClearID web portal

5.16 | Viewing your profile in ClearID

You can use the Profile page to view your profile and check your access or role membership in Genetec ClearID™.

What you should know

- The profile in ClearID is displayed to the employee in a read-only view and can't be modified. The profile contains the site, worker type description, supervisor name, and other information.
- An *employee* can check their profile at any point in time to understand what information ClearID stores about them. They can also see if the information is outdated and request an update.

Tip: Check your department or job title after a job change to ensure that you have the correct access.

Procedure

1. From the homepage, click My Profile.

The screenshot shows a user profile page for 'John Doe'. At the top, there's a 'My Profile' header with a sub-header 'John Doe'. Below this is a navigation bar with tabs: General (selected), Access, Roles, Delegations, Direct reports, Credentials, Preferences, and Manage. The main content area is titled 'My Profile' with a status 'Active'. It features a profile picture of a man with glasses and a beard. Below the picture are several input fields for personal information: First name (John), Last name (Doe), Phone number, Mobile phone number, Middle name, Business email (jdoe@hmi.com), Personal email, Preferred name (John), Date of birth (MM/DD/YYYY), and Gender (Male). There are also fields for Country (Canada), State or Province (Quebec), City, and Zip or Postal code. The 'Company' section includes Company (Genetec), Primary site (Type to search...), Worker start date (mm/dd/yyyy), Worker end date, Department (United Content Services), Supervisor name, Job title (Content Developer), and Employee number. The 'Supervisors' section shows a table with columns 'Name' and 'Email', and a message 'No supervisors' with a person icon and a checkmark. At the bottom, it states 'Requests from this user do not require supervisor approval.'

2. In the General tab, review your identity details including any associated supervisors, and the identity status (active or inactive).
3. (Optional) Additional tabs are also provided to review other details and options associated with your identity as follows:

Custom fields

Custom fields associated with your identity.

Access

Access associated with your identity.

Roles

Roles associated with your identity added by a provisioning policy or manually added.

Delegations

Delegations associated with your identity.

Direct reports

Reportees associated with your identity.

Access control

Access control associated with your identity including extended grant time, cardholder activation, provisioning attributes, and associated cardholders.

User permissions

Web portal user or administrator access permissions associated with your identity.

Visitor management

List of sites where your identity can invite visitors.

Credentials

Synchronized credentials associated with your identity.

Logs

Identity event logs for activities associated with your identity.

After you finish

[View your site and area access.](#)

5.16.1 | Configuring your ClearID portal theme preferences

You can customize your Genetec ClearID™ portal theme to match your personal preferences by choosing between light or dark mode.

What you should know

Your theme preferences only apply to your user profile. If you don't configure a personal theme, your theme matches the portal theme configured by the *Administrator*.

Procedure

1. In the ClearID web portal, click My Profile > Preferences.
2. In the Theme section, configure your theme preferences.
 - a. From the Mode list, choose between Light, Dark, and System.

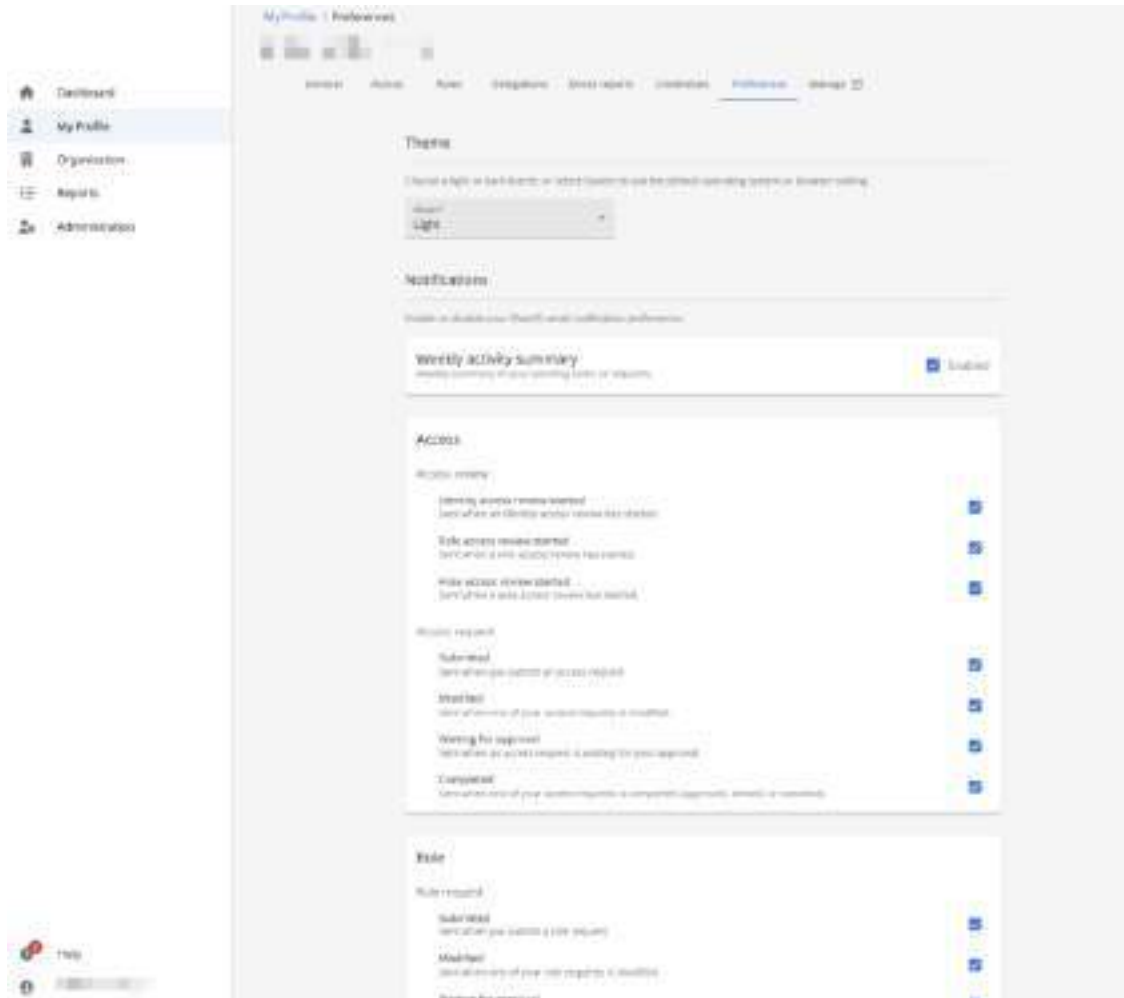


NOTE: Selecting System uses your default operating system or browser settings.

3. Click Save.

Example

The ClearID portal of a user with light mode selected:



Parent topic: Viewing your profile in ClearID

5.17 | Viewing your site and area access in ClearID

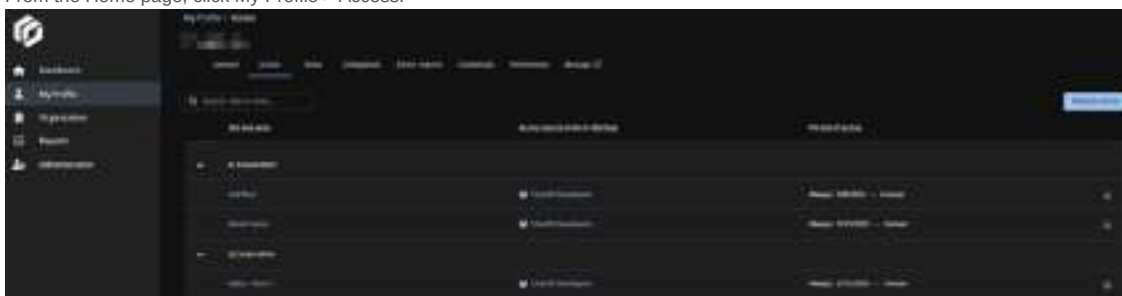
You can use the Profile Access page to review your site and area access. This information can be used to help you identify if you need to request more access in your main site or other sites.

What you should know

The Access page displays all sites and areas that the logged in user has access to and includes the access source and the period of access.

Procedure

1. From the Home page, click My Profile > Access.



The sites and areas you have access to are displayed in the Site and area column.

2. (Optional) Click the blue text in the Site and area column to jump to the Access page.
3. (Optional) Click the blue text in the Access source column to jump to the Roles page.

After you finish

Submit access requests for other areas as required.

5.18 | Setting request visibility for users in ClearID

To manage the types of requests that web portal users can make, you can change the request visibility settings in the Genetec ClearID™ web portal.

What you should know

You must be an *Account administrator* to change request visibility settings.

NOTE: Changing these settings affects the types of requests all web portal users can make.

Procedure

1. In the ClearID portal, click Administration > Account configuration.
2. In the Request visibility section, configure the settings as needed:

Enable request visibility for web portal users

Turn on the Enable request visibility for web portal users option to allow users to make requests in the web portal.

Request access

Select Request access to allow users to request access to an area for themselves, for roles, or for other identities.

Request role

Select Request role to allow users to request role membership for themselves or for other identities.

Request an identity

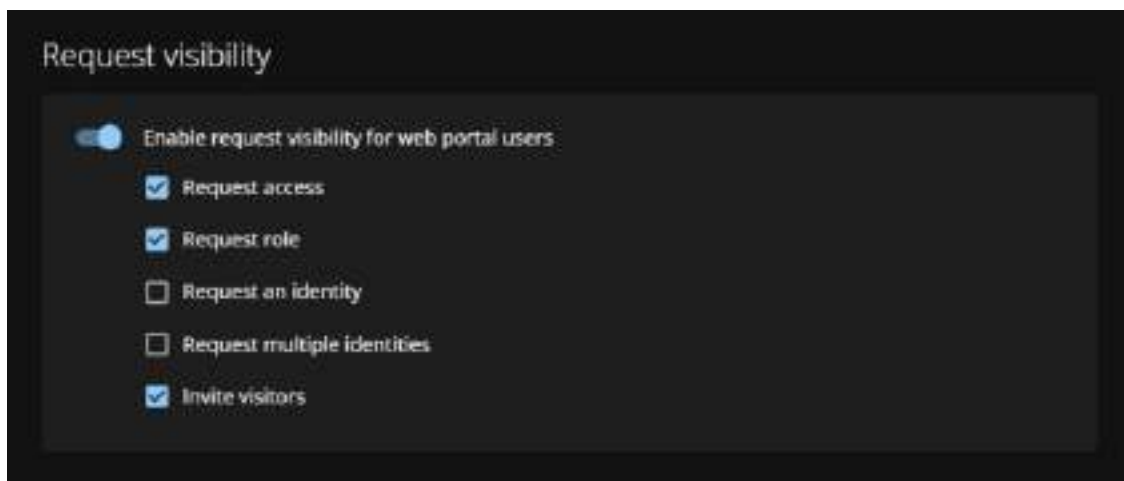
Select Request identity to allow users to create an identity in the system.

Request multiple identities

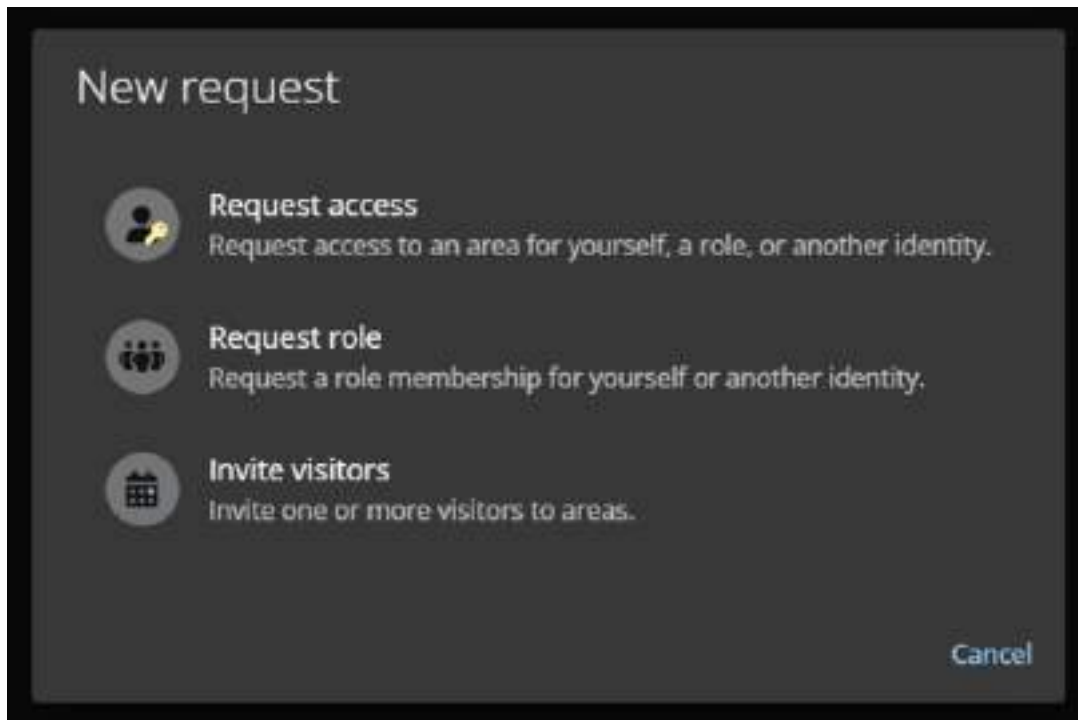
Select Request multiple identities to allow users to create multiple identities in the system.

Invite visitors

Select Invite visitors to allow users to invite one or more visitors to areas.



3. Click Save.
Users can only access selected request types in the New request dialogue.

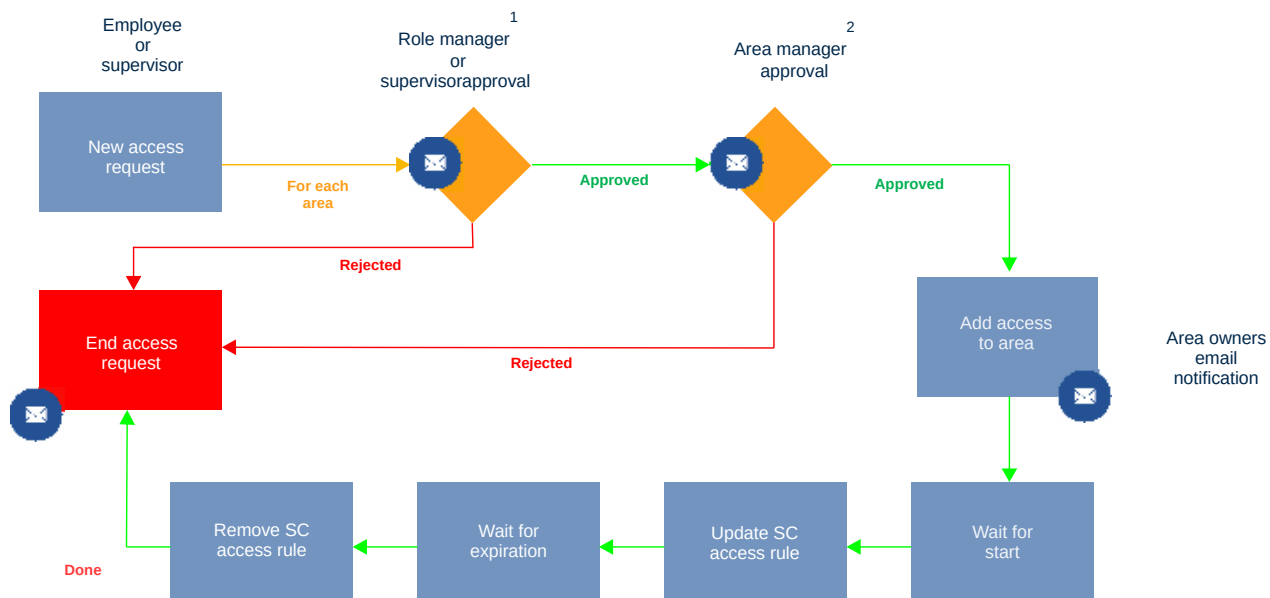


5.19 | About access request workflow in ClearID

An access request workflow is a series of activities performed by the system or authorized people during the life cycle of an access request. The activities can change the state and properties of access requests, affect other entities in the system, or wait for a condition to be met.

The workflow helps automate access request tasks, such as approving or rejecting access requests, so that people involved in the review and approval process can focus on other tasks.

The following diagram illustrates the *access request workflow* that occurs in Genetec ClearID™ and Synergis™.



¹ (Optional) Role manager or supervisor approval can be enabled for the area.

² (Optional) Area manager approval can be enabled for the area.

NOTE: By default, access requests are limited to the minimum access required. This limits what a user can do with an access card.
Browse

- About workflows in ClearID
- Creating exceptions to the access request approval workflow in ClearID

5.20 | Requesting access in ClearID

To request access for yourself, another identity, or a team member, you can use the Genetec ClearID™ self-service portal. Using a self-service portal with area managers specified simplifies the approval process, and avoids interrupting a chain of people who might or might not be the correct approvers.

Before you begin

- Familiarize yourself with workflows.

What you should know

Employees, managers, and supervisors of different secure areas can request access for themselves or their employees using a self-service Web portal.

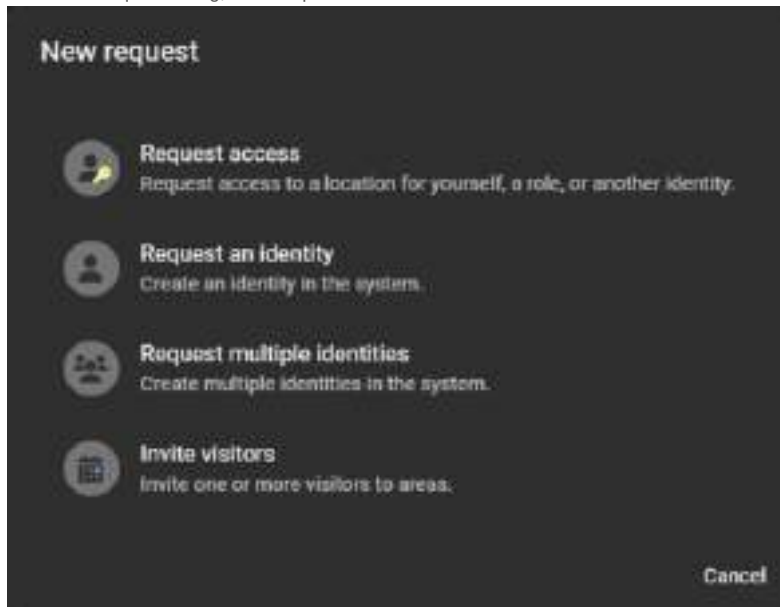
NOTE: In the past, most sites access control solutions would typically not track or record why access was required.

In ClearID, the access request includes: who requested access, site, area, when, and why the access is required.

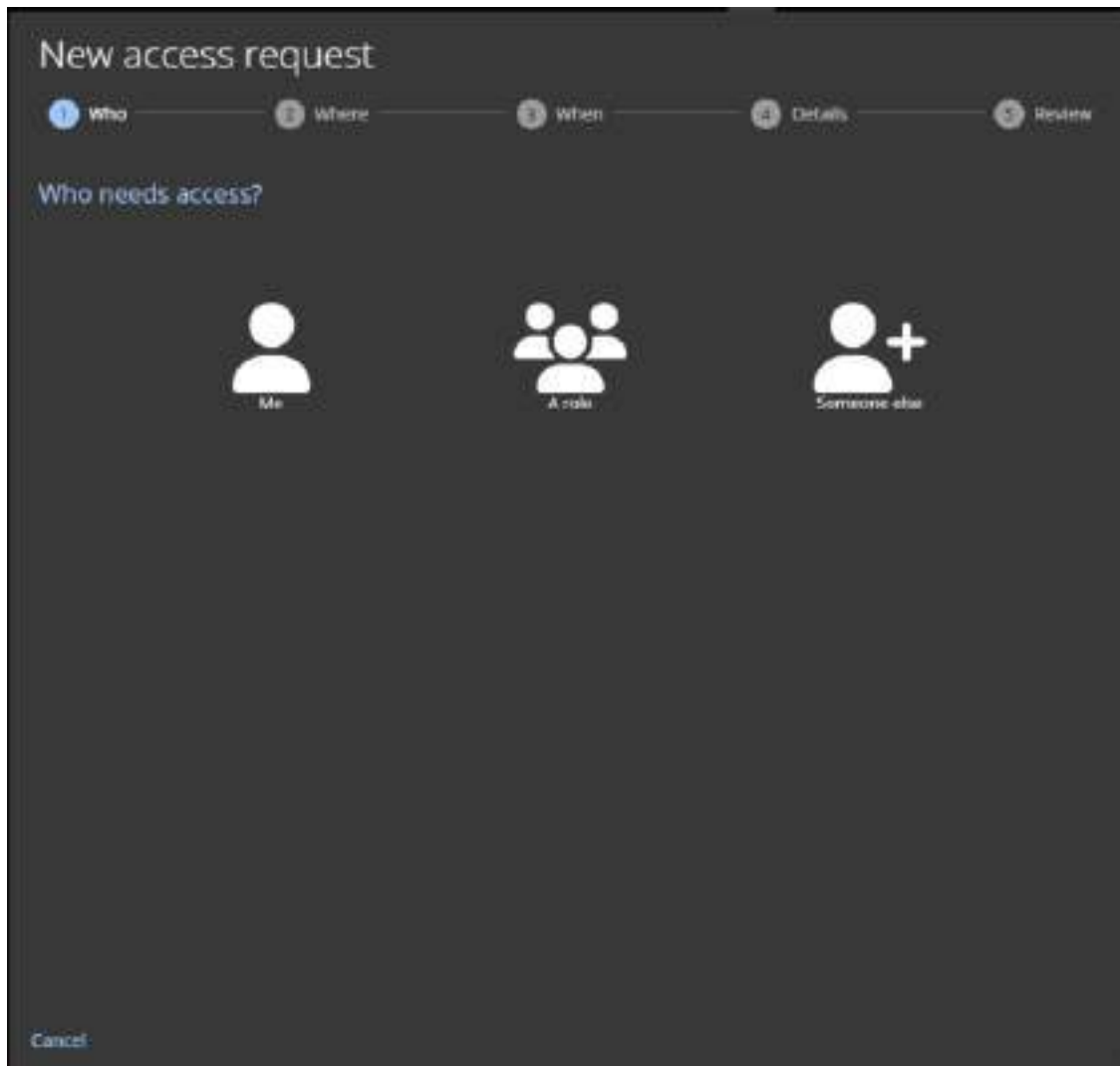
- Separate access requests and approval workflows are created for each request for access to an area.
- After the request summary is confirmed, it's automatically assigned to the right individuals for approval.
- After the approval process occurs, the requester receives an email notifying them whether the access request was approved or rejected.

Procedure

1. Log on to the self-service portal.
2. Click Dashboard > My requests.
3. Click New request.
4. In the New request dialog, click Request access.



5. In the Who section of the New access request dialog, click an option to choose who needs access:



a. (Optional) If you selected Me, the New access request wizard is automatically updated to include the information of the currently logged in user.

b. (Optional) If you selected A role, search for or select a role from the list.

The New access request wizard is updated to include the information of the selected role.

IMPORTANT: Only a *role owner* or *role manager* can view and request access for roles. They can only request access for the roles that they manage.

c. (Optional) If you selected Someone else, search for or select an individual from the list.

The New access request wizard is updated to include the information of the selected individual.

NOTE: A supervisor or team leader can request access for someone in their team, group, or department.

6. In the Where section of the New access request dialog, select a site from the site list.

a. Search for or select one or more areas and click Next.

The screenshot shows a dark-themed dialog box titled "New access request for John Doe". At the top, a progress bar indicates five steps: 1. Who (checked), 2. Where (active), 3. When, 4. Details, and 5. Review. The main heading is "Which site do you need access to?". Below it is a dropdown menu labeled "Site*" with the selected value "Genetec Albert Einstein". The next heading is "Which areas do you need access to?", followed by a note: "One request will be created for each area selected. A maximum of 10 areas can be selected at a time." Below this is a section labeled "Areas" containing a list with one item, "Main Entrance", which has a selection icon. To the right of the list is a button labeled "Add more" and a search input field with the placeholder text "Type to search...". At the bottom left is a "Cancel" button, and at the bottom right are "Back" and "Next" buttons.

NOTE: Only areas created with Public visibility are shown in this list.

7. In the When section of the New access request dialog, enter the dates that you require or select them using the calendar picker.

New access request for John Doe

Who Where **When** Details Review

When do you need access?

ⓘ A site policy limit is currently active. Individual access is limited to 30 days.

ⓘ The dates and times shown here are in the America/Toronto time zone.

Start date* 04/03/2025

End date* 04/04/2025

Duration 24

Following which schedule?

Select a period with a schedule that meets your access requirements for each area.

Main Entrance Schedule* Always

Cancel Back Next

- a. Select the schedule that you require for each area and click next.

IMPORTANT: If a site access duration has been enabled, you can't select a duration that exceeds the maximum limit specified in the site access configuration.

8. In the Details section of the New access request dialog, enter the reason for the access request.

NOTE: The Reason for request is a required field and the reason is stored for access review auditing purposes.

- a. Upload any supporting documents to the access request and click Next.

New access request for John Doe

✓ Who

✓ Where

✓ When

4 Details

5 Review

Why do you require this access?

Reason for request *

Access required while performing maintenance work.

50 / 300

Mandatory documents

Driver's license * Provided ⓘ

✕ JohnDoe_DriverLicense.pdf
10 KB

Certificate of qualification * Provided ⓘ

✕ JohnDoe_CertificateOfQualification.pdf
10 KB

Work permit * Provided ⓘ

✕ JohnDoe_WorkPermit.pdf
10 KB

Cancel Back Next

9. Review the request summary.

New access request for John Doe

✓ Who

✓ Where

✓ When

✓ Details

5 Review

Review

The following access requests will be created.



Genetec Albert Einstein • Main Entrance
April 3, 2025 to April 4, 2025 • Always

[Cancel](#)[Back](#)[Request access](#)

- If changes are required, click Back and modify the settings.
- If the information is correct, click Request access to submit the access request.
- Click Finish to return to My requests.

Results

Your access request has been submitted and is waiting for the required approvals. Depending on your setup, the request is either automatically approved or waiting for the required approvals. In some situations, the access request might also be manually or automatically canceled or rejected.

Waiting for the required approvals. In some situations, the access request might also be manually or automatically canceled or rejected.

Dashboard

My requests

My location

Help

ALL

NEW REQUEST

Type	Status	Description	Date submitted
 John Doe Access request • All ID	 Pending for approval	Genetec Albert Einstein Main Entrance 4/3/2025 to 4/4/2025	12 minutes ago
 Jack Access request • All ID	 Approved	Genetec Albert Einstein Main Entrance 2/14/2024 to 2/14/2024	1 month ago
 John Doe Access request • All ID	 Canceled	Genetec Head Office Training Room 11/20/2024 to 11/23/2024	4 months ago
 John Doe Access request • All ID	 Canceled	Genetec Head Office Training Room 10/18/2024 to 10/25/2024	3 months ago
 Jack Access request • All ID	 Approved	Genetec Montreal Data Center 8/20/2024 to 8/26/2024	1 month ago

0 Canceled Request

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Confirm whether the request was approved or rejected:

- Check your email for an *Access approved* email.
- Check My requests in ClearID.

Browse

- [Setting a maximum duration for site access in ClearID](#)
- [About email notifications in ClearID](#)
- [Checking the status of access requests in ClearID](#)

Browse

- [Access Request Feature Note \(2 pages\)](#)

5.21 | Adding supervisors manually in ClearID

To help manage requests from your direct reports, you can manually add supervisors to the relevant identity profiles so that the supervisor approval workflow can be used.

Before you begin

[Create your identities.](#)

What you should know

This procedure is for Supervisors who have direct reports.

- To manually add supervisors to identity profiles, you must be an account administrator.

Procedure

1. From the homepage, click Organization > Identities.
2. Search for or select an identity from the list.
 - a. (Optional) Use the Active, Inactive, or All filters to narrow your search.
3. Click the identity that you require.
4. In the Supervisors section, click .

The screenshot shows the Genetec ClearID user profile page for John Doe. The page is divided into several sections: General, Company, and Supervisors. The General section contains fields for Name, Email, Password, and other user details. The Company section contains fields for Company Name, Address, and other company information. The Supervisors section is currently empty, showing 'No supervisors'.

5. Search for or select one or more users from the list that you want to add as supervisors and click Add to confirm your selection.
NOTE: Adding multiple supervisors is useful when employees or supervisors work shifts or a rotating days system. In these situations, it's common to have multiple supervisors for different employees on different days.
6. (Optional) Click  to remove any supervisors that are no longer required.
7. Click Save to confirm your changes.

Results

The supervisors that you selected have now been added to the supervisors list for this identity.

The screenshot shows the Genetec ClearID user profile page for John Doe, with the Supervisors list now populated. The list contains one supervisor, John Doe, who is highlighted with a yellow box. The page also shows the General and Company sections, which are identical to the previous screenshot.

After you finish

View your direct reports.

5.22 | Viewing direct reports in ClearID

As a *Supervisor*, you can check the access control status, general identity information of your direct reports. You can also use the direct report list for security reviews or auditing purposes.

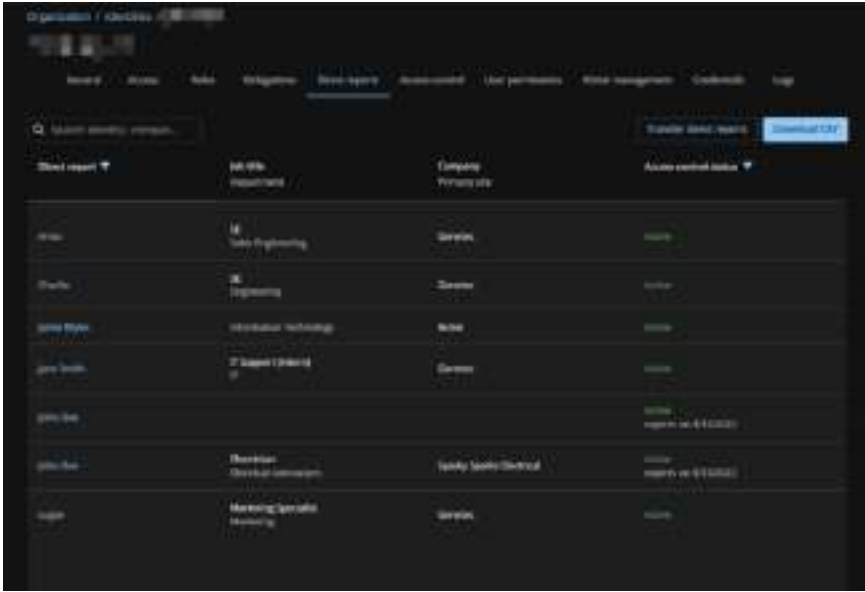
Before you begin

To view *direct reports*, you must be a *Supervisor* or *Account administrator*.

- A *Supervisor* can check general identity information for their direct reports at any point in time, to understand what information Genetec ClearID™ stores about them. They can also see if the information is outdated and request an update.
- An *Account administrator* can check the direct reports of an identity to validate the supervisor link and other information.

Procedure

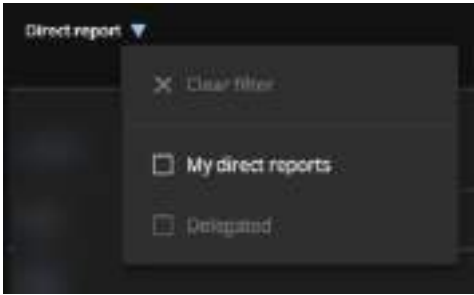
1. From the Home page, click My Profile > Direct reports.



2. Filter the list based on your required criteria:

Direct reports

Click the Direct report filter icon (Y) to filter the list. Choose either My direct reports, Delegated, or both.



My direct reports

Displays employees that are your direct reports.

Delegated

Displays delegated employees (because another user delegated their tasks to you).

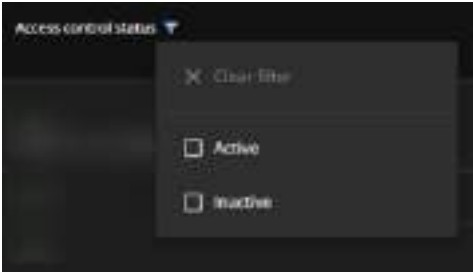
NOTE: Delegated employees are highlighted in the list using a DelegateFromAnotherUser icon 

Clear filter

Click Clear filter (X) to remove selected filters.

Access control status

Click the Access control status filter icon (🔍) to filter the list. Choose either Active, Inactive, or both.



Active

Displays direct reports with an Active access control status.

Inactive

Displays direct reports with an Inactive access control status.

Clear filter

Click Clear filter (✕) to remove selected filters.

Search

Use the Search bar to search for an identity by first name, last name, or company.

3. Click Download CSV, to download a copy of the direct reports list in CSV format. The report can then be used for auditing purposes, to keep a physical copy, to attach to an audit request, to review offline, or to manipulate or consolidate data in a spreadsheet for other audiences.
 - a. Follow your browser prompts to complete downloading the exported file.

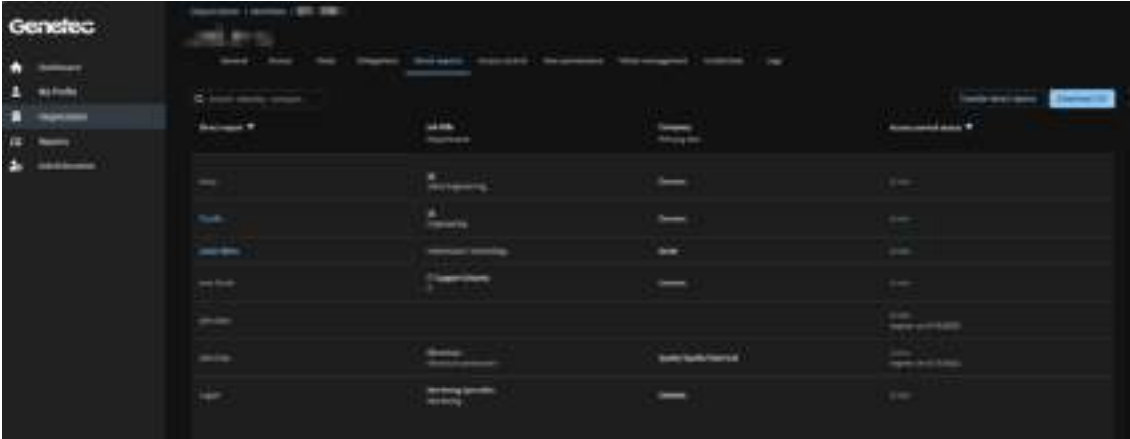
The file is exported as a .CSV file to the default download location for your browser (ClearID Direct reports.csv).

NOTE: The columns and entries in the CSV file can vary depending on the filters you've selected when you download the report.

4. (Optional) Click the name of a direct report in the list to view their identity profile in more detail.

You can also view more details about the identity by browsing the following identity profile pages:

- General
- Access
- Roles
- Delegations
- Access control
- User permissions
- Visitor management
- Credentials
- Logs



After you finish

Manage your direct reports access and roles if required.

Browse

- Adding supervisors manually in ClearID
- Creating identities in ClearID
- About direct reports report in ClearID

5.23 | Managing direct reports in ClearID

Supervisors can manage their direct reports access. This can include general identity information, area access, modifying or removing roles, task delegation, and access control.

Before you begin

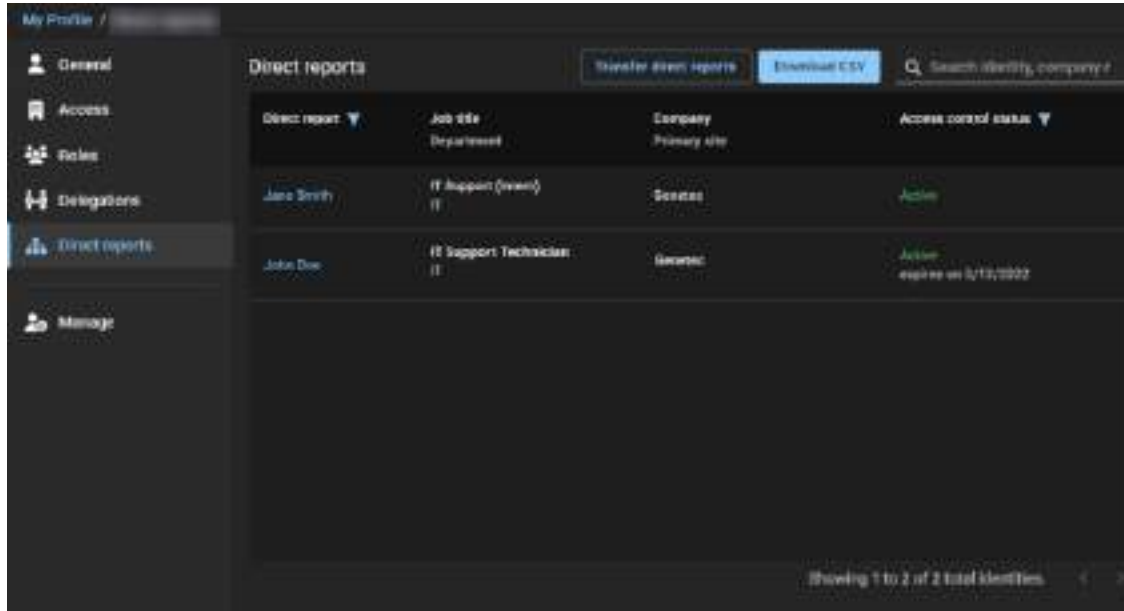
- Adding supervisors manually in ClearID.
- (Optional) Add supervisor access to manage direct reports.

What you should know

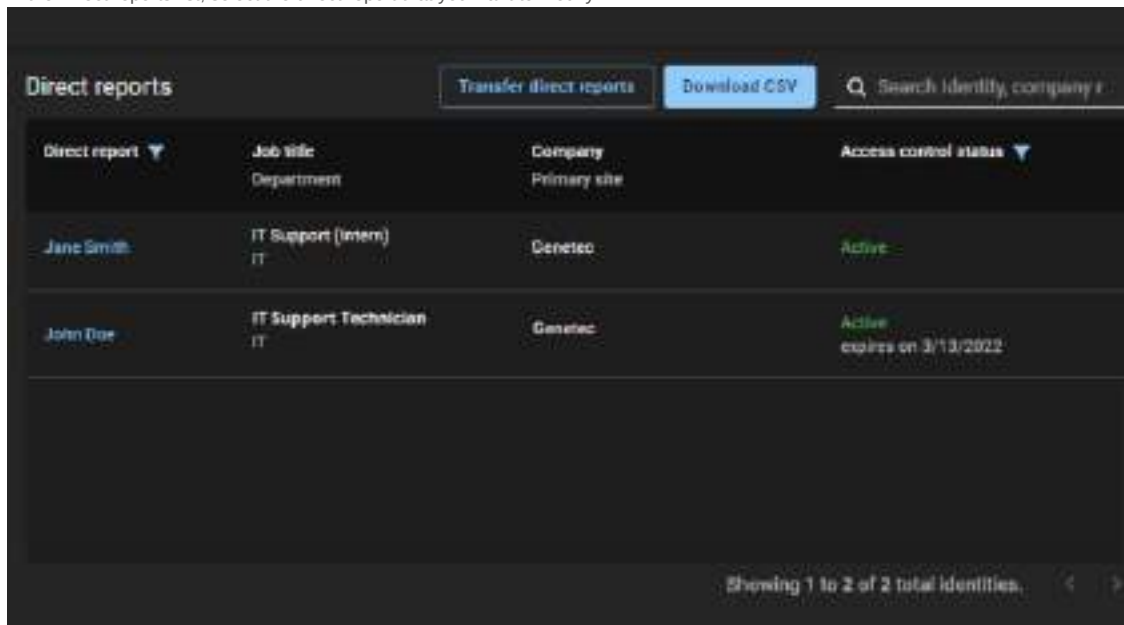
- To manage *direct reports*, you must be a supervisor.
- To modify General identity information or Access control settings for a direct report, you must be a supervisor with the manage direct reports permission.

Procedure

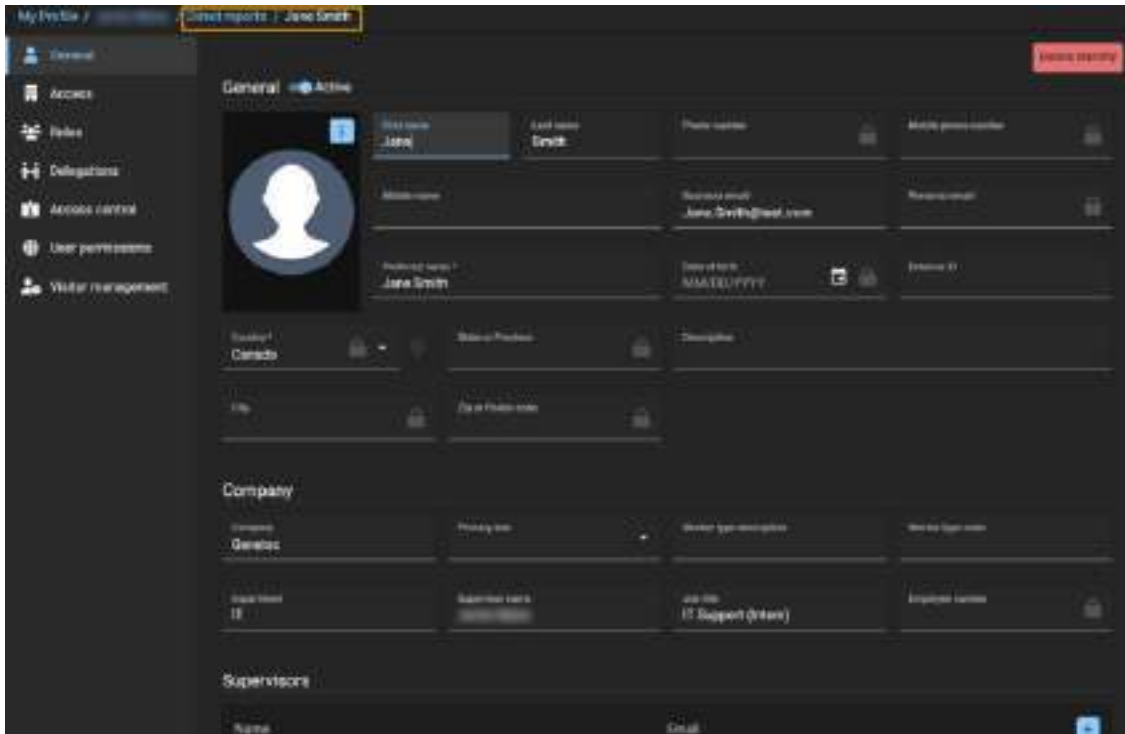
1. From the Home page, click My Profile > Direct reports.



2. In the Direct reports list, select the direct report that you want to modify.



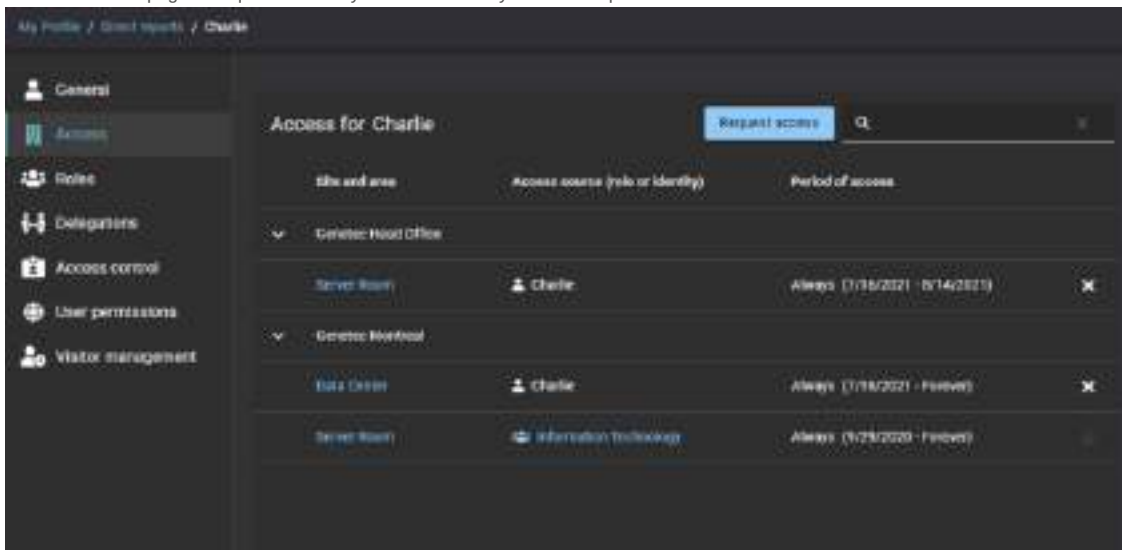
Tip: Use the filters described in [Viewing direct reports in ClearID](#) to search for and select the direct report you require.



IMPORTANT: General identity information attributes are typically synchronized from an external data source to populate the general identity information. If you make updates to identities that are synchronized with an external data source, your changes can be overwritten by the synchronization.

- A supervisor with default permissions cannot modify any of the General identity information for their direct reports.
- A supervisor with manage direct reports permission can modify the General identity information if required. This enhanced permission is typically used to manage contractors or temporary workers who are not synchronized from an external data source.

3. Click the Access page to request or modify area access for your direct report.

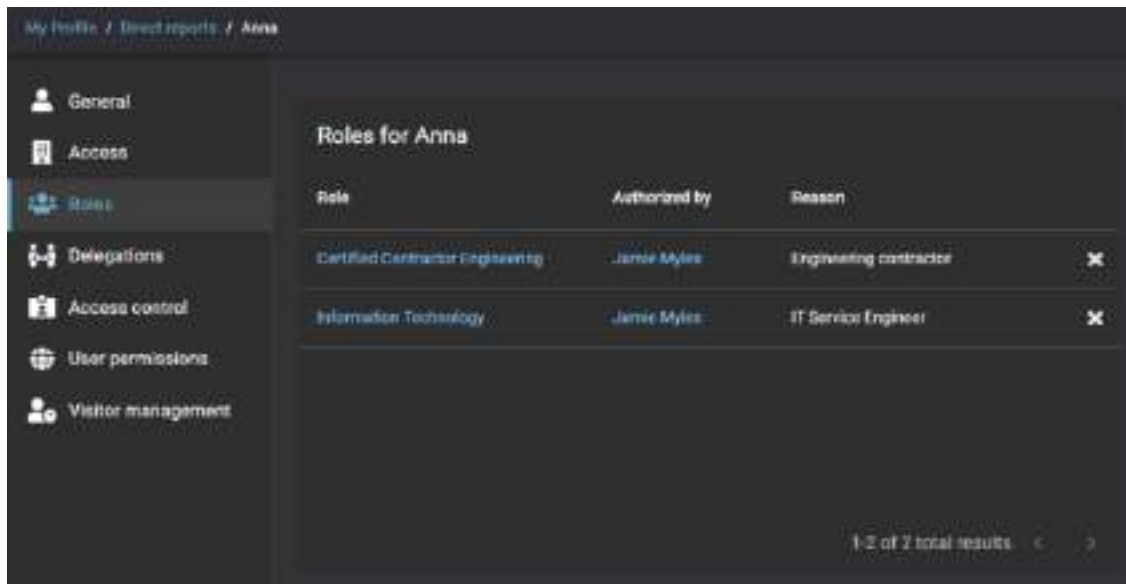


a. Click Request access to request access to one or more areas.

b. Click  to remove any area access that is no longer required and click Revoke to confirm the removal.

NOTE: You can only remove area access that was manually added. Area access that was added using a provisioning policy is identified using the locked () icon and cannot be modified.

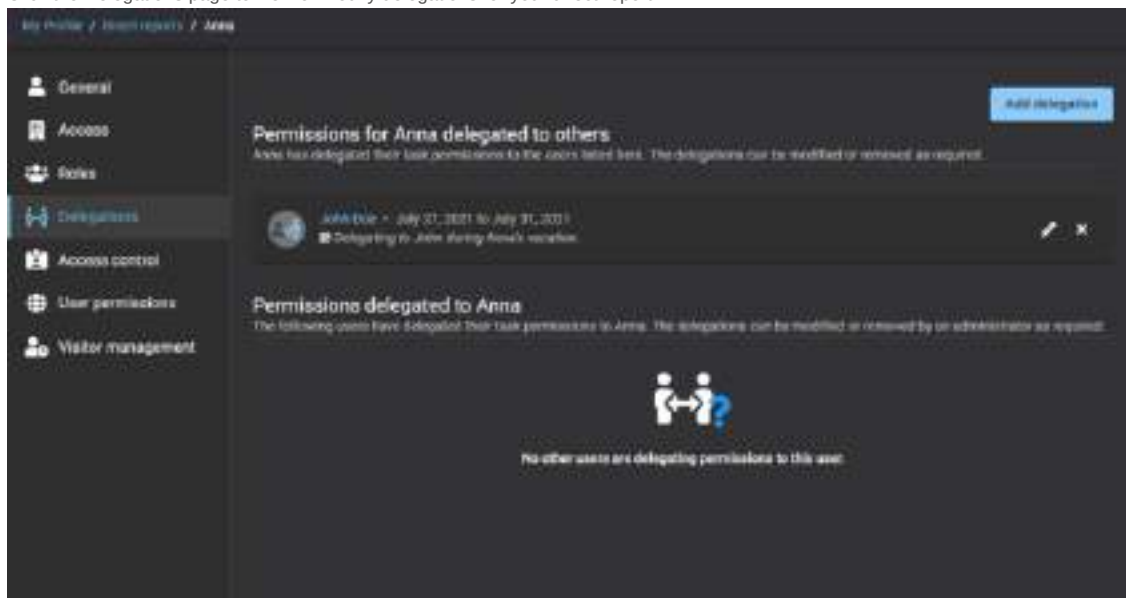
4. Click the Roles page to modify or delete role access for your direct report.



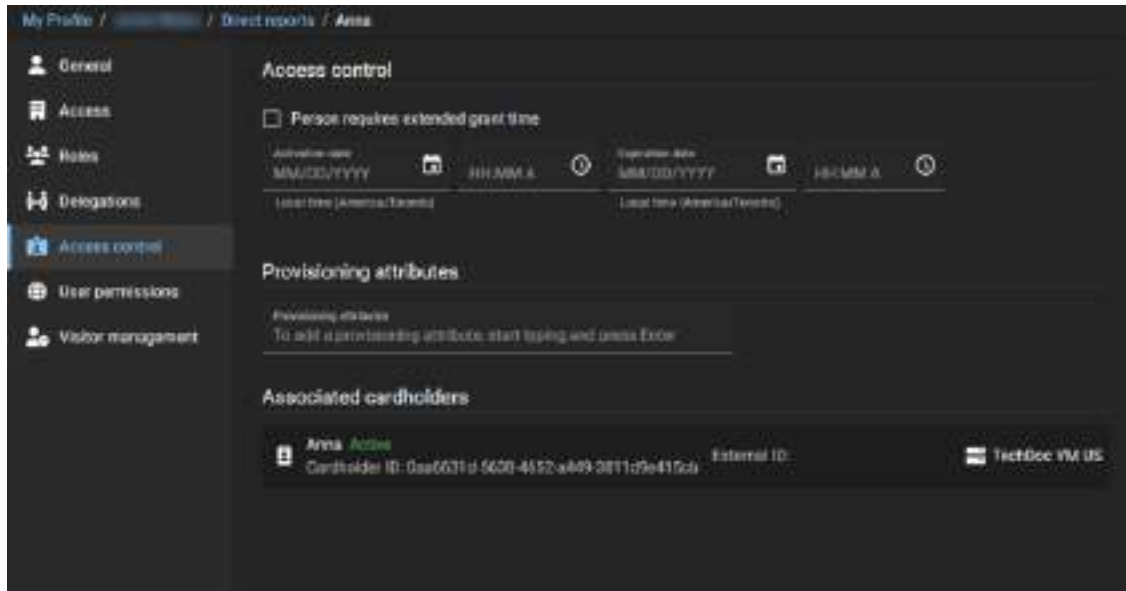
- Click a role hyperlink to view the role details.
- Click  next to a role to remove the role access that is no longer required and click Remove again to confirm.

NOTE: You can only remove roles that were manually added. Roles that were added using a provisioning policy are identified using the locked  icon and cannot be modified.

- Click the Delegations page to view or modify delegations for your direct report.

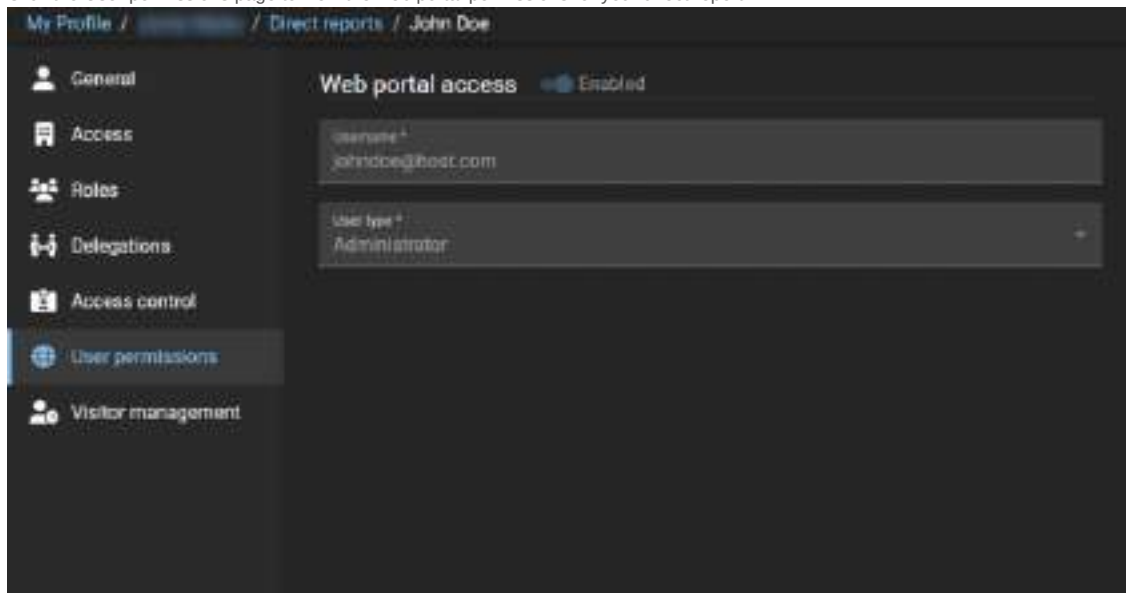


- Click Add delegation to delegate tasks to another user.
 - Click  next to a delegation to modify the settings.
 - Click  next to a delegation to remove a delegation that is no longer required.
- Click the Access control page to view the access control settings for your direct report.

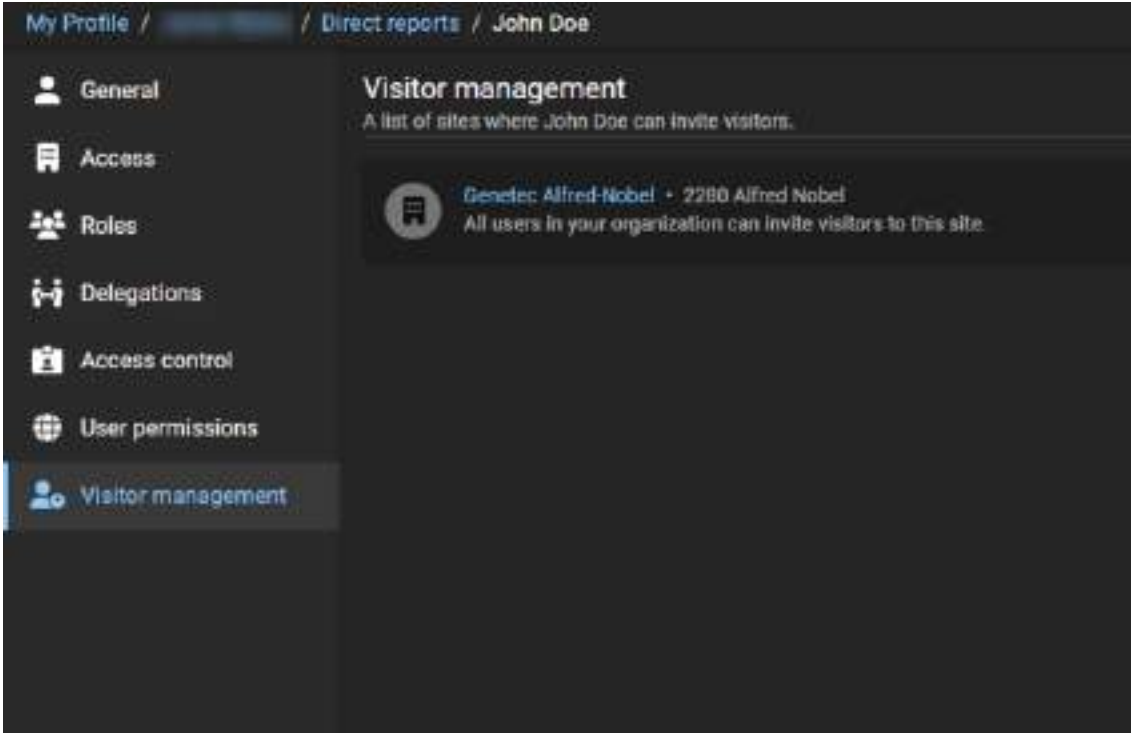


a. (Optional) A supervisor with manage direct reports permission can modify the Access control settings if required.

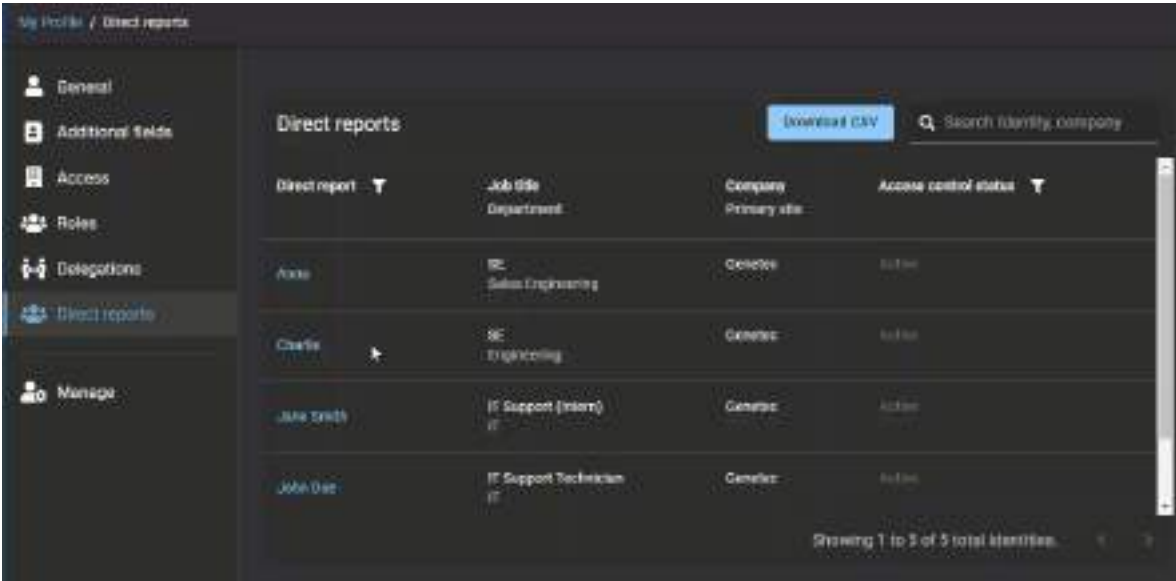
7. Click the User permissions page to view the web portal permissions for your direct report.



8. Click the Visitor management page to view the visitor management settings for your direct report.



Example



Browse

- Granting additional permissions for supervisors in ClearID

5.24 | Transferring direct reports in ClearID

From time to time a supervisor, account administrator, or an identity might need to transfer direct reports. For example, transferring direct reports to a new hire or for a change in supervisor.

Before you begin

You must have a supervisor or an identity with direct reports ready to transfer.

What you should know

To transfer *direct reports*, you must be a supervisor or an identity with elevated write permissions for identities, or an account administrator.

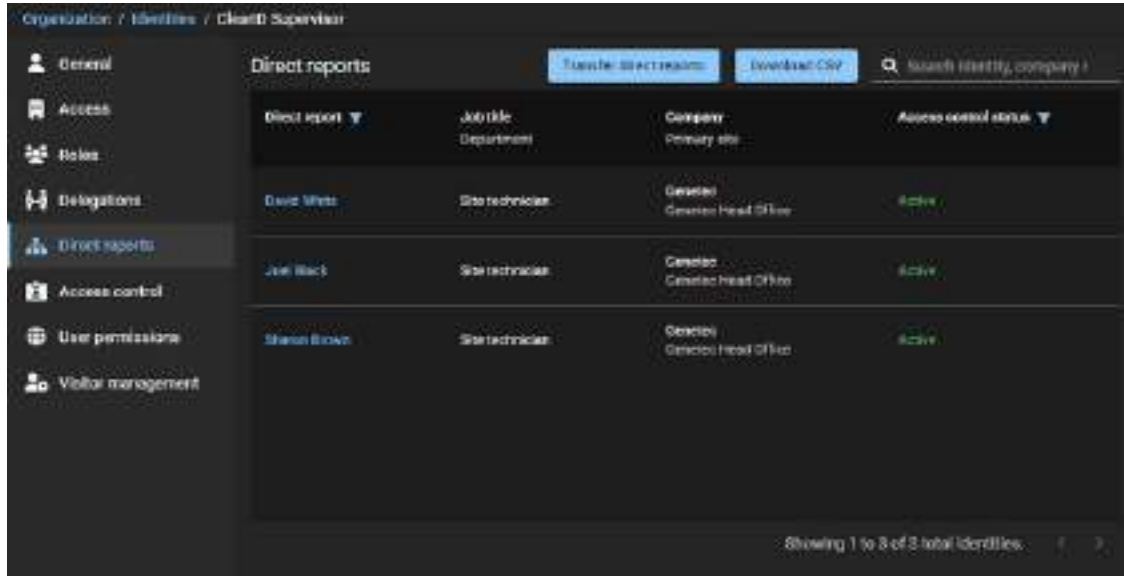
- You can transfer direct reports to another identity (regardless of their permissions).
- You can add a maximum of 20 supervisors when transferring direct reports.

IMPORTANT: This function is intended for identities that are locally managed in Genetec ClearID™. If identities are managed using an external data source, the transfer of direct reports will be overwritten.

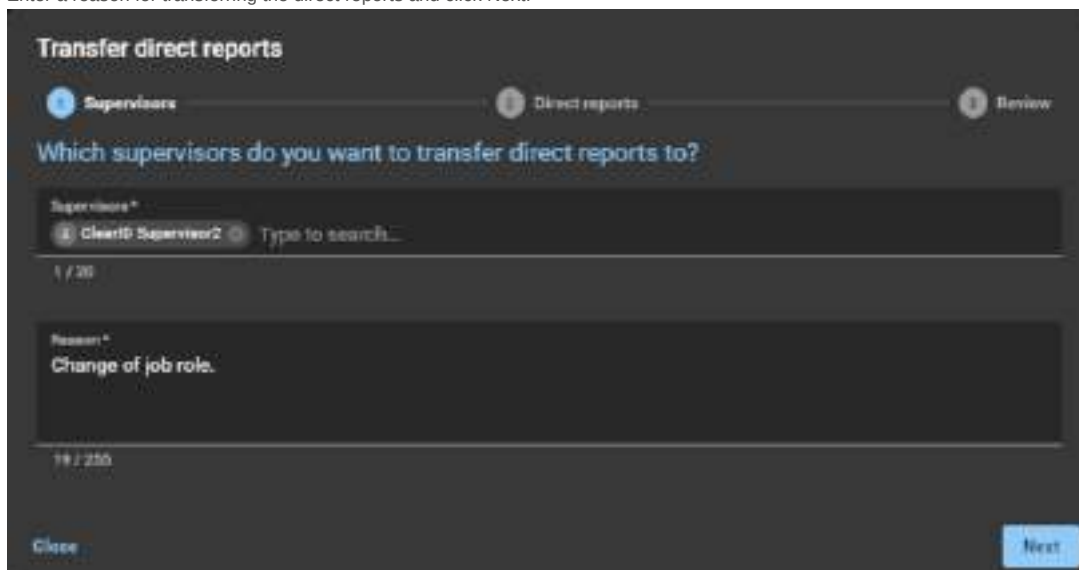
Procedure

To transfer direct reports (Performed by an account administrator or an identity):

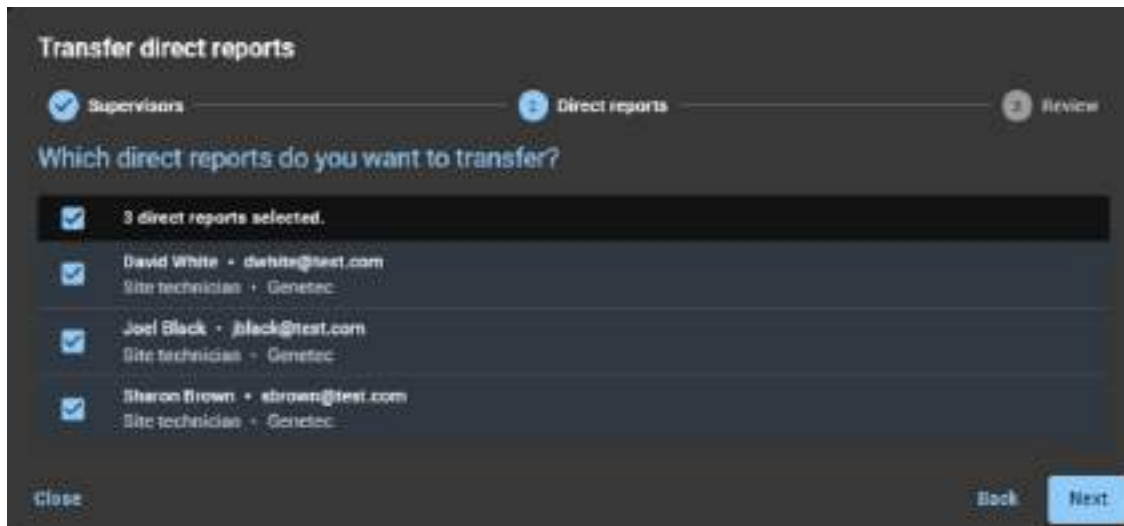
1. From the Home page, click Organization > Identities.
2. Select the identity whose direct reports you want to transfer.
3. Click Direct reports.
4. Click Transfer direct reports.



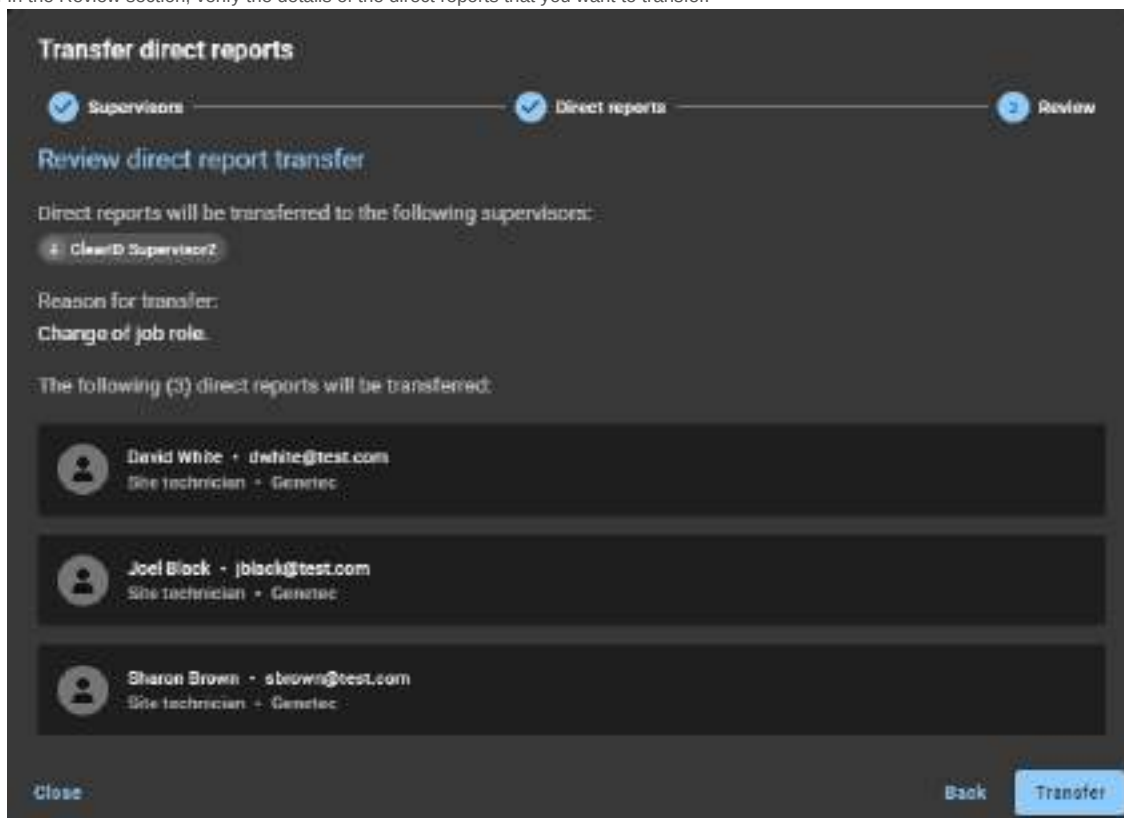
5. In the Supervisors section of the Transfer direct reports dialog, complete the fields.
 - a. Search for and select one or more supervisors.
 - b. Enter a reason for transferring the direct reports and click Next.



6. In the Direct reports section, select the direct reports you want to transfer and click Next.

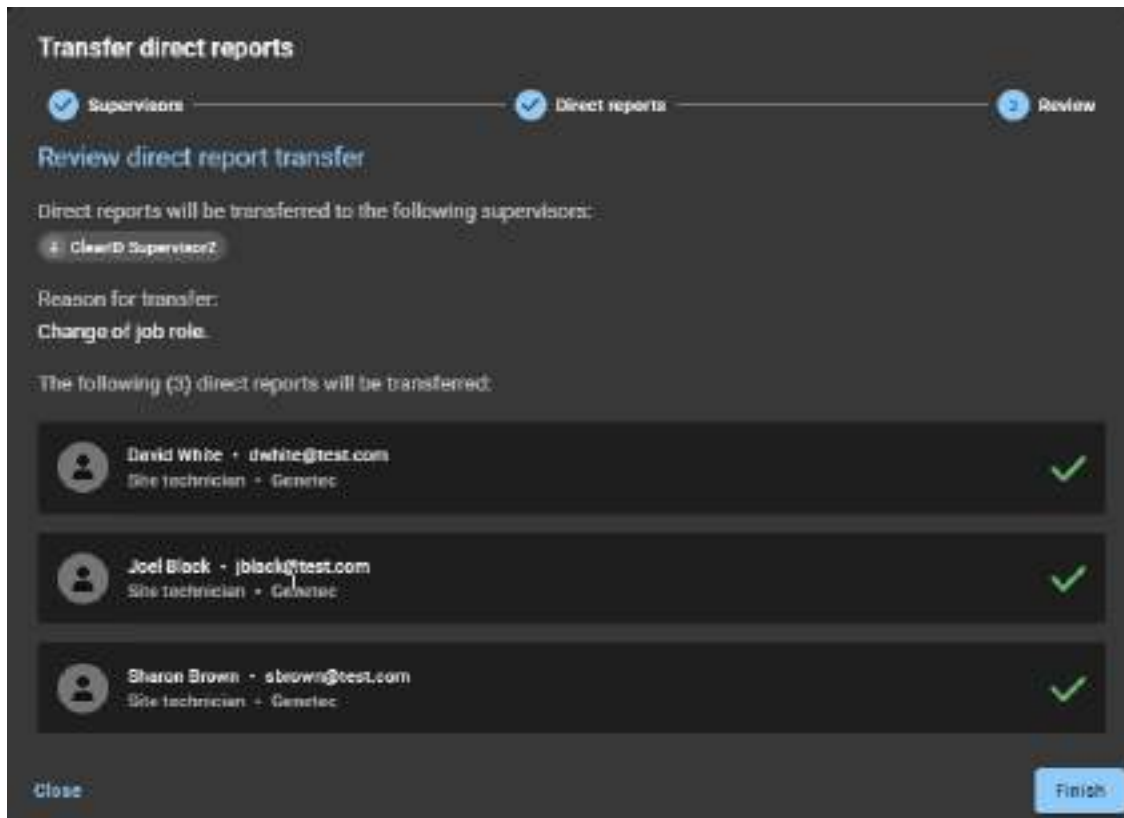


7. In the Review section, verify the details of the direct reports that you want to transfer.



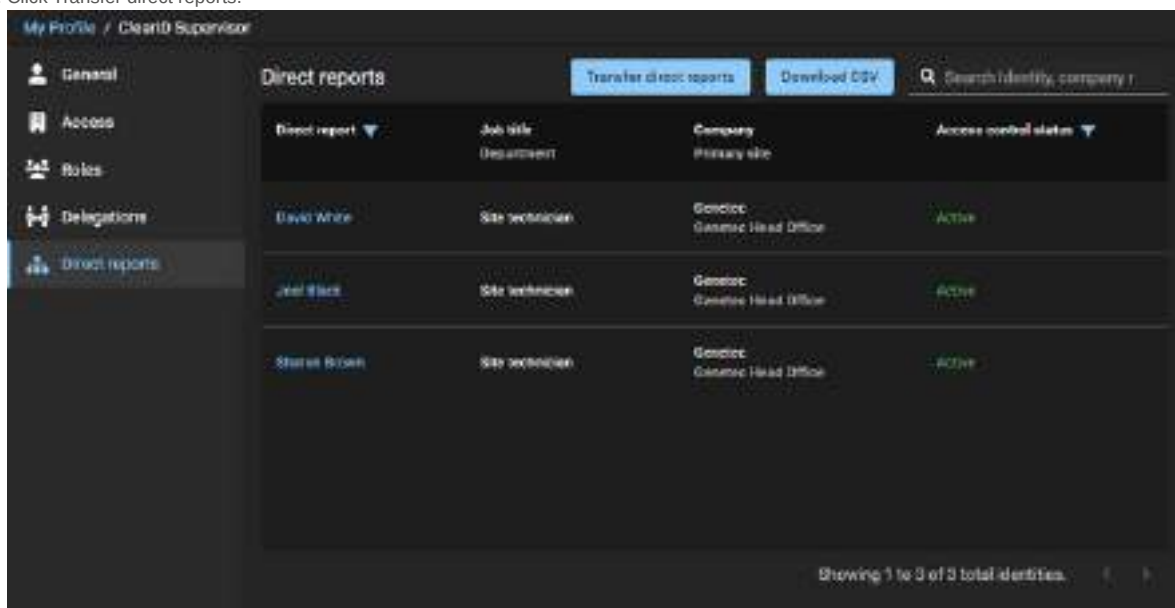
- a. (Optional) If you need to make some additions or changes, click Back to return to previous steps.
- b. If no further changes are required, click Transfer to initiate the transfer.

8. Click Finish to complete the transfer request.



To transfer direct reports (Performed by a supervisor):

1. From the Home page, click My Profile > Direct reports.
2. Click Transfer direct reports.



3. In the Supervisors section of the Transfer direct reports dialog, complete the fields.
 - a. Search for and select one or more supervisors.
 - b. Enter a reason for transferring the direct reports and click Next.

The screenshot shows the 'Transfer direct reports' dialog box with three steps: 1. Supervisors, 2. Direct reports, and 3. Review. The first step, 'Supervisors', is active. The question is 'Which supervisors do you want to transfer direct reports to?'. There is a search bar with 'ClearID Supervisor2' entered and a 'Type to search...' placeholder. Below the search bar, it says '1 / 20'. There is a 'Reason' field with 'Change of job role.' entered. Below the reason field, it says '19 / 235'. At the bottom left is a 'Close' button and at the bottom right is a 'Next' button.

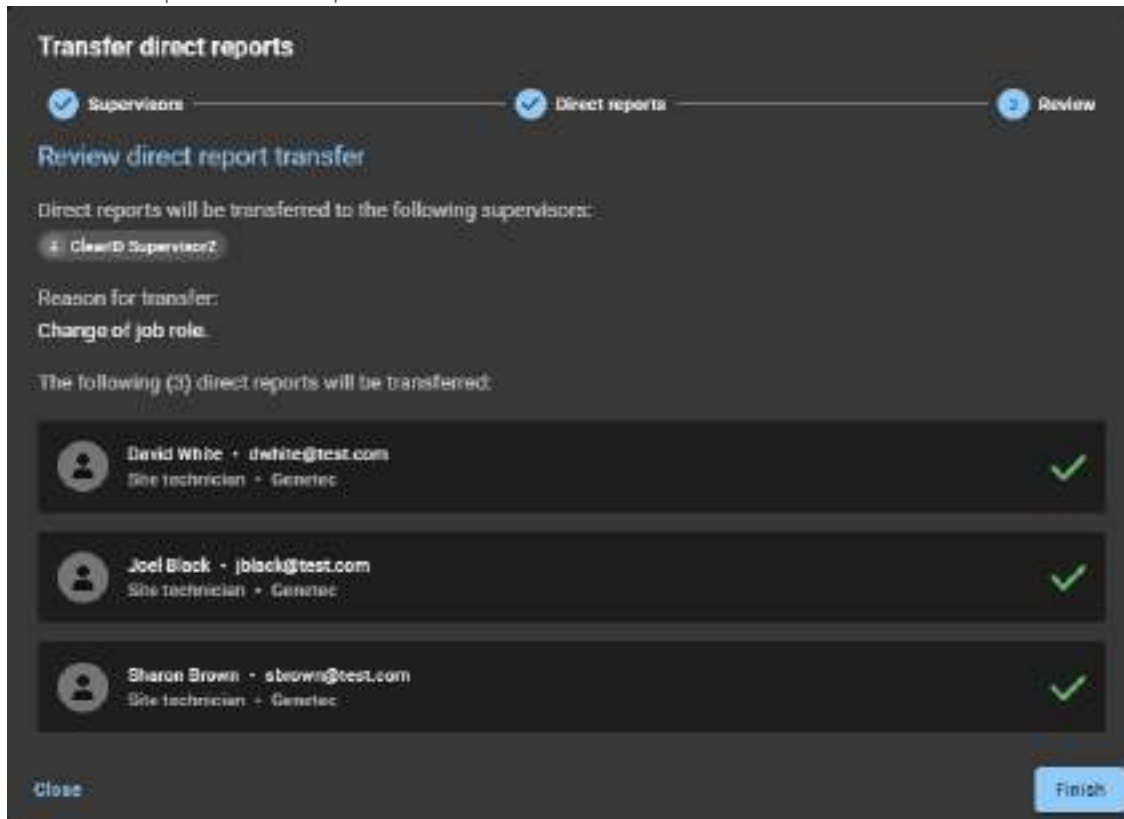
4. In the Direct reports section, select the direct reports you want to transfer and click Next.

The screenshot shows the 'Transfer direct reports' dialog box with three steps: 1. Supervisors, 2. Direct reports, and 3. Review. The second step, 'Direct reports', is active. The question is 'Which direct reports do you want to transfer?'. There is a list of three direct reports, each with a checkbox and a plus icon. The first report is 'David White - dwhite@test.com, Site technician - Genetec'. The second report is 'Joel Black - jblack@test.com, Site technician - Genetec'. The third report is 'Sharon Brown - sbrown@test.com, Site technician - Genetec'. All three reports are selected. At the bottom left is a 'Close' button and at the bottom right are 'Back' and 'Next' buttons.

5. In the Review section, verify the details of the direct reports that you want to transfer.

The screenshot shows the 'Transfer direct reports' dialog box with three steps: 1. Supervisors, 2. Direct reports, and 3. Review. The third step, 'Review', is active. The question is 'Review direct report transfer'. It says 'Direct reports will be transferred to the following supervisors:'. Below this, there is a search bar with 'ClearID Supervisor2' entered. Below the search bar, it says 'Reason for transfer: Change of job role.'. Below the reason, it says 'The following (3) direct reports will be transferred:'. Below this, there is a list of three direct reports, each with a plus icon and a minus icon. The first report is 'David White - dwhite@test.com, Site technician - Genetec'. The second report is 'Joel Black - jblack@test.com, Site technician - Genetec'. The third report is 'Sharon Brown - sbrown@test.com, Site technician - Genetec'. At the bottom left is a 'Close' button and at the bottom right are 'Back' and 'Transfer' buttons.

- a. (Optional) If you need to make some additions or changes, click Back to return to previous steps.
 - b. If no further changes are required, click Transfer to initiate the transfer.
6. Click Finish to complete the transfer request.



Example



After you finish

View the new supervisors identity to check that the direct reports were transferred successfully.
Browse

- Granting additional permissions for identities and roles in ClearID
- Granting additional permissions for supervisors in ClearID

5.25 | About direct reports report in ClearID

In Genetec ClearID™, a direct reports report is a list of identities of employees that report to a supervisor. The report includes information about direct reports, delegated direct reports, job titles, companies, and access control status.

Organization / Overview **Users** **Groups** **Roles** **Workflows** **Event types** **Automation** **User permissions** **Role management** **Connected** **Log**

Search users, groups, roles, workflows, event types, automation, user permissions, role management, connected, log

Transfer event type **connected 1/2**

Event report ▼	API title Description	Category Primary role	Action control status ▼
APIs	16 Task Engineering	Service	active
Workflows	26 Engineering	Service	active
Event type	10 Industrial technology	Role	active
API details	27 Support (Internal)	Service	active
APIs list			active request via API (1/2/3/4)
APIs list	10 Industrial technology	Support (Internal)	active request via API (1/2/3/4)
Log	10 Monitoring	Service	active

Direct reports report

The direct reports report is used by supervisors to view their direct reports to check their access control status and general identity information. The report can also be used to provide direct reports information to auditors.

Filters can be used to help refine the search results by direct reports (or delegated direct reports) and access control status (active or inactive).
Browse

- Viewing direct reports in ClearID

5.26 | Resetting user passwords in ClearID

If you're unable to authenticate while signing in to an account managed by Genetec ClearID™, you can reset your password.

What you should know

Password reset is only available for users with accounts managed by ClearID. Use industry best practices for creating strong passwords.

NOTE: This procedure isn't applicable to corporate single sign-on.

Procedure

1. In a web browser, do one of the following:
 - o If you have a production account, got to <https://portal.clearid.io>.
 - o If you have a demo or test account, go to Go to <https://demo.clearid.io>.
2. Enter your email address and click Sign in.

You're redirected to the new Genetec™ sign in page.

A screenshot of the Genetec sign-in page. The page has a dark blue background. At the top left is the Genetec logo. Below it is the text "Sign in to your account". There are two input fields: "Email address" with the text "johnDoe@gmail.com" and "Password". Below the password field is a link "Forgot password?" which is highlighted with a yellow rectangular box. Below the link is a blue "Sign in" button. At the bottom left is the copyright notice "© 2024 Genetec Inc. All rights reserved." and at the bottom right is a link "Privacy Policy".

3. Click Forgot password?.
You're redirected to the Reset password page.
4. On the Reset password page, click Send code to receive an email with a verification code.
 - a. Enter the verification code in the Verification code field on the Reset password page.
 - b. Click Verify code.
 - c. After your email is validated, click Continue.

A screenshot of the Genetec reset password page. The page has a dark blue background. At the top left is the Genetec logo. Below it is the text "Reset password". Underneath is the message "Your email address has been validated." Below this message are two buttons: a white "Cancel" button and a blue "Continue" button. The "Continue" button is highlighted with a yellow rectangular box. Below the buttons is the text "Please wait". At the bottom left is the copyright notice "© 2024 Genetec Inc. All rights reserved." and at the bottom right is a link "Privacy Policy".

5. Enter and confirm your new password, then click Continue.

Results

You can now access ClearID using the password you created.

5.27 | About email notifications in ClearID

Genetec ClearID™ sends email notifications to inform users about specific system events related to access, identities, roles, and visits.

Email notifications are sent from noreply@clearid.io. If you don't receive email notifications in either your Inbox or Spam (Junk) folders, contact your *account administrator*.

To opt out of or resubscribe to email notifications, see [Configuring your ClearID email notification preferences](#)

The following events can trigger email notifications:

Trigger event for notification	Possible notification recipients
Activity Summary	
Weekly activity summary NOTE: - The weekly activity summary summarizes all pending tasks or requests related to visit events, identity requests, or area access requests that require approval. You don't receive these notifications if you have no tasks or requests. - Weekly activity summary emails are sent every Monday at 9:00 am based on the identity's primary site. If no primary site is set, the email is sent at 9:00 am GMT.	- Requesters - Visit approvers - Supervisors - Identity approvers - Area owners - Area managers - Role managers
Access for an identity	
Account is created for an identity IMPORTANT: If a corporate log on (single sign-on using Microsoft Office 365 or similar) is used, the account is automatically activated and no activation email is received.	- Identity - Account administrators
Area access request for an identity is submitted	Identity requester
Area access request for an identity is canceled	- Identity requester - Area managers - Area owners
Area access request for an identity requires approval or denial Tip: - No email is sent if the request is auto-approved. - The email recipient depends on the system's workflow settings.	- Supervisors - Area managers
Area access request for an identity is approved or denied NOTE: If the person who submits an access request and the identity the access request is for are different, both receive the email.	- Identity - Area owners
Area access for an identity is granted	- Identity - Identity supervisors
Area access for an identity is revoked (or expired) NOTE: Access expired emails are sent at midnight based on the time zone specified for the site.	- Identity - Identity supervisors
Access for a role	
Access request submitted for a role NOTE: Both <i>role owners</i> and <i>role managers</i> can request access for roles. The user who made the request receives the email.	- Role managers - Role owners
Area access request for a role requires approval or denial	- Supervisors - Area managers
Area access request for a role is approved or denied	Approved:

Genetec ClearID®; User Guide

Displayed in the header

Trigger event for notification	Possible notification recipients
NOTE: <i>Supervisors</i> or <i>area managers</i> must approve or deny the request.	• <i>Area managers</i> Denied: • <i>All Role managers</i>
Area access granted for role NOTE: <i>Area managers</i> can approve area access requests for roles, or the requests can be auto-approved. A role can also be manually granted access to an area.	• <i>All Role managers</i>
Area access revoked for a role	• <i>All Role managers</i>
Identity added to role membership	• Identity
Identity removed from role membership	• Identity
Identity requests	
Identity requested NOTE: If one of the requested identities is canceled, all configured approvers are added to the Cc list of the identity request approval and completion email. The subject of the email is: "Identity request for <i>identity</i> has been updated".	• Requester • <i>Supervisors</i> (if configured in the identity template) • <i>Identity approvers</i> (if configured in the identity template)
Visit events	
Visit created	• Requester • Hosts
Visit requires approval or denial NOTE: No email is sent if the request is auto-approved.	• <i>Supervisors</i>
Visit approved or denied	• Requester • Hosts
Visitor confirmation	• Visitor
Visit request requires approval or denial NOTE: No email is sent if the visit is auto-approved.	• <i>Area managers</i> (depending on workflow) • <i>Visit approvers</i> (depending on workflow)
Visitor checked-in	• Hosts
Visitor watchlist alert (notify or block)	• <i>Watchlist managers</i>
Access reviews	
Access review pending	• <i>Area managers</i> • <i>Role managers</i>

Browse

- [Configuring your ClearID email notification preferences](#)
- [Configuring email notification preferences in ClearID \(administrator\)](#)

5.27.1 | Customizing the email banner for sites in ClearID

You can customize the email banner image that is used for access requests and visitor requests email notifications sent for the site.

Before you begin

Configuring the ClearID Self-Service Kiosk iPad

Tip: Ensure that your email banner image meets the requirements described in the  tooltip on the Images page of the Genetec ClearID™ web portal.

What you should know

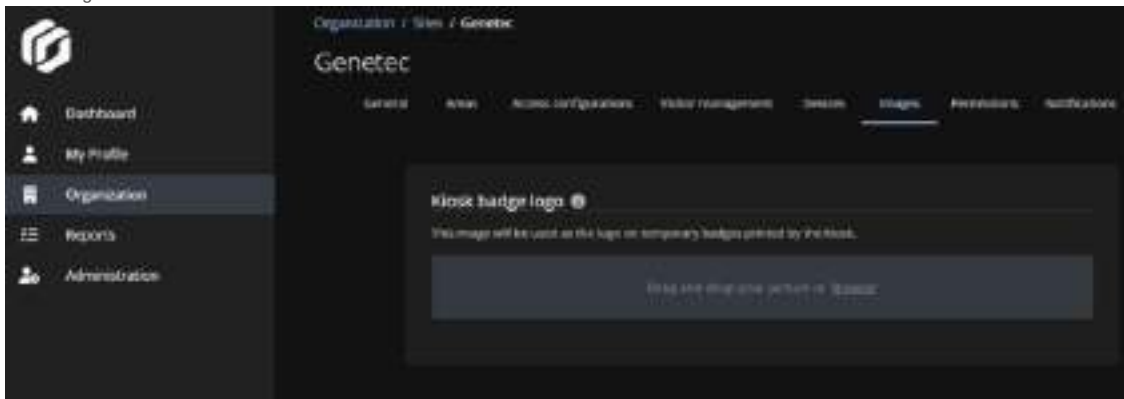
Only a site owner or account administrator can customize email banners.

- Customized email banner changes are synchronized with your site every 60 seconds.

Best Practice: For optimum results, use transparent .PNG images when customizing your email banner.

Procedure

1. In the ClearID web portal, click Organization > Sites.
2. Search for and select a site.
3. Click Images.



- a. In the Email banner section, drag and drop your picture or browse to select the Email banner image.
- b. Click Save.

The following example shows an email banner with a custom image.



Parent topic: About email notifications in ClearID

5.27.2 | Configuring email notification preferences in ClearID (administrator)

Genetec ClearID™ portal users receive email notifications for visit requests, access requests, activity summaries, and more. *Account administrators* can decide which notifications users receive by default and whether users can opt out of email notifications.

What you should know

Only *Account administrators* can configure which email notifications are sent out and which stakeholders receive them, where applicable.

Procedure

1. In the ClearID portal, click Administration > Notifications.
2. In the Emails and recipients section, configure your preferences as needed:

Enabled

Turn on the Enabled option to send an email notification to users by default.

Can opt out

Turn on the Can opt out option to allow users to opt out of a notification in their personal email notification preferences.

NOTE: You can only allow users to opt out of a notification type if the Enabled option for that notification is turned on.

3. Where applicable, choose which stakeholders receive the notification email.



4. Click Save.

Parent topic: [About email notifications in ClearID](#)

Browse

- [About email notifications in ClearID](#)

5.27.3 | Configuring your ClearID email notification preferences

You receive email notifications for visit requests, access requests, various activity summaries, and more from Genetec ClearID™. You can decide which notifications you want to receive and configure your notification preferences accordingly.

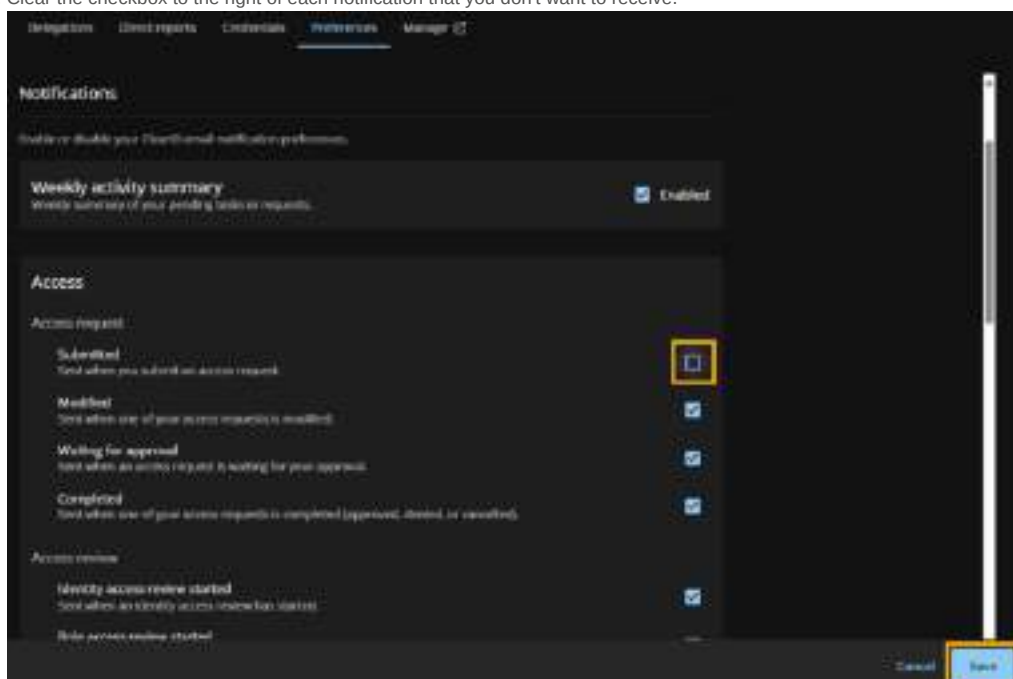
What you should know

Your notification preferences only apply to your user profile. All email notifications are turned on by default.

Tip: Use the Weekly activity summary email to keep track of your pending tasks and requests.

Procedure

1. In the ClearID web portal, click My Profile > Preferences.
2. In the Notifications section, configure your notification preferences as needed.
 - a. Clear the checkbox to the right of each notification that you don't want to receive.



3. Click Save.

Parent topic: [About email notifications in ClearID](#)
[Browse](#)

- [About email notifications in ClearID](#)

5.28 | About delegation in ClearID

In Genetec ClearID™, delegation is the process of transferring Genetec ClearID™ tasks within your organization, for example, due to a vacation or sabbatical. Tasks may be transferred among site owners, area owners, area managers, role owners, role managers, supervisors, and visit event approvers.

Planned delegation

In this situation, the delegation requirement is known about in advance and is planned for by the permission owner. For example, a planned vacation, sabbatical, or maternity leave.

A delegate is then temporarily given the same permissions as the person delegating responsibility so that they can manage the delegated tasks.

New delegation from Erika Della Cioppa

Delegating from Erika Della Cioppa to
Jack

From: 05/23/2025 To: 05/31/2025

Comments
On vacation until June 2025.
28 / 300

Close Create

For example, if an area manager delegates to you, you are temporarily given permissions to perform that area manager's tasks. The delegated tasks are then displayed in the My tasks section of your Dashboard.

Permissions for *user* delegated to others

- If required, you can delegate to more than one person. This can be useful when tasks are performed by multiple people. For example, different supervisors or shift workers.
- You cannot delegate tasks that have been delegated to you because this would potentially create a trust conflict. When you create a delegation you are only delegating your own tasks.
- The delegation period can be modified (✎) or turned off (✖) early if your delegation requirements change.



Permissions delegated to user

Permissions can also be delegated to you from another person.

NOTE: You cannot delegate permissions to a user that is already delegating to you. In this situation, the following error message is displayed: The specified user is already delegating permissions to you. That delegation must be removed before you can delegate to them.

Unplanned delegation

From time to time, an unplanned delegation might be required because the delegator is not available to set the delegation. For example, in the event of an unplanned absence or period of unavailability. In this situation, an account administrator can perform a delegation on behalf of an unavailable delegator. The account administrator can also modify or remove a delegation if required.

IMPORTANT: Administrator permissions cannot be delegated. You can only assign administrator permissions through the normal official channels.

Delegation email notifications

Any email notifications associated with delegated tasks are sent to both the original permission owner and the delegate. Using these email notifications or the My tasks page, the delegate can access and perform the delegated tasks.

Email notifications sent to delegates include contact details in the email notifications footer so that the delegate can contact the permission owner if they want to request changes to the delegation configuration.



5.29 | Delegating ClearID tasks to another user

Site owners, area owners, area managers, role owners, role managers, supervisors, and visit event approvers can temporarily transfer their Genetec ClearID™ task responsibilities to someone else in their organization by delegating their tasks to another user. For example, during a planned vacation, sabbatical, and so on.

Before you begin

[Learn about delegation.](#)

Best Practice: Before delegating your tasks, consider contacting the potential delegate to make them aware of the delegation and confirm their availability.

What you should know

- Only the logged in user can delegate their ClearID tasks to one or more users.
- The delegation period can be modified (📅) or turned off (❌) early if your delegation requirements change.
- An account administrator can also perform an unplanned delegation on the behalf of an unavailable delegator. For example, in the event of an unplanned absence or period of unavailability.

IMPORTANT: Administrator permissions cannot be delegated. You can only assign administrator permissions through the normal official channels.

Procedure

1. From the Dashboard, click My Profile > Delegations.
2. Click Add delegation.
3. Complete the fields

New delegation from Erika Della Cioppa

Delegating from Erika Della Cioppa to
Search for a name...

From * 05/23/2025 To MM/DD/YYYY

Comments
0 / 300

Close Create

- a. Search for or enter the name of the user that you want to delegate your ClearID tasks to.
- b. Enter the From and To dates for the period of time that you want the delegation in place.
- c. In the Comments field, add an explanation about why your tasks are being delegated to other users.

New delegation from Erika Della Cioppa

Delegating from Erika Della Cioppa to
Jack

From * 05/23/2025 To 05/31/2025

Comments
On vacation until June 2025.
28 / 300

Close Create

4. Click Create.



5. (Optional) In the Permissions for *user name* delegated to others section, click  to modify an active delegation.

- Enter the From and To dates for the period of time that you want the delegation in place.
- In the Comments field, add an explanation about why your tasks are being delegated to other users.
- Click Update to save your changes.

Your delegation is now active and will automatically expire on the date specified.

6. (Optional) Click  to remove a delegation.

- In the Remove delegation dialog, click Remove to confirm the delegation is no longer required.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.

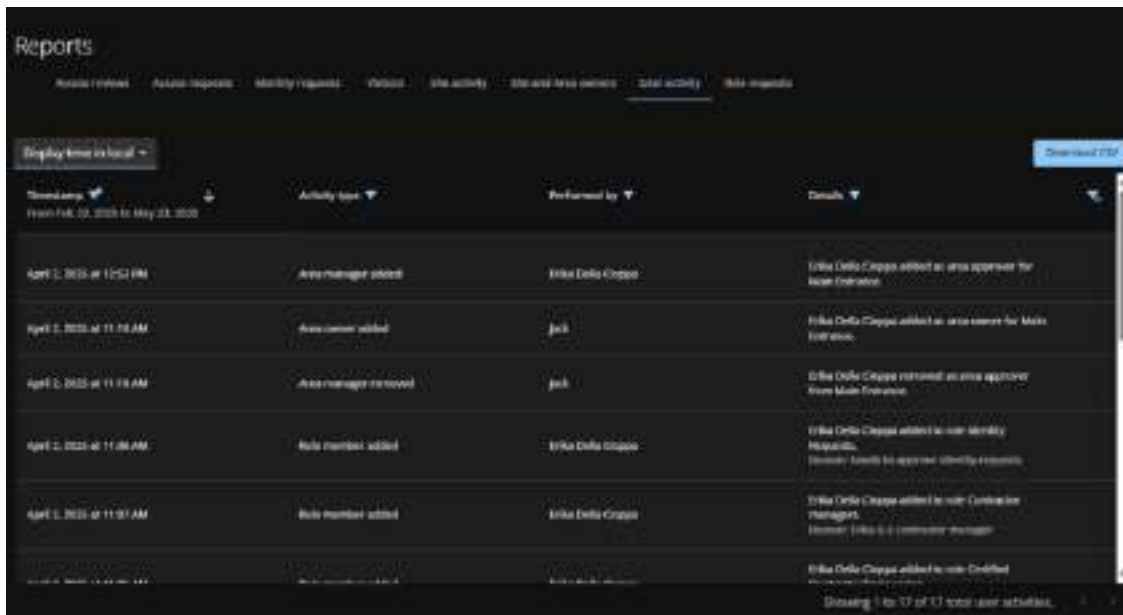
Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

5.30 | About user activity report in ClearID

In Genetec ClearID™, a user activity report is an audit trail of all activities related to users. The report includes timestamp information, activity type, who activity was performed by, and a details section including reason information.

User activity report



Timestamp	Activity type	Performed by	Details
April 1, 2023 at 11:57 AM	Area manager added	Ulrika Della Cappa	Ulrika Della Cappa added as area approver for Main Entrance
April 1, 2023 at 11:58 AM	Area owner added	jack	Ulrika Della Cappa added as area owner for Main Entrance
April 1, 2023 at 11:58 AM	Area manager removed	jack	Ulrika Della Cappa removed as area approver from Main Entrance
April 1, 2023 at 11:58 AM	Role member added	Ulrika Della Cappa	Ulrika Della Cappa added to role Identity Requests. (Security Alerts) to approve Identity Requests
April 1, 2023 at 11:58 AM	Role member added	Ulrika Della Cappa	Ulrika Della Cappa added to role Customs Managers. (Homes) Ulrika is a contractor manager
April 1, 2023 at 11:58 AM	Role member added	Ulrika Della Cappa	Ulrika Della Cappa added to role Certified Access Control (Access Control) (Access Control)

As an account administrator, you can use this report to view all data corresponding to the following activities:

- Area owner added or removed
- Area manager added or removed
- Identity access granted or removed
- Role access granted or removed
- Role owner added or removed
- Role manager added or removed
- Role member added or removed
- Supervisor added or removed
- Identity created, updated, or deleted
- Custom field created, updated, or deleted
- Custom field section created, updated, or deleted

You can use filters to help refine the report search results by timestamp, activity type, performed by, and details.

Browse

- [Viewing a user activity report in ClearID](#)

5.31 | Viewing a user activity report in ClearID

You can consult the User activity report to review all user-related activities. Use the report for auditing purposes, download a copy to attach to an audit request to review offline, or manipulate or consolidate data in a spreadsheet for other audiences.

Before you begin

To view the User activity report and review audit trail information, ensure that you're an account administrator.

NOTE: The User activity report is empty if there is no activity logged by area owners or managers, role managers, or role members in your Genetec ClearID™ system.

Procedure

1. From the Home page, click Reports > User activity.

The screenshot shows the 'Reports' section of the Genetec ClearID interface. At the top, there are tabs for 'Area manager', 'Area manager', 'Identity request', 'Access', 'Site activity', 'Site and Area owners', 'Total activity', and 'Area manager'. The 'Total activity' tab is selected. Below the tabs, there is a 'Display time in local' dropdown menu and a 'Download CSV' button. The main table displays a list of activities with columns for 'Timestamp', 'Activity type', 'Performed by', and 'Details'. The table shows several entries related to area manager and role member additions and removals. At the bottom, it indicates 'Showing 1 to 17 of 17 total user activities'.

Timestamp	Activity type	Performed by	Details
April 2, 2021 at 11:52 AM	Area manager added	Mike Della Cappa	Mike Della Cappa added as area manager for Main Entrance.
April 2, 2021 at 11:51 AM	Area manager added	jack	Mike Della Cappa added as area manager for Main Entrance.
April 2, 2021 at 11:51 AM	Area manager removed	jack	Mike Della Cappa removed as area manager from Main Entrance.
April 2, 2021 at 11:50 AM	Role member added	Mike Della Cappa	Mike Della Cappa added to role Identity Request. Identity Request is approved Identity Request.
April 2, 2021 at 11:51 AM	Role member added	Mike Della Cappa	Mike Della Cappa added to role Custom for managers. Manager: Mike D. C. (operator manager)
April 2, 2021 at 11:51 AM	Role member added	Mike Della Cappa	Mike Della Cappa added to role Custom for managers. Manager: Mike D. C. (operator manager)

2. In the User activity report tab, select the display time setting that you require.

Display time in local

Report times are displayed using the system time from the computer of the logged-in user.

Display time in UTC

Report times are displayed using Coordinated Universal Time (UTC).

3. Filter the report based on your required criteria:

Timestamp

In the Timestamp column, click  to filter the results by date. Select a pre-defined date range from the choices available or enter a specific date range using the date range picker.

The screenshot shows a date range picker interface. It has five radio buttons for pre-defined date ranges: 'Last 24 hours', 'Last 7 days', 'Last 30 days', 'Last 90 days', and 'Last 365 days'. The 'Date range (UTC)' option is selected. Below these options, there is a date range picker with 'From' and 'To' fields. The 'From' field is set to '10/21/2021' and the 'To' field is set to '10/22/2021'. The time for both fields is '6:25 PM'. At the bottom, it says 'Time period limited to a maximum of one year'.

(Optional) Use the sort icons ( and ) to display the results in descending or ascending order.

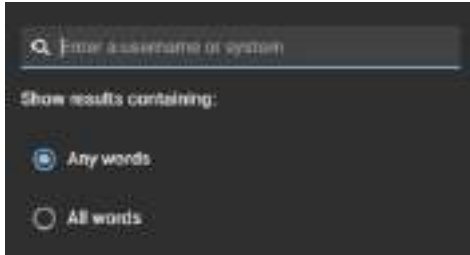
Activity type

In the Activity type column, click  to filter the results by activity type:

- o Area owner added or removed
- o Area manager added or removed
- o Identity access granted or removed
- o Role access granted or removed
- o Role owner added or removed
- o Role manager added or removed
- o Role member added or removed
- o Supervisor added or removed
- o Identity created, updated, or deleted
- o Custom field created, updated, or deleted
- o Custom field section created, updated, or deleted

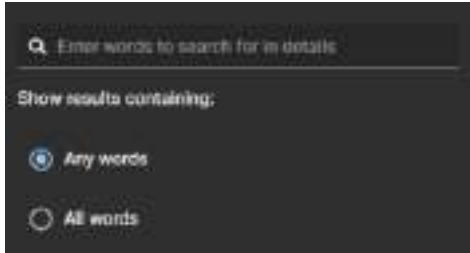
Performed by

In the Performed by column, click  to open a search dialog and filter the results by who performed an activity. For example, search for tasks performed by a particular user, or tasks performed automatically by the system.



Details

In the Details column, click  to open a search dialog to search the details or reason using a search criteria.



(Optional)

Click  to reset filter selections.

- Click Download CSV to download a copy of the User activity report.

Follow your browser prompts to complete downloading the exported file.

The file is exported as a .CSV file to the default download location for your browser. By default the exported file is created using the report name and download date. For example, UserActivities_2022-02-14.csv.

NOTE: The columns and entries in the CSV file can vary depending on the filters you selected when you downloaded the report.

Browse

- About user activity report in ClearID

5.32 | User levels in ClearID

The following information can be used to help you understand which actions the users or roles in Genetec ClearID™ can perform.

Identity management

Actions	Account owners (and API key)	Site owners	Area owners	Area managers	Identity supervisors	Authenticated users
Create identities	✓ ¹					
Update identities	✓ ¹					
View private information about identities	✓ ¹					
List identities when adding to an area or role	✓ ¹	✓	✓	✓	✓	✓
Create sites	✓ ¹					
Delete identities	✓ ¹					

Genetec ClearID™ User Guide

Displayed in the header

Actions	Account owners (and API key)	Site owners	Area owners	Area managers	Identity supervisors	Authenticated users
View direct reports	✓ ¹				✓	
Manage direct reports	✓ ¹				✓	
Transfer direct reports	✓ ¹				✓	

¹ Users assigned as a delegate for another user do not inherit the permission.

Area management

Actions	Account owners (and API key)	Site owners	Area owners	Area managers	Identity supervisors	Authenticated users
Create and delete sites	✓ ¹					
Edit site details	✓ ¹	✓				
Assign site owners	✓ ¹	✓ ¹				
Create and delete areas	✓ ¹	✓				
Edit area automatic provisioning attributes	✓ ¹	✓				
Edit area name	✓ ¹	✓				
View all private areas of a site	✓ ¹	✓				
Assign area owners	✓ ¹	✓				
Assign area managers	✓ ¹	✓	✓ ¹			
Edit area visibility (Public or Private)	✓ ¹	✓	✓			
Edit approval workflow	✓ ¹	✓	✓			
Edit area schedules	✓ ¹		✓			
View area configuration and access list	✓ ¹	✓	✓	✓		
Add people or roles to areas	✓ ¹		✓	✓		
Remove people or	✓ ¹		✓	✓		

Actions	Account owners (and API key)	Site owners	Area owners	Area managers	Identity supervisors	Authenticated users
roles from areas						
Approve access request for an area	✓ ¹			✓	✓	
Edit period and schedule before approving access request	✓ ¹			✓	✓	
Schedule area access reviews	✓	✓				
Receive and complete area access reviews	✓ ¹	✓	✓	✓		
View area access reviews report	✓	✓				

¹ Users assigned as a delegate for another user do not inherit the permission.

Role management

Actions	Account owners (and API key)	Site owners	Role owners	Role managers	Identity Supervisor	Any user on account
Create and delete roles	✓ ¹					
Assign role owners	✓ ¹					
Assign role managers	✓ ¹		✓ ¹			
Change automatic provisioning rules and configuration for a role	✓ ¹		✓			
Edit role name, description, notes	✓ ¹		✓			
List roles when adding to an area or access request	✓ ¹		✓	✓		
Manually add or remove a person from a role	✓ ¹		✓	✓		

Actions	Account owners (and API key)	Site owners	Role owners	Role managers	Identity Supervisor	Any user on account
Submit an access request on behalf of a role			✓	✓		
Receive and complete role access reviews			✓	✓		
Remove identities from a role	✓ ¹		✓	✓		

¹ Users assigned as a delegate for another user do not inherit the permission.

Visitor management

Actions	Account owners (and API key)	Visit requester	Requester supervisor	Site owners	Visit hosts	Area managers
Visit event						
Create a visit event		✓ ¹				
Add guests to an event or remove guests from an event		✓ ¹			✓ ¹	
Approve or reject a visit event			✓			
Approve or reject specific guest access to an area						✓
Create an event (copy event) from an existing event		✓ ¹	✓		✓ ¹	
Cancel event		✓ ¹			✓ ¹	
View list of upcoming events		✓ ¹			✓ ¹	
View event details		✓ ¹	✓		✓ ¹	✓
Visitor management configuration						
Edit visitor management configuration (Area)	✓ ¹			✓		
Edit visitor management configuration (Site)	✓ ¹			✓		

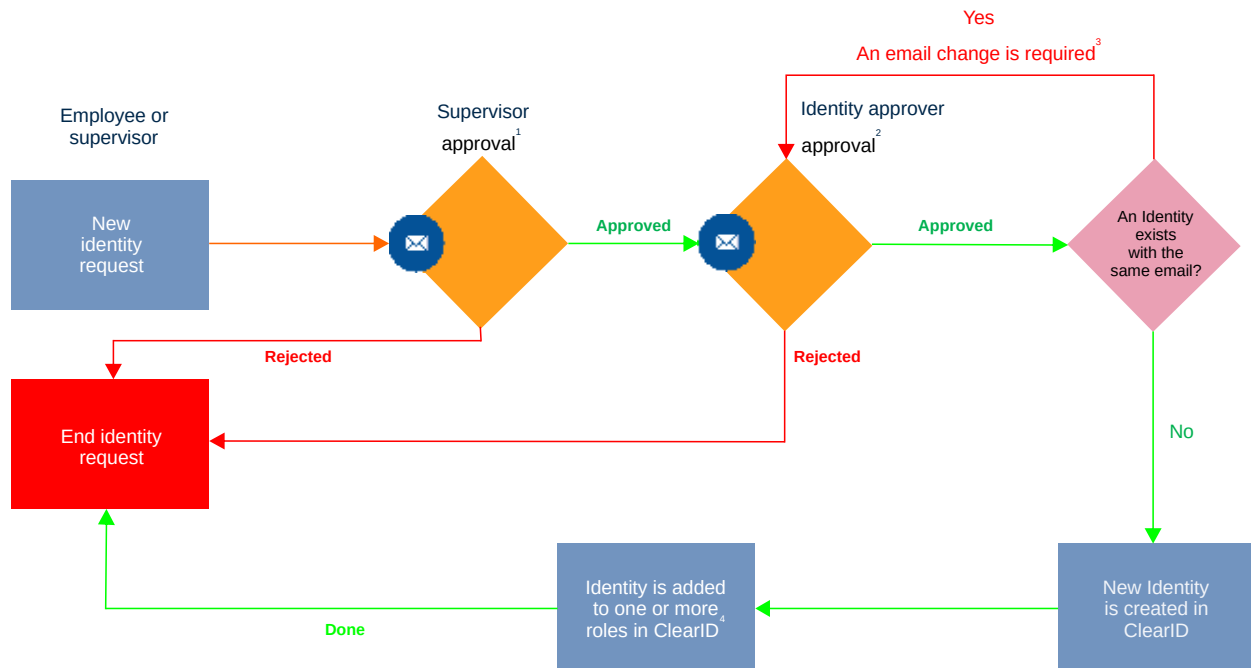
¹ Users assigned as a delegate for another user do not inherit the permission.

5.33 | About identity request workflow in ClearID

An identity request workflow is a series of activities performed by the system or authorized people during the life cycle of an identity request. The activities can create an individual identity, or multiple identities using a CSV import, and add each new identity to a role to inherit relevant access for a specified period.

The workflow helps automate identity request tasks, such as approving or rejecting identity requests, so that people involved in the review and approval process can focus on other tasks.

The following diagram illustrates the *identity request workflow* that occurs in Genetec ClearID™ and Synergis™.



¹ (Optional) Supervisor approval can be enabled and disabled for each identity template.

² (Optional) Identity approver approval can be enabled and disabled for each identity template.

³ (Optional) Email address must be unique in the system.

⁴ (Only if applicable) Cardholder is added to corresponding cardholder group in Security Center.

Browse

- [About workflows in ClearID](#)

Browse

- [Identity Request Feature Note \(2 pages\)](#)

5.34 | Creating an identity template in ClearID

Before you can submit an identity request, you must create your identity templates.

Before you begin

- Familiarize yourself with workflows.
- Create the roles that will be allowed to request identities.
- (Optional) Create roles containing the role access your identity templates will use.
- (Optional) If you want to use Supervisor approvals, add a supervisor for each identity that can request an identity.

What you should know

Only an account administrator can create an identity template.

Create identity templates to address the identity requests that your organization frequently encounters.

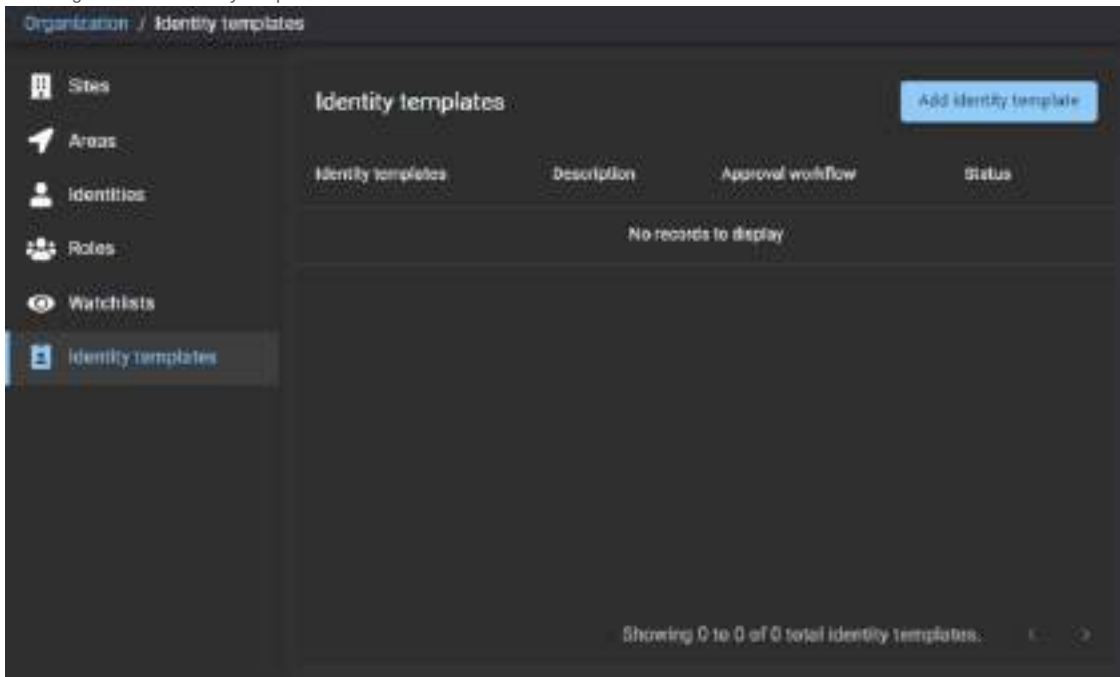
Genetec ClearID® User Guide

Displayed in the header

- You can create identity templates with predefined role access to suit different requirements. For example, identity requests for different types of contractors, or identity requests for large groups of specific employees who require access to a specific site or building.
- When an identity request is submitted using an identity template, the identity is added as a role member to the roles that apply to the template and inherits the associated role access.

Procedure

1. Click Organization > Identity templates.



2. Click Add identity template.
3. In the Identity template section, complete the fields or configure the settings as required:

The screenshot shows the 'New identity template' form. At the top, there's a progress indicator with three steps: 1. Identity template, 2. Permissions, and 3. Approval setting. The form fields include: 'Identity template name *' with the value 'Electrical contractors' and an 'Enabled' toggle switch; 'Description' with the value 'Electrical contractors for HQ Main Building'; and 'Form type *' with a dropdown menu set to 'Standard'. Below these are sections for 'Web portal access' (with a checked checkbox 'Enable option for web portal access') and 'Access control' (with checked checkboxes 'An expiry date is required' and 'Enforce a maximum duration for the period of access'). A text input field shows 'Limit the maximum duration to 365 days'. At the bottom left is a 'Cancel' button and at the bottom right is a 'Next' button.

Identity template name

Enter a name that summarizes the type of identity requests that the template is intended for. For example, Electrical contractors.

Description

Enter a meaningful description that describes the purpose of your template. For example, Electrical contractors for HQ Main Building.

Form type

Standard is the default.

Enabled

Move the slider to the Enabled position for this template to be available for selection when requesting an identity. Enabled is the default.

- a. In the Web portal access section, configure the option that you require.

Enable option for web portal access

Select the check box if you want to display the web portal access option when requesting an identity.

NOTE: When requesting multiple identities the availability of the web portal access option is dependent on your template configuration.

- If your template does not include the web portal access option, the web portal access fields are ignored.
- If your template does include the web portal access option, the web portal access fields are processed.

- b. In the Access control section, configure the options that you require.

An expiry date is required

Select the check box if you want to enforce an expiry date when creating identity requests.

Enforce a maximum duration for the period of access

Select the check box if you want to specify a maximum duration when creating identity requests.

Limit the duration to *nnn* days

Specify a maximum duration. For example, 365 days.

- c. Click Next.

4. In the Permissions section, configure the settings or add roles as required:

- a. In the Who can request this identity template? section, do one of the following:
- If you want all users to be able to select this identity template, select the All users can request identities check box.
 - If you want to select specific roles, click Add role.

NOTE: If you selected All users can request identities proceed to step 6.

5. If you clicked Add role, search for or select one or more roles and click Add.

NOTE: The roles that you add in the Who can request this identity template? section determine who can request identities using this template. For example, you might add a role, so that only *Contractor managers* can request identities. Another example could include buildings with tenants spaces, for that situation you might want to create *Tenant managers*.

6. (Optional) In the What roles do you need? section, add the roles that you require.
- a. Click Add role.
- b. Search for or select one or more roles and click Add.

Electrical contractors

Identity template Permissions Approval setting

Who can request this identity template?

☒ All roles can request identities

What roles do you need?

Identities created using this identity template are added as role members and inherit the associated role access

Add role

Role	Description
Certified Contractor Engineering	

Cancel Back Next

NOTE: The roles that you add in the What roles do you need? section determine the access that the identity inherits when an identity is requested using this template. For example, an electrical contractor role could be setup with access to rooms containing electrical infrastructure.

c. Click Next.

7. In the Approval setting section, select the Identity request approval workflow that you require.

New identity template

Identity template Permissions Approval setting

Identity request approval workflow

- No approval required
- Supervisor approval required
- Identity approvers approval required
- Supervisor and identity approvers approval required
- APT approval

No approval required
Automatically approved.

Supervisor approval required
Approved by the supervisor of the requester.
NOTE: If the requester has no supervisor (or is a trusted requester) the supervisor approval step is bypassed.

Identity approvers approval required
If selected, identity approvers must be added.
a. Click Add and choose either Add identities or Add roles.
b. Complete the steps as prompted.

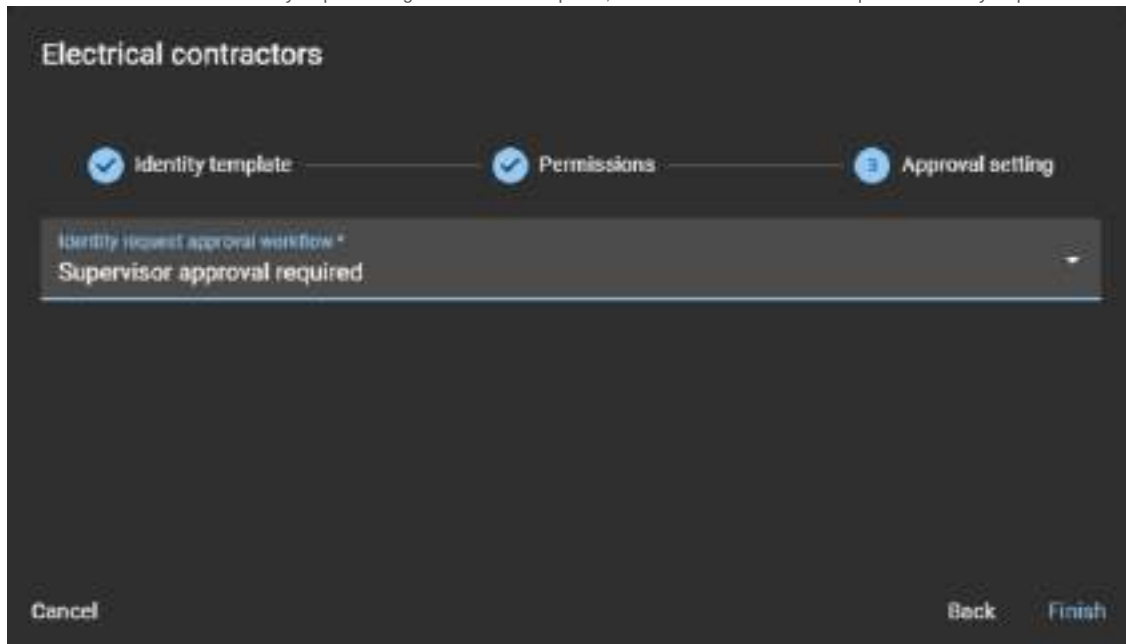
Supervisor and identity approvers approval required
If selected, supervisors are already associated with the identity, however the identity approvers must be added as described previously.
NOTE: If the requester has no supervisor (or is a trusted requester) the supervisor approval step is bypassed.

API approval

API approval is only used when the identity request approval workflow is customized to handle requests from an external service.

For example, Genetec ClearID™ LDAP Synchronization Agent, Genetec ClearID™ One Identity Synchronization Tool, or an API workflow for a plugin integration. In this situation, the request approvals are not shown in the ClearID user interface.

NOTE: If a user creates an identity request using the ClearID web portal, that user will still see their requests in the My requests dashboard.



8. Click Finish.

Results

Your template is now ready to be used.

Example



After you finish

Request an identity.

Browse

- Identity Request Feature Note (2 pages)

5.34.1 | Modifying an identity template in ClearID

After you have created your identity templates, you can modify the template settings or delete the template if required.

Before you begin

Create your identity templates.

What you should know

Only an account administrator can modify an identity template.

Procedure

1. Click Organization > Identity templates.
2. (Optional) If a template is no longer required click Delete (X) to delete the template.
3. Click a template in the list.
4. In the Identity template section, make any changes that you require and click Next.
5. In the Permissions section, make any changes that you require and click Next.
6. In the Approvals section, make any changes that you require and click Finish.

Parent topic: [Creating an identity template in ClearID](#)

5.35 | Requesting identities in ClearID

You can use the Genetec ClearID™ self-service portal to request an individual identity, or to request multiple identities using a CSV import. Using the self-service portal with optional approver workflow simplifies the approval process by only notifying the specified approvers.

Before you begin

- Familiarize yourself with workflows.

What you should know

Anyone with the required permission can submit an identity request.

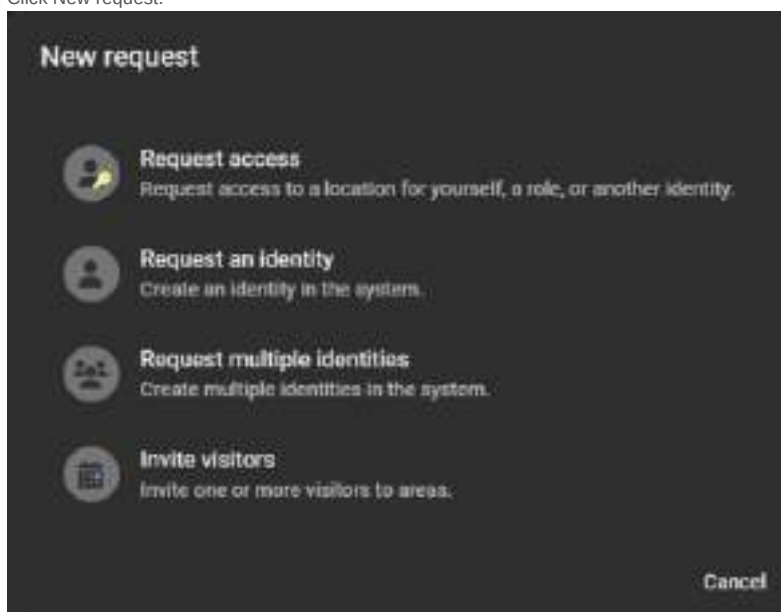
NOTE: In the past, most access control solutions would typically not track or record why an identity was required.

In ClearID the identity request includes: who requested the identity, when, and the reason for the identity request.

- Separate identity requests and approval workflows are created for each identity requested.
- After the request summary is confirmed, it is automatically assigned to the right individuals for approval.
- After the approval process occurs, the requester receives an email notifying them whether the identity request was approved or rejected.

Procedure

1. Log on to the self-service portal.
2. Click Dashboard.
3. Click New request.



4. In the New request dialog, do one of the following:
 - Requesting an identity in ClearID
 - Requesting multiple identities using a CSV import in ClearID
5. Click Finish.

Results

After you finish

Depending on the identity template that you selected, your identity requests are either approved automatically or approvers review identity requests and approve (or reject) as required.

Browse

- [Identity Request Feature Note \(2 pages\)](#)

Browse

- [Checking the status of identity requests in ClearID](#)

5.35.1 | Requesting an identity in ClearID

You can use the Genetec ClearID™ self-service portal to request an identity. This request adds someone (as an identity) that does not currently exist in the system. Using the self-service portal with an optional approver workflow simplifies the approval process by only notifying the specified approvers.

Before you begin

- [Familiarize yourself with workflows.](#)

What you should know

Anyone with the required permission can submit an identity request.

This task describes how to use the identity request wizard in the web portal to request an identity. The requester can use the wizard to add someone (as an identity) that does not already exist in the system.

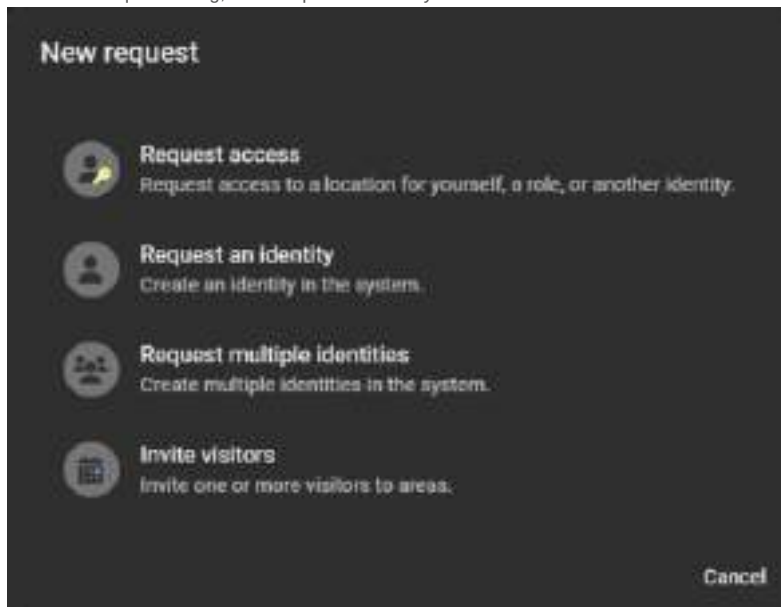
NOTE: In the past, most access control solutions for sites typically did not track or record why an identity was required.

In ClearID, the identity request includes: who requested the identity, when, and the reason for the identity request.

- Separate identity requests and approval workflows are created for each identity requested.
- After the request summary is confirmed, it is automatically assigned to the right individuals for approval.
- After the approval process occurs, the requester receives an email notifying them whether the identity request was approved or rejected.

Procedure

1. Log on to the self-service portal.
2. Click Dashboard.
3. Click New request.
4. In the New request dialog, click Request an identity.



5. In the New identity request wizard, select a template from the Identity template list and click Next.
6. In the General information section, complete the fields.

The screenshot shows a web interface for creating an identity request. At the top, a progress bar indicates four steps: 1. Identity template (completed), 2. General information (current step), 3. Work details, and 4. Review. The 'General information' section contains several input fields: 'First name' (John), 'Last name' (Doe), 'Email' (johndoe@test.com), 'Middle name' (empty), 'Mobile phone number' (123-456-7899), 'Preferred name *' (John Doe), and 'External ID' (empty). Below this is the 'Web portal access' section, which includes a slider for 'Grant user access to the web portal' set to 'N/A'. At the bottom left is a 'Save as draft' button, and at the bottom right are 'Back' and 'Next' buttons.

Tip: At any point during the creation of the request, you can click Save as draft to save an incomplete request (while waiting for missing information). Alternatively, you can click Delete if the request is no longer required. You can access your drafts from the My requests tab in the Dashboard.

7. (Optional) In the Web portal access section, move the Grant user access to the web portal slider to the Enabled position if you want to allow the identity being requested to be able to log on and use the ClearID web portal.

NOTE: The Grant user access to the web portal slider is disabled when the identity template you are using does not include the option for web portal access.

- a. If you enabled web portal access enter a user name.

NOTE: The user name must be a valid email address.

8. In the Access control section, complete the fields. Mandatory fields are highlighted with an asterisk (*).

Time zone

Select the time zone that you require.

Activation date

Select the date when the requested identity should be activated.

Expiration date

Select the date when the requested identity should be deactivated.

NOTE: Depending on the identity template selected, the expiration date might not be mandatory.

The screenshot shows the 'identity request' form. At the top, there are two input fields: 'Preferred name *' with the value 'John Doe' and 'External ID'. Below these is the 'Web portal access' section with a toggle switch for 'Grant user access to the web portal' set to 'N/A'. The 'Access control' section includes a 'Time zone *' dropdown set to 'America/Toronto (-05:00) [EST]'. A message states: 'A template policy limit is currently active, individual access is limited to 365 days.' Below this are 'Activation date *' (01/01/2022) and 'Expiration date *' (03/31/2022) fields, each with a calendar icon. A 'Duration' field shows '90 d'. At the bottom are 'Save as draft', 'Back', and 'Next' buttons.

NOTE: The identity activation and expiration times are dependent on and triggered by the access period specified in the identity request and the time in the selected time zone. If a *maximum duration* was specified and enabled in the identity template, a message is displayed to indicate the maximum period of access that you can specify.

a. Click Next.

9. In the Work details section, complete the fields.

The screenshot shows the 'New Identity request' form with a progress bar at the top indicating four steps: 'Identity template' (completed), 'General information' (completed), 'Work details' (current step), and 'Review'. The 'Work details' section contains three input fields: 'Company' (Sparky Sparks Electrical), 'Employee ID', and 'Job title' (Electrician). Below these are 'Department' (Electrical Contractors) and 'Country *' (Canada) fields. A section titled 'Supervisors of John Doe' shows a table with one entry: 'Fred Smith' with email 'fred.smith@test.com'. At the bottom are 'Save as draft', 'Back', and 'Next' buttons.

Company

Enter the company name.

Employee ID

Enter the Employee ID.

Job title

Enter the job title.

Department

Enter the department.

Country

Select a country from the list. This country setting is only used by the *Standard* form.

Tip: Enter the first letter of the country to jump to that part of the country list.

- In the Supervisors of section, click  to add supervisors.

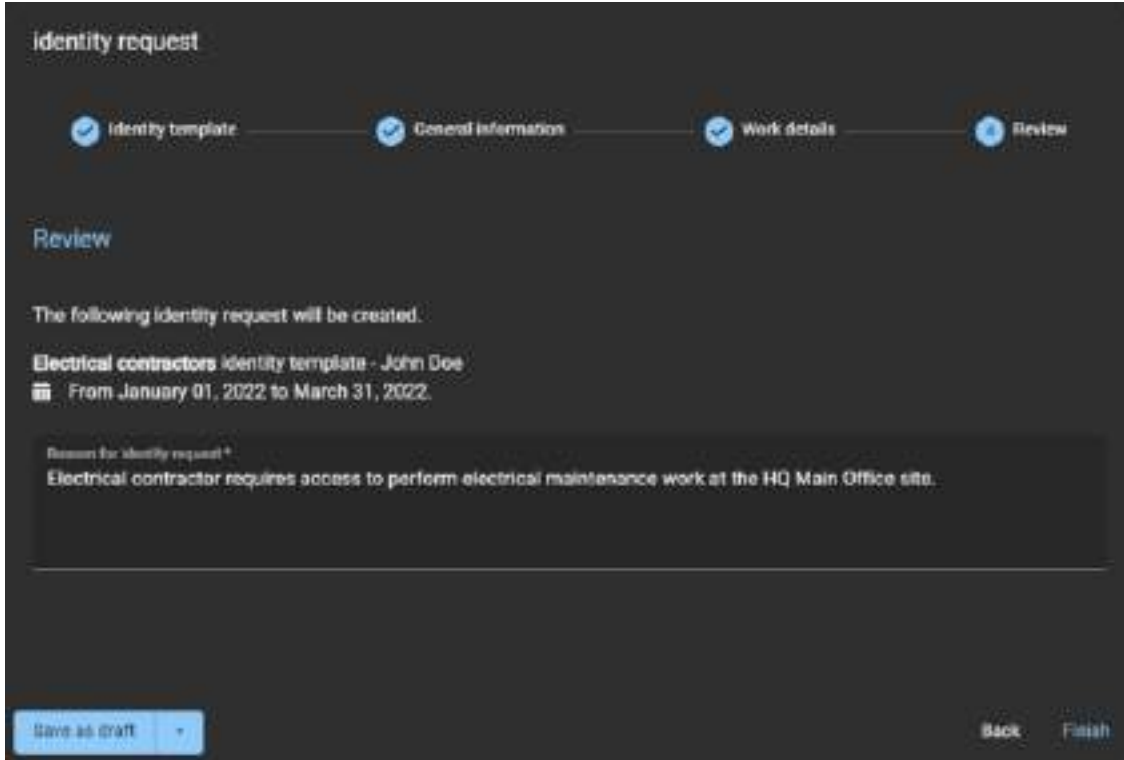
NOTE: The supervisors specified here are the supervisors of the new identity being created. The requester is automatically added to the Supervisors of list by default.

- (Optional) Add more supervisors as required.

- (Optional) Click  to remove any supervisors that are no longer required. For example, If you requested identities on behalf of someone else, you might remove yourself (if required) after the relevant supervisors are added.

- Click Next.

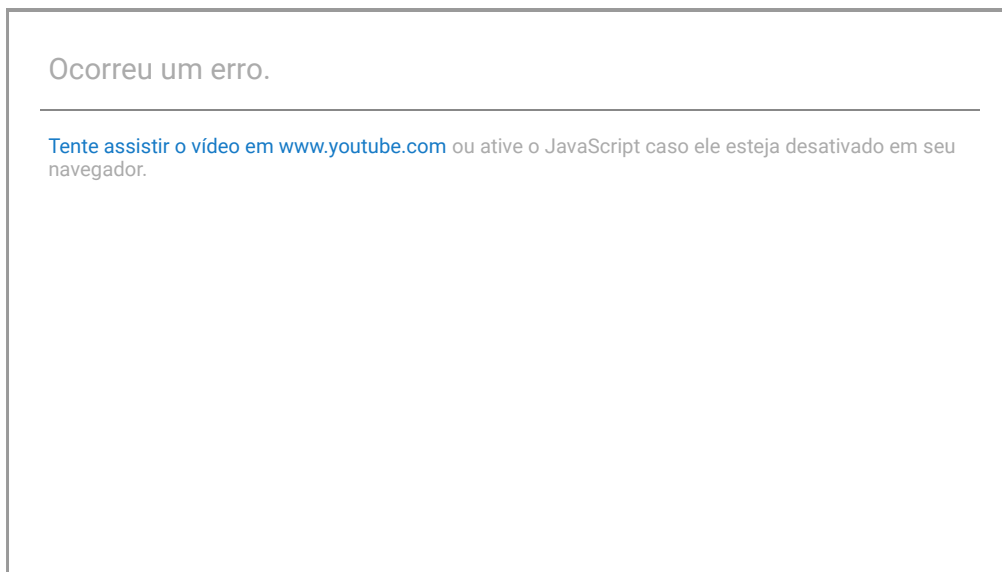
- In the Review section, verify that the identity request details are correct.



- If the details are correct, add a reason for the request and click Finish.

An email notification is sent to approvers (if applicable).

Example



After you finish

Depending on the identity template that you selected, your identity requests are either approved automatically or approvers review identity requests and approve (or reject) as required.

Parent topic: [Requesting identities in ClearID](#)

Browse

- Identity Request Feature Note (2 pages)

5.35.2 | Requesting multiple identities using a CSV import in ClearID

You can use the Genetec ClearID™ self-service portal to request multiple identities. This request adds multiple people (as identities) that do not currently exist in the system. Using the self-service portal with the optional approver workflow simplifies the approval process by only notifying the specified approvers.

Before you begin

- Familiarize yourself with workflows.

What you should know

Anyone with the required permission can submit an identity request.

This task describes how to use the identity request wizard in the web portal to request multiple identities using a CSV import. The requester can use the wizard to add people (as identities) that do not already exist in the system.

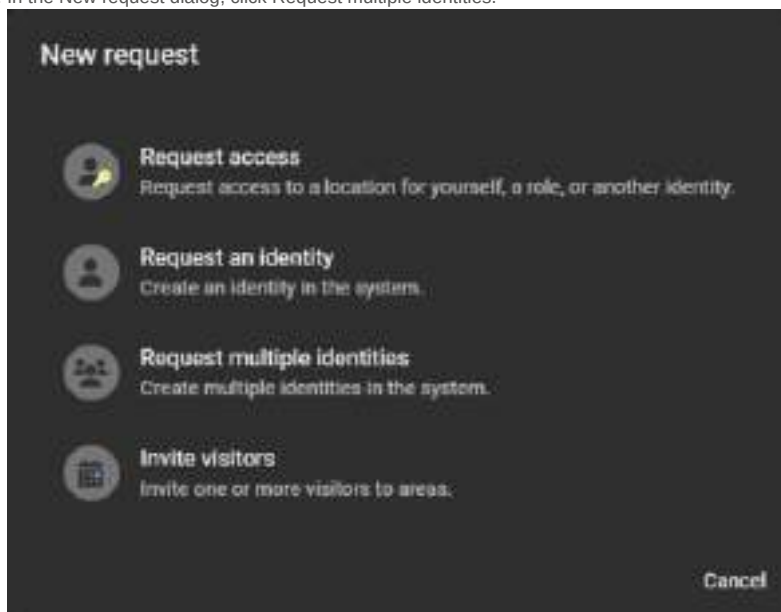
NOTE: In the past, most access control solutions would typically not track or record why an identity was required.

In ClearID, the identity request includes: who requested the identity, when, and the reason for the identity request.

- Separate identity requests and approval workflows are created for each identity requested.
- After the request summary is confirmed, it is automatically assigned to the right individuals for approval.
- After the approval process occurs, the requester receives an email notifying them whether the identity request was approved or rejected.

Procedure

1. Log on to the self-service portal.
2. Click Dashboard.
3. Click New request.
4. In the New request dialog, click Request multiple identities.



5. In the Request multiple identities wizard Basic information section, complete the fields.
 - a. In the Request name section Name field, enter a meaningful name for your request.

This meaningful name ensures that your request can be easily identified in the My requests or My tasks dashboards later.
 - b. In the Supervisors section, search for and select one or more identities to assign as supervisors for the imported identities. You can assign a maximum of 20 supervisors.

NOTE: The supervisors specified here are the supervisors of the new identities being created. The requester is automatically added to the Supervisors list by default.
 - c. In the Identity request template section, select a template from the list.
 - d. In the Reason for request section, add a reason for the request and click Next.

The screenshot shows the 'Request identities' form with three steps: 1. Basic Information, 2. Import, and 3. Review. Step 1 is active. The form includes a 'Request name' field with the value 'Renovation contractors (4th floor)', a 'Supervisors' section with an 'Add New' button, an 'Identity request template' dropdown set to 'Electrical contractors', and a 'Reason for request' text area with the text 'Electrical contractors for 4th floor renovations'. At the bottom are 'Cancel' and 'Next' buttons.

Request identities

1 Basic Information 2 Import 3 Review

Request name
Enter a meaningful name for your request so that it can be easily identified in the "My requests" or "My team" dashboards later.

Name *
Renovation contractors (4th floor)

Supervisors
Start typing in the Identities field to search for and select the supervisors that you require for the new identities being created.

Identities
+ Add New
1 / 35

Identity request template

Template *
Electrical contractors

Reason for request

Reason *
Electrical contractors for 4th floor renovations

Cancel Next

6. In the Import section, click Import from CSV.

The screenshot shows the 'Request identities' form with three steps: 1. Basic Information, 2. Import, and 3. Review. Step 2 is active. The form has a heading 'Import identities' and a warning message about CSV imports. An 'Import from CSV' button is in the top right. Below is a table with the message 'No records to display'. At the bottom are 'Cancel', 'Back', and 'Next' buttons.

Request identities

1 Basic Information 2 Import 3 Review

Import identities
Import your identities for this request below. If any data errors are encountered during the identities import, fix the issues in the CSV file then import the file again. CAUTION: Importing the file again overwrites any data already imported into the grid.

Import from CSV

No records to display

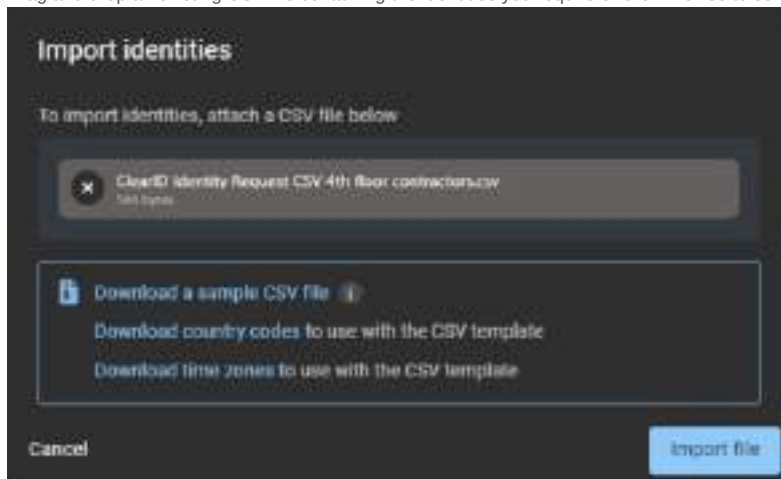
0 total results.

Cancel Back Next

NOTE: You can import a maximum of 1000 identities per identity request.

7. Choose one of the following:

- Use an existing CSV file.
 - Download a sample CSV file.
8. If you chose to use an existing CSV file, do the following:
- a. Drag and drop an existing CSV file containing the identities you require or click Browse to select the file you require.



- b. Click Import file to import the identities list.
9. Review the imported identities data and check for any errors.
- NOTE: When requesting multiple identities, the availability of the web portal access option depends on your template configuration.
- If your template does not include the web portal access option, the web portal access fields are ignored.
 - If your template does include the web portal access option, the web portal access fields are processed.

The following example shows imported identities that do not include web portal access.

Request identities

1

Identity Information

2

Import

3

Review

Import identities

Import your identities for this request below. If any data errors are encountered during the identities import, the identities in the CSV file that import the file again. (NOT FOR IMPORTING THE file again) (Importing the file again overwrites any data already imported into the grid)

Import from CSV

First name	Last name	Mobile name	Email	Mobile phone number	Preferred name	First name	Activation date	Expiration date	Company	Employee ID	Job title	Department	Job country	Terminal ID
John	Smith	J	johnsmith@corp.com	12345	John S. Smith	American Express	1/15/2023, 7:44 PM	3/31/2023, 7:44 PM	Corp Co.	123456	Manager	Sales	Canada	Terminal 11
John	Doe	J	john.doe@corp.com	57890123	John A.D.	American Express	1/15/2023, 7:44 PM	3/31/2023, 7:44 PM	Corp Co.		Admin eng.	Sales	United States of America (US)	

0/1000 identities

Cancel

Back

Next

The following example shows imported identities that include web portal access.

The following example shows imported identities that include web portal access:

Request identities

Step 1: Identity Information

Step 2: Import

Step 3: Review

Import identities

Import your identities for this request below. If any data errors are encountered during the identities import, the identities in the CSV file that import the file again. (NOT FOR IMPORTING THE file again) (Importing the file again overwrites any data already imported into the grid)

Import from CSV

First name	Last name	Mobile name	Email	Mobile phone number	Preferred name	First name	Activation date	Expiration date	Company	Employee ID	Job title	Department	Job country	Terminal ID
John	Smith	J	johnsmith@corp.com	12345	John S. Smith	American Express	1/15/2023, 7:44 PM	3/31/2023, 7:44 PM	Corp Co.	123456	Manager	Sales	Canada	Terminal 11
John	Doe	J	john.doe@corp.com	56789012	John A.D.	American Express	1/15/2023, 7:44 PM	3/31/2023, 7:44 PM	Corp Co.		Admin eng.	Sales	United States of America (US)	

0/1000 identities

Cancel

Back

Next

If any errors are encountered in the imported CSV file, they are highlighted in red. Any corrections must be applied in the CSV file and then imported again.

CAUTION:

Correcting any errors will overwrite identities data already imported into the grid.

- a. (Optional) If your identities list is long, consider using the Show errors only slider.
- b. Click Next.

10. In the Review section, review the information to ensure that everything is correct.

The screenshot shows the 'Request identities' dialog box with the 'Review' tab selected. The dialog has a progress bar at the top with three steps: 'Basic information' (completed), 'Import' (current step), and 'Review' (next step). The 'Review' section contains a list of fields with their corresponding values:

Field	Value
Request name	Renovation contractors (4th Floor)
Supervisors	John Doe
Identity request template	Electrical contractors
Reason for request	Electrical contractors for 4th floor renovations.
Identities	2 identities will be requested

At the bottom of the dialog, there are three buttons: 'Cancel', 'Back', and 'Finish'.

- a. If the details in the Review section are correct, click Finish.

11. If you chose Download a sample CSV file, do the following:

- a. Click Download a sample CSV file.

The screenshot shows the 'Import identities' dialog box. It has a title bar and a main area with the text 'To import identities, attach a CSV file below'. Below this text is a large rectangular area with the text 'Drag and drop a CSV file here or Browse'. Below this area is a button labeled 'Download a sample CSV file'. Below the button are two links: 'Download country codes to use with the CSV template' and 'Download time zones to use with the CSV template'. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Import file'.

- b. Select and open the downloaded CSV file.

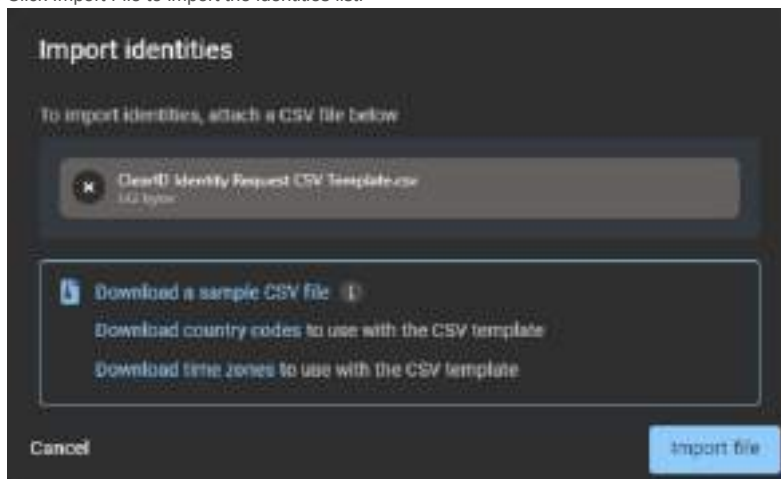
Tip: Download the *country codes* and *time zones* samples for reference if the *country codes* and *time zones* you require are not shown in the downloaded sample.

- c. For each identity, complete a row of identity information in the CSV template file.

first name	last name	middle name	email	mobile phone number	preferred time zone	activation date	expiration date	company	employee id	job title	department	job count	external id	enable id	web portal username	password
John	Smith	B.	john@smith.com	12345	John (B. Smith) America/12345	1/1/2021	12/31/2021	Smith Co.	1012345	Manager	Sales	CAN	00000011	TRUE	john@smith.com	12345678
Jane	Doe	A.	jane@smith.com	67890	Jane (A. Doe) America/12345	1/1/2021	12/31/2021	Smith Co.	1012346	Sales rep	Sales	USA	00000012	FALSE		

NOTE: The columns in the CSV template can vary depending on the settings in your site configuration.

- Save the identities list as a CSV file.
- Return to the Import identities dialog, to drag and drop or click Browse to select the file you created.
- Click Import File to import the identities list.



- Review the imported identities data and check for any errors.

First name	Last name	Middle name	Email	Mobile phone number	Preferred time zone	Activation date	Expiration date	Company	Employee ID	Job title	Department	Job count	External ID	Internal ID
John	Smith	B.	john@smith.com	12345	America/12345	1/1/2021 7:44 PM	12/31/2021 7:44 PM	Smith Co.	1012345	Manager	Sales	Canada	00000011	
Jane	Doe	A.	jane@smith.com	67890	America/12345	1/1/2021 7:44 PM	12/31/2021 7:44 PM	Smith Co.	1012346	Sales rep	Sales	United States of America (EST)		

If any errors are encountered in the imported CSV file, they are highlighted in red. Any corrections must be applied in the CSV file and then imported again.

CAUTION:

Correcting any errors will overwrite identities data already imported into the grid.

- (Optional) If your identities list is long, consider using the Show errors only slider.
- Click Next.

- In the Review section, review the information to ensure that everything is correct.

Request identities

Basic information Import Review

Review
Ensure that all information is correct before completing the request.

Request name	Renovation contractors (4th Floor)
Supervisors	John Doe
Identity request template	Electrical contractors
Reason for request	Electrical contractors for 4th floor renovations.
Identities	2 identities will be requested.

Cancel Back Finish

a. If the details in the Review section are correct, click Finish.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Depending on the identity template that you selected, your identity requests are either approved automatically or approvers review identity requests and approve (or reject) as required.

Parent topic: [Requesting identities in ClearID](#)

Browse

- [Identity Request Feature Note \(2 pages\)](#)

5.36 | Canceling identity requests in ClearID

To cancel identity requests, the identity requester must review the pending requests and then decide which requests to cancel.

Before you begin

Ensure that some identity requests have already been submitted.

What you should know

Only identity requesters can cancel identity requests.

- Only pending requests can be canceled.
- Completed requests cannot be canceled.

NOTE: If one of the requested identities is canceled, all the configured approvers are added to the .cc list in the email notification for identity request approval and completion titled: "Identity request for *identity* has been updated".

Procedure

To cancel an identity request:

1. Click Dashboard > My requests.
2. From the Status list, filter the requests that are displayed:

Status

Select a status from the following:

All

Displays all pending or completed tasks.

Pending

Displays tasks waiting for approval.

Completed

Displays completed tasks and their status. For example, approved, completed, denied, or canceled.

3. In the My requests list, click an identity request to display additional details about the request.

Identity request for Jim Brown

Identity requested by: Fred Smith on December 16, 2021 9:52 AM
fsmith@test.com

Waiting for approval from 1 approver

Identity template: Electrical contractors

General information

First name	Middle name	Last name
Jim		Brown
Preferred name	Email	Phone number
Jim Brown		
External ID		

Work details

Company	Employee ID	
Job title	Department	Country
		Canada

Access control

Activation date	Expiration date	Time zone
December 16, 2021	March 31, 2022	America/Toronto

Supervisors

Name	Email
Fred Smith	fsmith@test.com

Web portal access

Grant user access to the web portal: N/A

History

- Dec 16 Genetec ClearID™ service edited the request.
- Fred Smith created the request.

Close Cancel request

NOTE: The buttons that are available in the identity request details vary depending on whether you are the requester, supervisor, or an approver.

4. Review the identity request details for accuracy and completeness.
5. If the identity request is no longer required click Cancel request.
 - a. Enter the reason for cancellation and click Confirm.

To cancel multiple identities requested using a CSV import:

1. Click Dashboard > My requests.
2. From the Status list, filter the requests that are displayed:

Status

Select a status from the following:

All

Displays all pending or completed tasks.

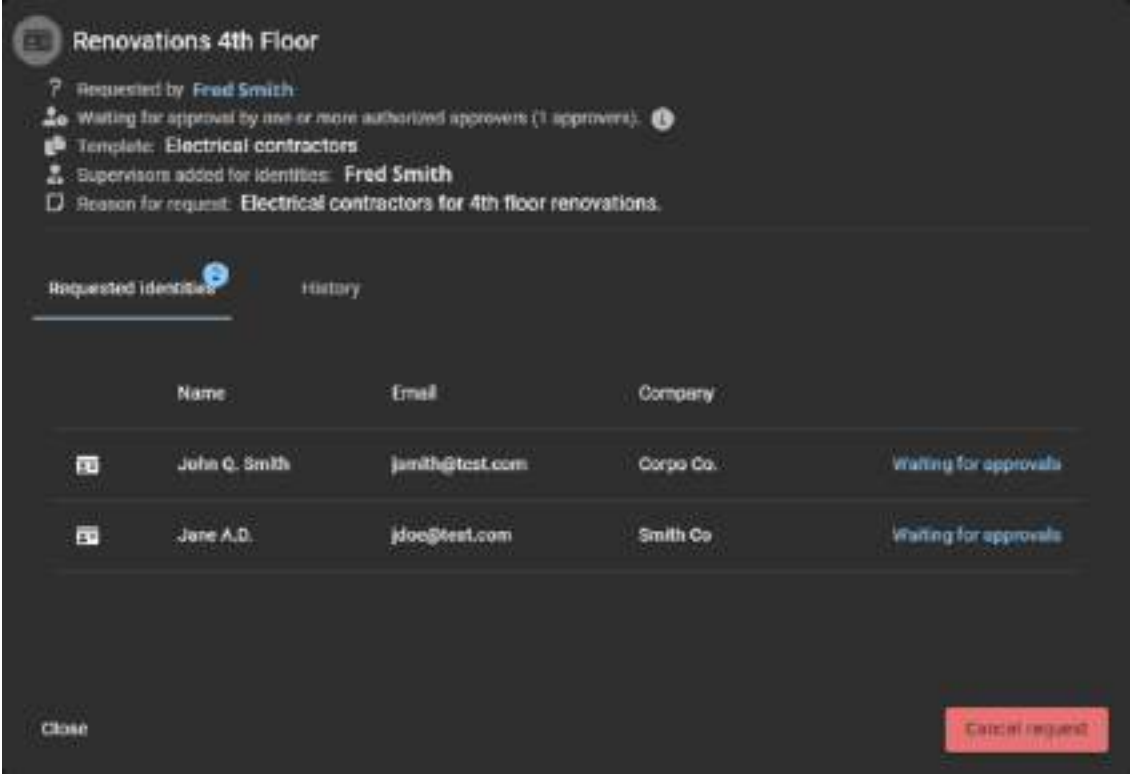
Pending

Displays tasks waiting for approval.

Completed

Displays completed tasks and their status. For example, approved, completed, denied, or canceled.

3. In the My requests list, click an identities request awaiting approval to display additional details about the request.



NOTE: The buttons that are available in the identities request details vary depending on whether you are the requester, supervisor, or an approver.

4. Review the identity request details for accuracy and completeness.
5. If the identity request is no longer required click Cancel request.
- a. Enter the reason for cancellation and click Confirm.

Results

The identity request is now canceled.

5.37 | Approving identity requests in ClearID

To approve identity requests, a supervisor or identity approver must review the pending approvals and then decide which requests to approve.

Before you begin

Ensure that some identity requests have already been submitted.

What you should know

Only supervisors or identity approvers can approve identity requests.

Procedure

To approve an identity request:

1. Click Dashboard > My tasks.
2. From the Status list, filter the tasks that are displayed:

Genetec ClearID®; User Guide

Displayed in the header

Status

Select a status from the following:

All

Displays all pending or completed tasks.

Pending

Displays tasks waiting for approval.

Completed

Displays completed tasks and their status. For example, approved, completed, denied, or canceled.

3. In the My tasks list, click an identity request to display additional details about the request.

Identity request for Jim Brown

Identity requested by: Fred Smith on December 14, 2021 9:52 AM
Email: fsmith@test.com

Waiting for approval from 1 approver

Identity template: Electrical contractors

General information			Work details		
First name: Jim	Middle name:	Last name: Brown	Company:	Employee ID:	
Preferred name: Jim Brown	Email:	Phone number:	Job title:	Department:	Country: Canada
External ID:					

Access control			Supervisor	
Activation date: December 14, 2021	Expiration date: March 31, 2022	Time zone: America/Toronto	Name: Fred Smith	Email: fsmich@test.com

Web portal access: Grant user access to the web portal: Yes/No

History:

- Dec 14 Genetec ClearID™ service edited the request.
- Fred Smith created the request.

Buttons: Edit, Deny, Approve

NOTE: The buttons that are available in the identity request details vary depending on whether you are the requester, supervisor, or an approver.

4. Review the identity request details for accuracy and completeness.
5. (Optional) If you need to modify the identity request, click Edit and make any changes that are required.
 - a. Click Save.
6. If the request is not valid or contains incorrect information, click Deny.
 - a. Enter the reason for denial and click Confirm.
7. If the request is valid and correct, click Approve.
8. In the Reason for approval field, enter the reason for approval and click Confirm.

Identity request for Jim Brown

Requested by: **Jim Brown** | Status: **Open** | Request ID: **123456789** | Job title: **Electrical Contractor** | Department: **Facilities** | Country: **Canada**

Access control

Activation date: **December 14, 2021** | Expiration date: **March 31, 2022** | Time zone: **America/Toronto**

Supervisors

Name	Email
Fred Smith	fsmith@test.com

Web portal access

Grant user access to the web portal: **Yes** (N/A)

Reason for identity request

Access required for electrical contractor work.

History

- Dec 14** Genetec ClearID® service edited the request.
- Dec 14** Fred Smith created the request.

Reason for approval

Reason: **Access granted for new electrical contractor**

48 / 300

Custom

To approve identities imported using a CSV import:

1. Click Dashboard > My tasks.
2. In the My tasks list, click an identities request to display additional details about the request.

Renovation contractors (4th Floor)

Requested by: **Fred Smith**

Waiting for approval by one or more authorized approvers (1 approver).

Template: **Electrical contractors**

Supervisors added for identities: **Fred Smith**

Reason for request: **Electrical contractors for 4th floor renovations**

Requested identities | History

Show errors only (0)

Name	Email	Company	Deny all	Approve all
John Q. Grey	jgrey@test.com	Corpo Co.	X	✓
Jane A.D.	jasmith@test.com	Smith Co	X	✓

Close | **Cancel request** | **Save**

NOTE: The buttons that are available in the identity request details vary depending on whether you are the requester, supervisor, or an approver.

3. Review the identities request details for accuracy and completeness.
 - a. If all the identities in the request are correct, click Approve all then click Save.
 - b. If all the identities in the request are not correct, click Deny all then click Save.
4. (Optional) If you need to modify an identity, click View identity request details (🔍) on the row for the identity to review the details of that request.
 - a. Click Edit to make any changes that you require.

- b. Click Save.
5. If the request is not valid or contains incorrect information, click Deny () on the row for the identity.
 - a. Enter the reason for denial and click Confirm.
6. If the request is valid and correct, click Approve () on the row for the identity.
 - a. Click Save.
 - b. In the Reason for approval field, enter the reason for approval and click Confirm.

Results

The identity request is now approved. The identity is now created and if applicable inherit the role access to associated areas during the periods specified in their identity request.

NOTE: (Optional) Additional communications might also be provided by your organization regarding where and how to retrieve a badge access card (if required) for the new identity.

Example



After you finish

Browse

- [Identity Request Feature Note \(2 pages\)](#)

5.37.1 | Modifying an identity request in ClearID

To modify identity requests, a supervisor or identity approver must review the pending approvals and then decide which requests to modify.

Before you begin

Ensure that some identity requests have already been submitted.

What you should know

Only supervisors or identity approvers can modify identity requests.

Procedure

To modify an identity request:

1. Click Dashboard > My tasks.
2. From the Status list, filter the tasks that are displayed:

Status

Select a status from the following:

All

Displays all pending or completed tasks.

Pending

Displays tasks waiting for approval.

Completed

Displays completed tasks and their status. For example, approved, completed, denied, or canceled.

3. In the My tasks list, click an identity request awaiting approval to display additional details about the request.

Identity request for Jim Brown

? Identity requested by: Fred Smith on: December 16, 2021 9:52 AM
✉ fsmith@test.com

👤 Waiting for approval from 1 approver: ⓘ

Identity template: Electrical contractors

General information

First name: Jim	Middle name:	Last name: Brown
Preferred name: Jim Brown	Email:	Phone number:
External ID:		

Work details

Company:	Employee ID:
Job title:	Department:
	Country: Canada

Access control

Activation date: December 16, 2021	Expiration date: March 31, 2022	Time zone: America/Toronto

Web portal access

Guest user access to the web portal: ⓘ [View](#)

Supervisors

Name	Email
Fred Smith	fsmith@test.com

History

👤 Dec 16	Genetec ClearID™ service edited the request.
👤	Fred Smith created the request.

Close

[Edit](#) [Deny](#) [Approve](#)

4. Review the identity request details for accuracy and completeness.
5. To modify the identity request, click Edit and make any changes that are required.
 - a. Click Save.

To modify multiple identities requested using a CSV import:

1. Click Dashboard > My tasks.
2. From the Status list, filter the tasks that are displayed:

Status

Select a status from the following:

All

Displays all pending or completed tasks.

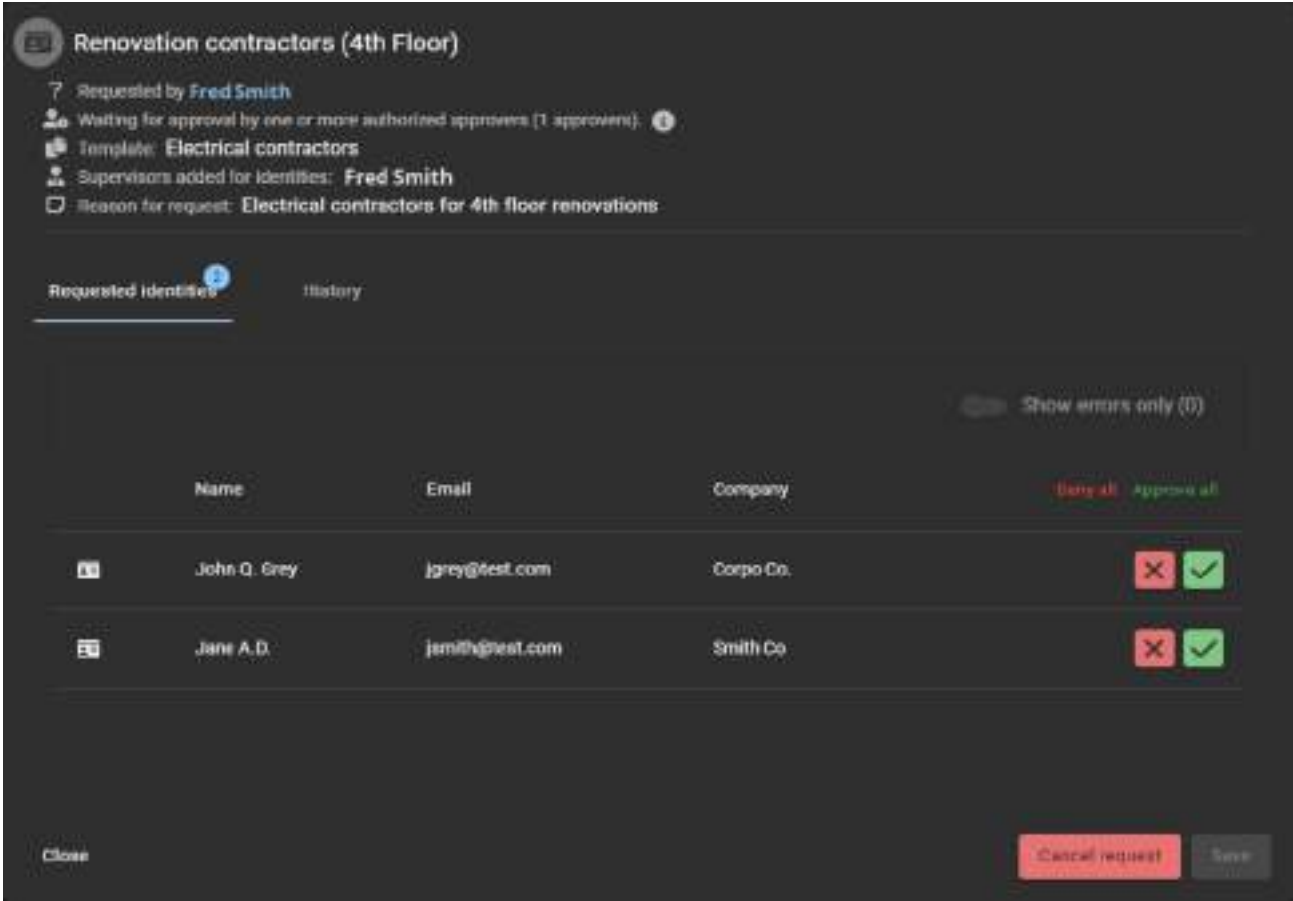
Pending

Displays tasks waiting for approval.

Completed

Displays completed tasks and their status. For example, approved, completed, denied, or canceled.

3. In the My tasks list, click an identities request awaiting approval to display additional details about the request.



4. (Optional) If you need to modify an identity, click View identity request details () on the row for the identity to review the details of that request.
- a. Review the identity request details for accuracy and completeness.
 - b. Click Edit to make any changes that you require.
 - c. Click Save.

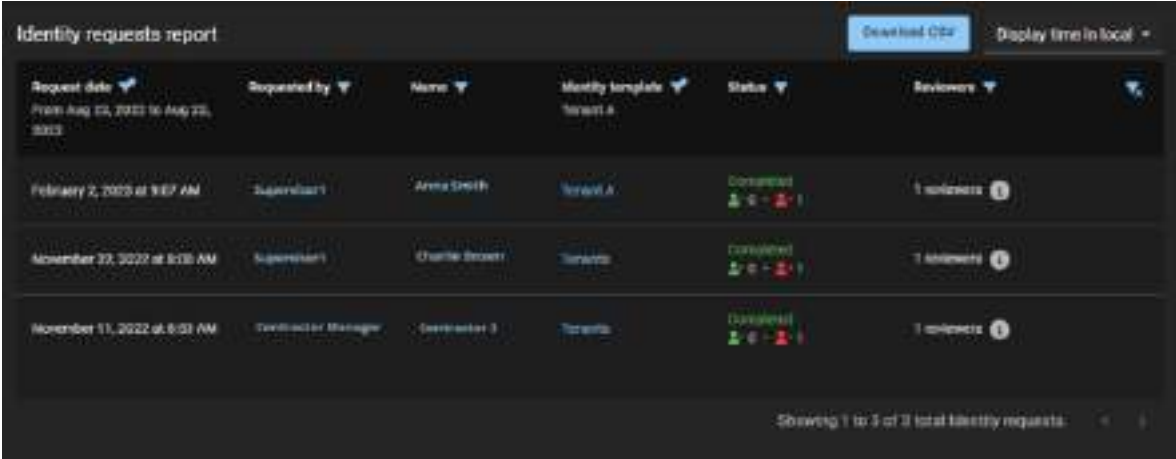
After you finish

Approve your identity requests.
Parent topic: Approving identity requests in ClearID

5.38 | About identity requests report in ClearID

In Genetec ClearID™, an identity requests report is a list of identity requests for your ClearID account. The report includes information about the identity request date, requester, name, identity template, status, and reviewers.

Identity requests report



The identity requests report is used by administrators to check the status of all identity requests at the account level. The report can also be used to provide identity requests information to auditors.

Filters can be used to help refine the search results by identity request date, requested by, name, identity template, status, and reviewers.

Browse

- [Checking the status of identity requests in ClearID](#)

5.39 | Checking the status of identity requests in ClearID

As an *Account administrator* you can check the status of identity requests to ensure that the organization is security-compliant, audit ready, and that the requests are processed in a timely fashion.

Before you begin

You must be an *Account administrator* to view the Identity requests report and check the status or progress of identity requests.

Procedure

1. From the homepage, click Reports > Identity requests.

Request date	Requested by	Name	Identity template	Status	Reviewers
February 2, 2022 at 9:07 AM	Supervisor1	Anna Smith	New Hire A	Completed	1 reviewers
November 22, 2022 at 1:05 AM	Supervisor1	Charlie Brown	Transfer	Completed	1 reviewers
November 11, 2022 at 6:03 AM	Contractor Manager	Contractor 3	Transfer	In Progress	1 reviewers

2. In the Identity requests report page, select the required display time format.

Display time in local

Report times are displayed using the system time from the computer of the logged-in user.

Display time in UTC

Report times are displayed using Coordinated Universal Time (UTC).

3. Filter the report based on your required criteria:

Request date

In the Request date column, click  to filter the results by date.

If you selected Date range, use the calendar picker to select the date range that you require.

NOTE: The Request date time period is limited to a maximum of 1 year.

Requested by

In the Requested by column, click  to filter the results by identity requester.

- Enter a user name or email address in the search field.
- (Optional) Click the Requested by hyperlink to display summary details about the requester.

Name

In the Name column, click  to enter a search string and filter the results by Any words or All words.

(Optional)

Click the Name hyperlink to display the identity request.

NOTE: If you're an approver, you can Approve or Deny the pending identity request while viewing the request.

Identity template

In the Identity template column, click  to filter the results by identity template type.

Status

In the Status column, click  to filter the results by status.

- Select one or more check boxes to filter the results by the statuses that you require (Submitted, Waiting for approvals, Denied, Approved, Canceled, or Completed).

Reviewers

In the Reviewers column, click  to filter the results by identity, role, or both.

(Optional)

Click  to reset filter selections.

4. Click Download CSV, to download a copy of the identity requests report in CSV format. The report can then be used for auditing purposes, to keep a physical copy, to attach to an audit request, to review offline, or to manipulate or consolidate data in a spreadsheet for other audiences.

- a. Follow your browser prompts to complete downloading the exported file.

The file is exported as a .CSV file to the default download location for your browser. By default the exported file is created using the name of your site. For example, *IdentityRequestReport_fromdate_to_todate_SiteActivityReport.csv* (IdentityRequestReport_2024-09-24.csv).

NOTE: The columns and entries in the CSV file can vary depending on the filters you've selected when you download the report.

After you finish

Approve or reject identity requests as required:

- [Approving identity requests in ClearID](#)

Browse

- [About identity requests report in ClearID](#)
- [Requesting identities in ClearID](#)

6 | Credential synchronization

6.1 | Configuring credential replication in ClearID

To replicate supported credentials across multiple Synergis™ systems, you must configure your credentials replication settings in the Genetec ClearID™ portal.

Before you begin

- [Learn about cardholder and identity relationships.](#)
- [Make sure that ClearID is managing your cardholder and credential changes.](#)

What you should know

Only an account administrator can configure credentials replication.

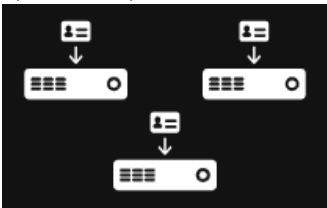
Credentials replication is intended to replicate *credentials* across two or more Synergis systems. For the replication functions to work, you must be using all the identity management functions provided by ClearID. Any credential changes that are only performed on a secondary system aren't replicated to the other systems.

NOTE: Credentials won't be sent to systems where cardholder and credential management is in read-only mode. In this situation, the access control system is highlighted in the ACS list with the Cardholder and credential management is disabled  icon.

Procedure

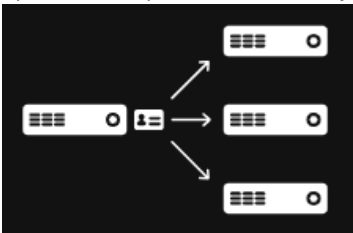
1. From the homepage, click Administration > Credentials.
2. In the Credential replication mode section, from the Mode list select a replication mode.

- a. Option 1: No replication between access control systems.



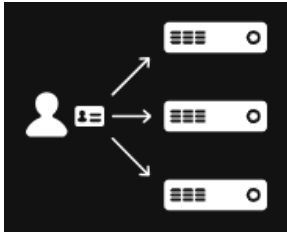
Each access control system operates independently, without synchronizing credentials with other systems. The credentials created in one system remain unique to that system, and aren't automatically synchronized or used in other systems.

- b. Option 2: Use a specific access control system as the source of credentials synchronization.



Credential modifications performed in the selected access control system are synchronized to all other systems where the identity is associated with a cardholder.

- c. Option 3: Use the system associated with the primary site of the identity as the source of credentials synchronization.



Credential modifications performed in the system associated with the primary site of the identity are replicated to all other systems where the identity is associated with a cardholder.

NOTE: If you selected No replication between access control systems, you can skip the following step.

3. In the Credential types and formats section, select the credential types that you want to synchronize.

NOTE: The credential options that are available for selection here varies depending on the credential information that is pulled in from your connected systems. Custom credentials are not supported.

- a. (Optional) If your organization has multiple formats, there might be situations where you only want to synchronize specific formats.

4. Click Save.

After you finish

(Optional) Do one or more of the following:

- Review the credential synchronization logs.
- Force a credentials synchronization.

6.2 | Viewing credential synchronization logs in ClearID

To check credential synchronization status or to review detailed information about the audit trail activities for all events related to credentials, view the credential synchronization logs in Genetec ClearID™.

Before you begin

Configure your credentials synchronization settings.

What you should know

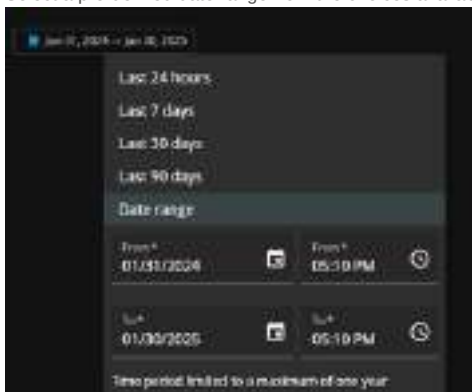
Only an account administrator can view the credential synchronization logs.

Procedure

1. From the homepage, click Administration > Credentials.
2. In the Credential replication logs section, click View logs.
3. (Optional) Use filters to help refine the log results based on one or more of the following criteria:

Date range

Select a pre-defined date range from the choices available or enter a specific date range using the date range picker.



Search field

In the search field, enter a search criteria.

Filter controls

Access control system

Search for an ACS system using its name or select one or more ACS systems from the list.

Associated identity

Search for an associated identity. For example, first name, last name, email, or a partial search string.

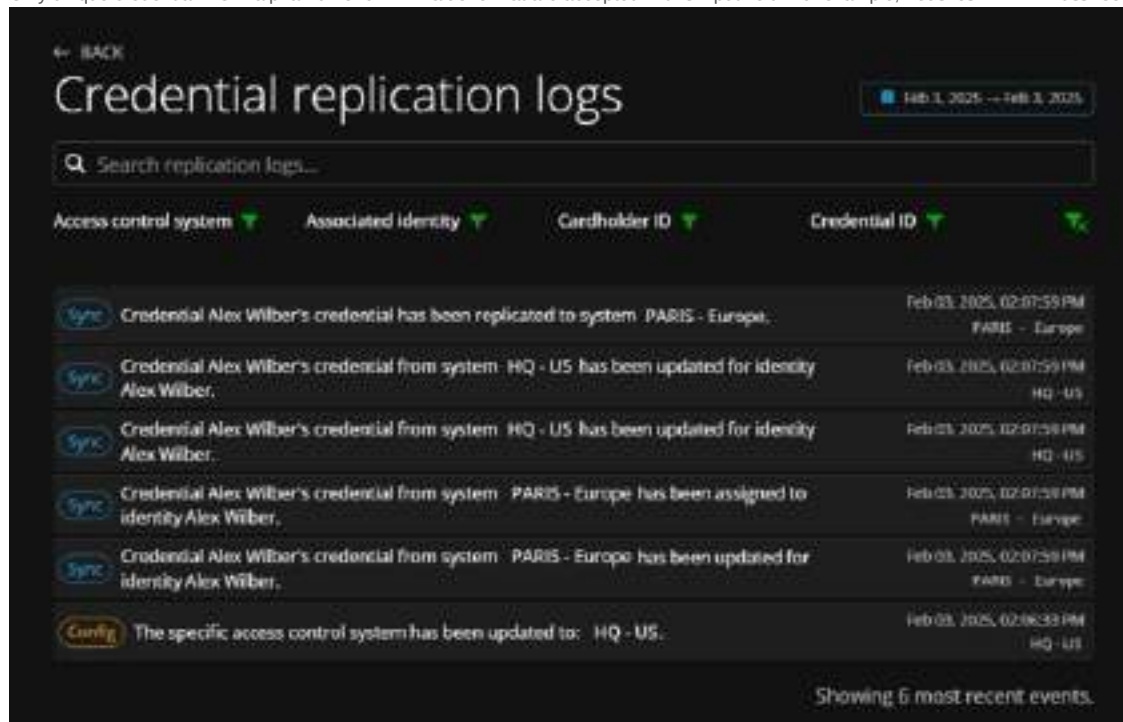
Cardholder ID

Only unique cardholder IDs in alpha-numeric HEX value format are accepted in this input field. For example, 29abdafb-f124-401a-b143-3c88556ec3c1.

NOTE: This filter is useful for users who primarily work with the information from Security Center.

Credential ID

Only unique credential IDs in alpha-numeric HEX value format are accepted in this input field. For example, fc6e4851-f429-40e5-bbe7-ba363c5cad1a.



After you finish

(Optional) Force a credentials synchronization.

6.3 | Forcing credential synchronization in ClearID

To resolve credential issues, you can force a synchronization to replace all credentials in Genetec ClearID. This force synchronization uses the latest values from your selected credential source and triggers the synchronization immediately.

Before you begin

- Configure your credential synchronization settings.
- (Optional) View the credential synchronization logs.

What you should know

Only an account administrator can force a credentials synchronization.

After credential synchronization settings have been configured, the synchronization is automatic.

- A forced synchronization can be used during initial setup as a preemptive measure to ensure that all credentials are propagated correctly.
- A forced synchronization is also used when the synchronization mode is updated from a specific system to the primary site option. Forcing the synchronization after a mode change ensures that the correct credentials are synchronized immediately to align with the selected mode.

Synchronization throughput is estimated at approximately 10 credentials a second. However, this throughput can vary depending on the machine running the Genetec ClearID™ plugin and the number of credentials assigned to identities.

If credential issues are encountered at a site contact the account administrator to view the logs, perform troubleshooting, and potentially force a synchronization.

NOTE: If you selected No replication between access control systems during your credentials synchronization configuration, the force synchronization function isn't available.

Procedure

1. From the homepage, click Administration > Credentials.
2. In the Force credential synchronization section, click Synchronize.
3. In the Synchronize dialog, click Synchronize.

The request to synchronize credentials is initiated and a Request to synchronize other systems sent successfully message is displayed.
IMPORTANT: No further progress is reported in the Credentials tab.

After you finish

Review the Credential replication logs to confirm that credentials information has been updated with the latest information.

7 | Managing sites

7.1 | About sites in ClearID

In Genetec ClearID™, a site is a logical entity. Sites include one or more areas. Each site and area can have a different owner.

A site typically represents either a building or a campus:

- If you have multiple buildings managed by one security team or one set of policies for visitors, consider setting them up using one site.
- Each site can have its own set of policies and site owners.
- If you have different buildings spread throughout a city, consider implementing one site per building.
- Multiple sites can be associated with the same Security Center access control system.

IMPORTANT: Your implementation choices can affect the Genetec ClearID™ solution costs. These costs can vary depending on the implemented functions, the number of identities, and the number of sites.

7.2 | Creating sites in ClearID

Before you can configure your areas in Genetec ClearID™, you must create the sites that you want to associate your areas with.

Before you begin

- [Add your systems.](#)

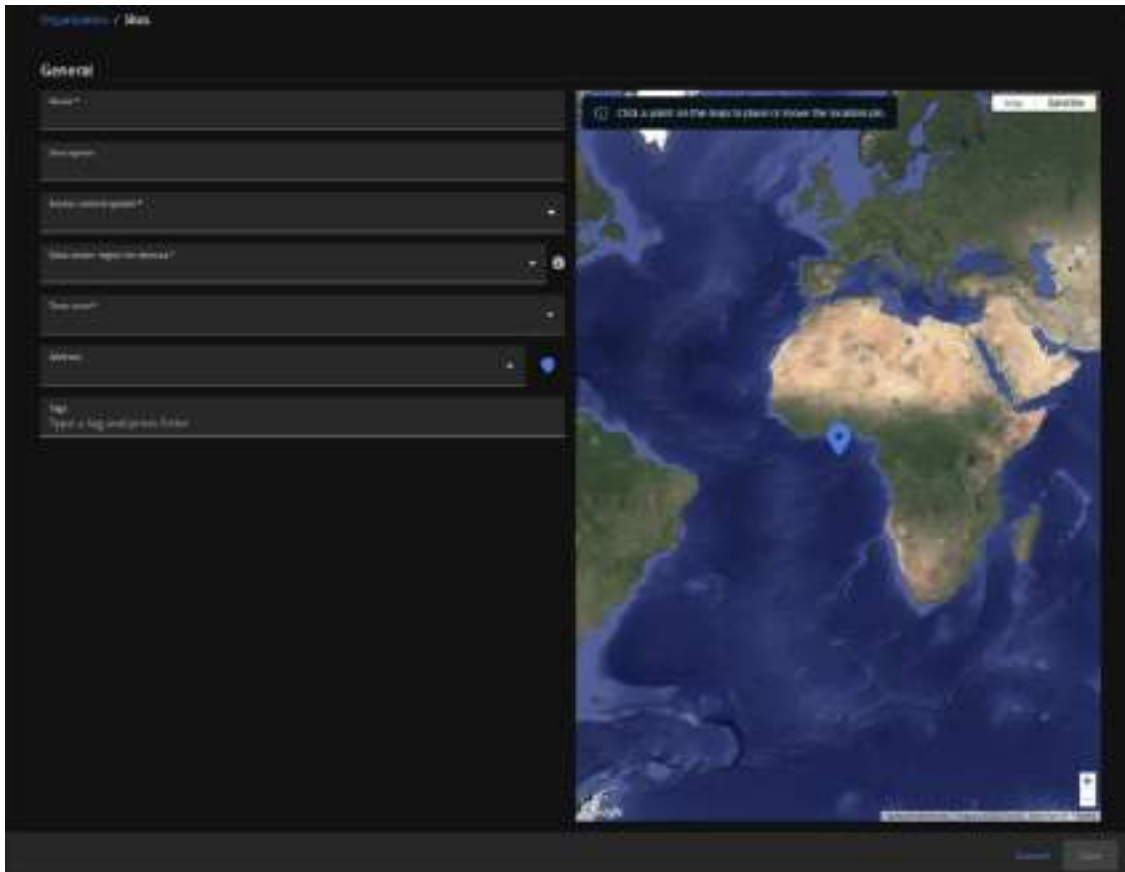
What you should know

To create sites in ClearID, you must be an *Account administrator*.

- An *Account administrator* can choose the *Site owners* and configure visitor management for the site.
- A *site* is associated with a Security Center access control system.
- Multiple sites can be associated with the same Security Center access control system.

Procedure

1. Click Organization > Sites.
2. Click Add site.



3. On the General page, complete the fields.

NOTE: Mandatory fields are highlighted in the user interface with an asterisk (*).

Name

Enter a name for your site.

Description

Enter a description that indicates the geographical location of the building or physical location of the site.

Access control system

Select the system that you require from the Access control system list.

NOTE: This access control system is used to synchronize changes in ClearID back to Security Center.

Data center region for devices

Select a data center region from the drop-down. This option is typically set to the data center region closest to where the device will be used. The data center region is used for device communications.

NOTE: This setting is permanent and can't be changed after the site is created. The data center option isn't available if your account is deployed in the Europe only architecture.

Time zone

Select a time zone from the drop-down. The time zone options are represented using the Internet Assigned Numbers Authority (IANA) format.

NOTE: When an access request or visitor request is made from anywhere in the world, the time zone of the requested site access or visit is used to ensure that the correct date and times are applied to the request.

Address

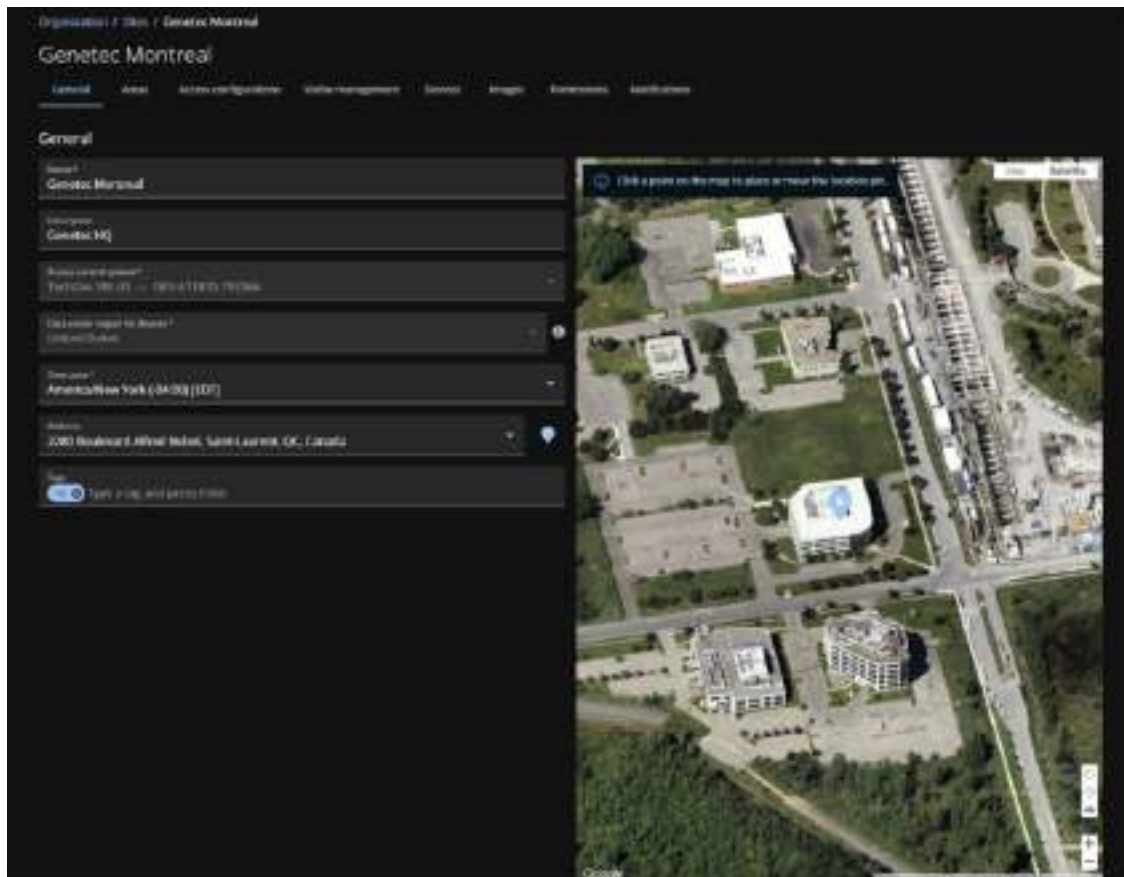
Enter an address for the site. As you type, Google Maps integration auto-complete processes the information and displays available addresses.

Center map

Click  to find the address on the map, and center the map on that address.

Tags

Enter alternative keywords or search term categorizations that might be used to find the site.



4. On the Notifications page, complete the fields.

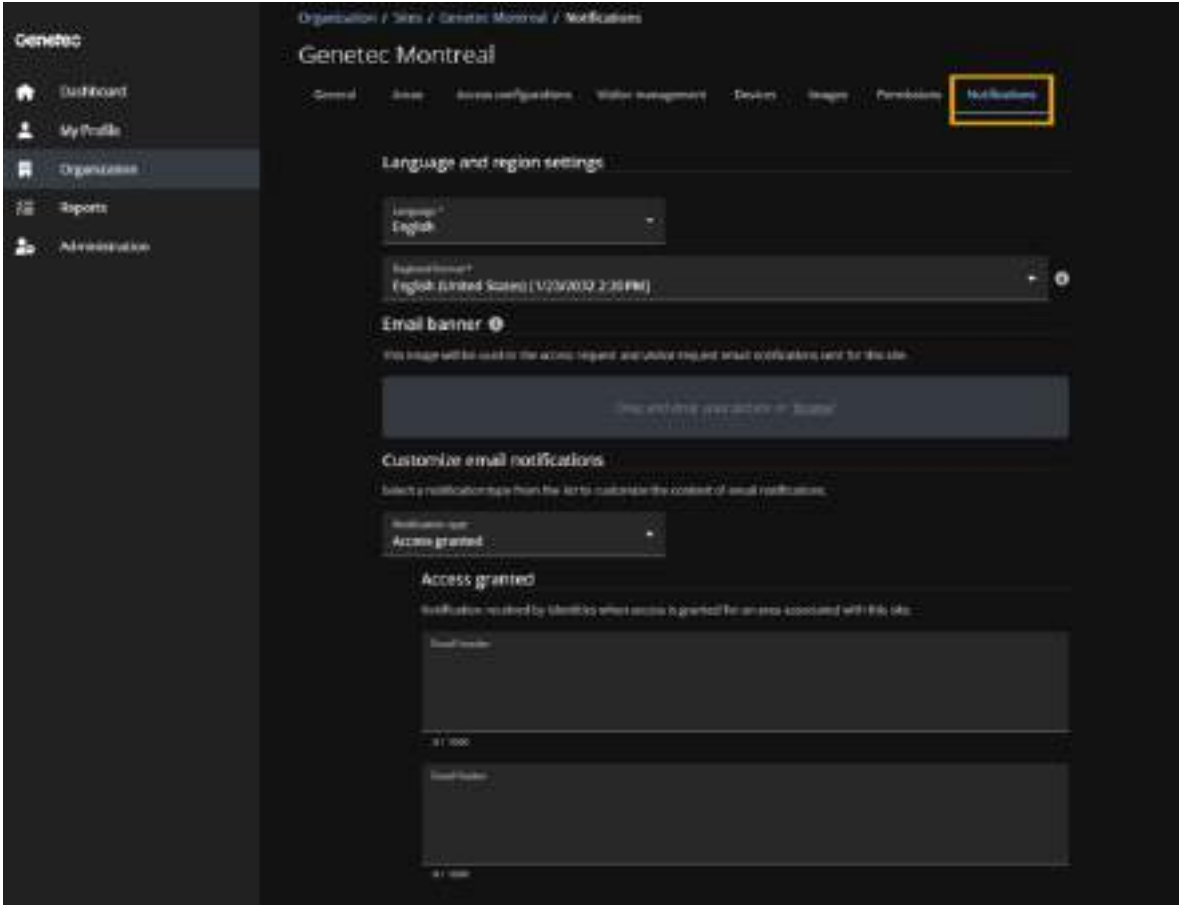
Language

Select a notification language from the drop-down. This setting is used for email notifications and SMS alerts. The notifications language selection is unique to a site and you can choose from English, French, Spanish, Portuguese, Italian, German, Dutch, and Japanese.

Regional format

Select a regional date and time format to use in email notifications for this site. The default regional format is American English (en-us). For example, 1/23/2032 2:20 PM.

5. Click Save.



Results

Your site has been created in ClearID.

Organization / Sites

Sites

Areas

Identities

Roles

Watchlists

Identity templates

Access reviews

Sites

Add site

Search sites...

Name	Address	Description	Access control system
Head	2250 Boulevard Alfred Nobel, Saint-L...		TechDoc VM US
Head	2250 Boulevard Alfred Nobel, Saint-L...	This is our Head	TechDoc VM Europe
Genetec Albert Einstein	Rue Albert Einstein, Saint-Laurent, QC...	Genetec Building 1	TechDoc VM US
Genetec Alfred Nobel	2250 Alfred Nobel		TechDoc VM Europe
Genetec B&B	2250 Alfred Nobel	Genetec	TechDoc VM Europe
Genetec Head Office	2250 Boulevard Alfred Nobel, Saint-L...	Head Office	TechDoc VM US
Genetec Head Office	2250 Boulevard Alfred Nobel, Saint-L...		TechDoc VM Europe
Genetec Montreal	2250 Boulevard Alfred Nobel, Saint-L...	Genetec HQ	TechDoc VM US

Showing 1 to 8 of 8 total sites.

After you finish

Add your site owners.
Browse

- [Modifying sites in ClearID](#)

Browse

- [IANA Time Zone Database](#)

7.2.1 | Adding site owners in ClearID

In Genetec ClearID™, a site owner is an identity that has authority over areas associated with a specific site. Before you can assign or modify area owners, configure specific area settings that are exclusive to site owners, or manage site access reviews you must add your site owners.

Before you begin

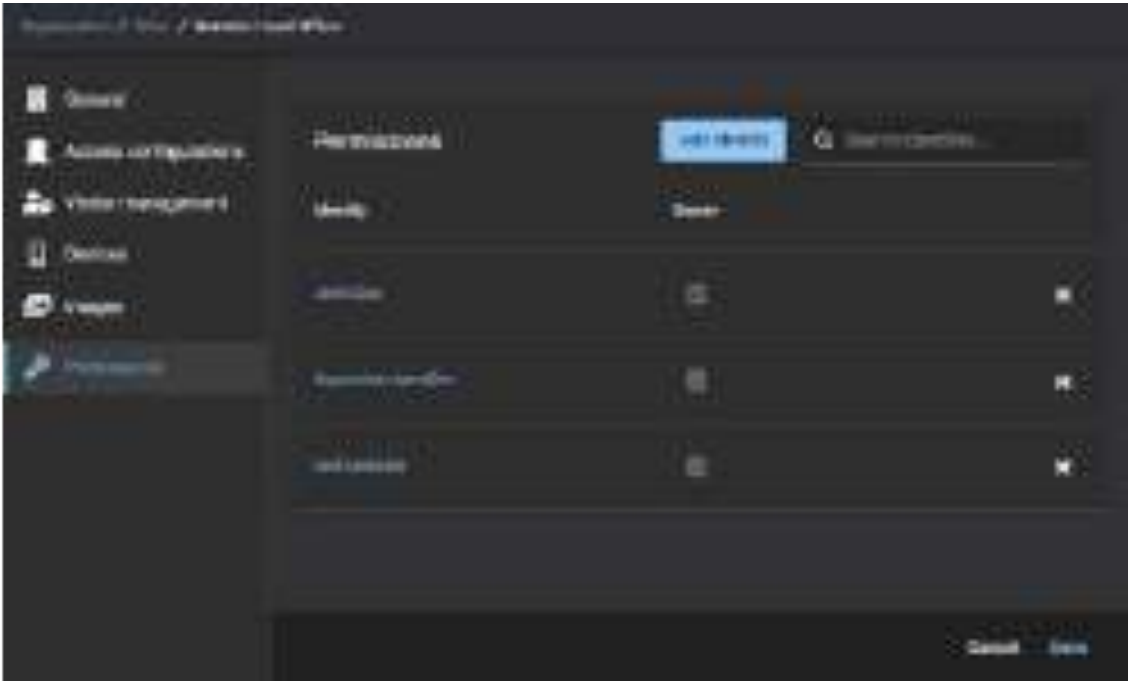
Create your sites.

What you should know

To add site owners in ClearID, you must be an account administrator.

Procedure

1. Click Organization > Sites.
2. Select your site and click Permissions.
3. Click Add identity to add site owners to the site Permissions list.



- a. Search for or select the identities that you require and click Add.
Tip: Click the identity hyperlink in the Identity column to review identity details (company, department, home site, supervisor, and email) and to verify that you have the correct identities in the list.
 - b. (Optional) Click  to remove any site owner permissions that are no longer required.
4. Click Save.

After you finish

Create your areas
Parent topic: [Creating sites in ClearID](#)

7.2.2 | Enabling visitor management for sites in ClearID

Before users can invite visitors, you must configure the visitor management settings for your site.

Before you begin

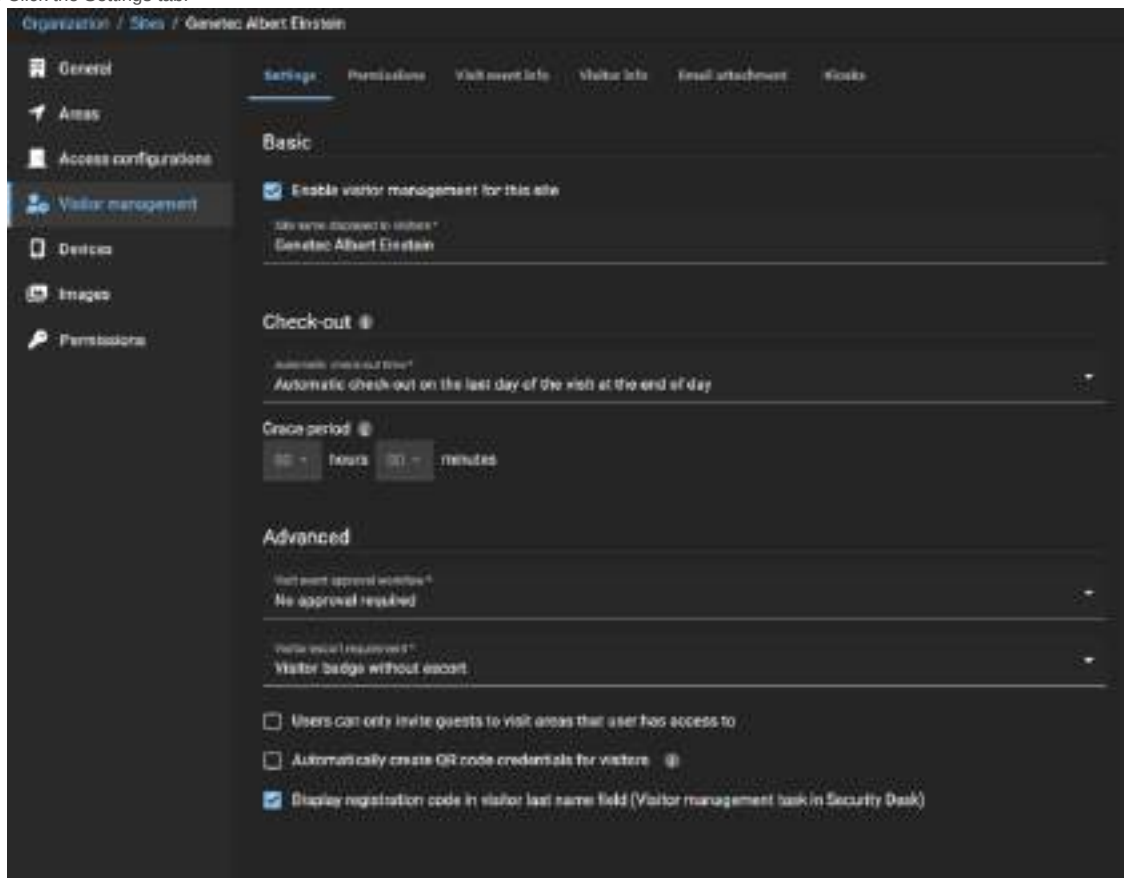
Create your sites.

What you should know

- Visitor management is disabled by default.
- Only account administrators or *site owners* can enable or configure visitor management for sites in Genetec ClearID™.
- The options displayed when a visit request is created vary depending on the users requesting access and also the settings that you configure here.
- Only account administrators can grant user permissions to invite visitors using roles.
- Users are automatically granted *Invite visitors* permissions for their home site by default.

Procedure

1. Click Organization > Sites.
2. Search for and select a site.
3. Click Visitor management to configure the visitor management options for a site.
4. Click the Settings tab.



- a. In the Basic section, configure the options you require:

Enable visitor management for this site

Select this checkbox to enable visitor management for this site.

Site name displayed to visitors

Enter the site name that you want displayed externally to visitors.

- b. In the Check-out section, configure the options you require:

Automatic check-out time

Automatic check-out on the last day of the visit at the end of the day

The visitor is checked out automatically on the last day of the visit at midnight.

Automatic check-out at the scheduled visit end time

The visitor is checked out at the specified visit end time.

NOTE: Visitor's temporary access rights and QR code credential are deactivated during automatic check-out. If a grace period is activated, visitors are checked out after the additional grace period lapses after the visit end time.

Grace period

Adds extra time to the scheduled end time of the visit event. After the grace period lapses, the visitor is checked out.

- c. (Optional) In the Advanced section, configure the options you require:

Visit event approval workflow

Select the approval workflow that you require:

No approval required

No approval is required to complete visit event approval. For example, to simplify employees inviting visitors at any time.

Supervisor approval required

Supervisor approval is required to complete visit event approval.

Visit event approver approval required

Visit event approver approval is required to complete visit event approval.

NOTE: If an area is selected during the visit event creation, it can trigger its own approval workflow.

Visit escort requirement

Select the badge type that you require:

Visitor badge without escort

Typically used for visitors who do not require an escort and who do not need door access to secure or sensitive areas.

Visitor badge with escort

Typically used for visitors who do require an escort or who need door access to secure or sensitive areas.

NOTE: The visitor escort rule must also be turned on for the areas in Synergis™ to enforce the visitor escort rule. For the escort function to work properly, the Cardholder groups can escort visitors option must also be enabled in the General settings of the Access control task in Config Tool.

Users can only invite guests to visit areas that they have access to

- If the checkbox is selected, users can only invite guests to visit areas that the requesting user has access to. This setting is enforced when a guest visit request is created.
- If the checkbox is cleared, users can invite guests to visit any area in ClearID that allows visitors.

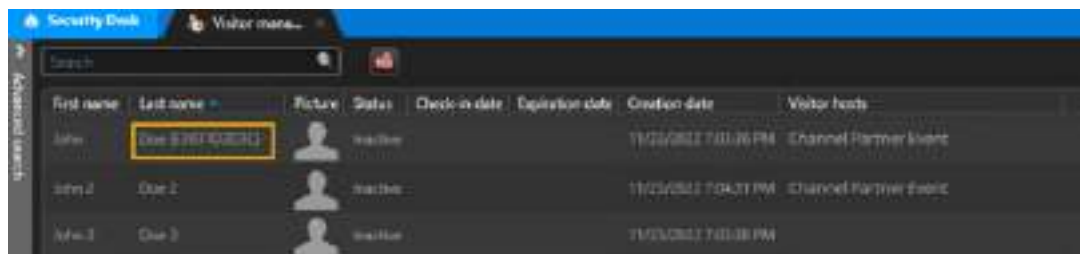
Automatically create QR code credentials for visitors

If the checkbox is selected, ClearID automatically creates a QR code credential for visitors when a visit request is created. Visitors can then use the QR code contained in the visitor confirmation email to access specific parking entrances, turnstiles, or gated facilities. The QR code can also be used during check-in with security, at a reception, or at a Genetec ClearID™ Self-Service Kiosk.

Display registration code in visitor last name field (Visitor management task in Security Desk)

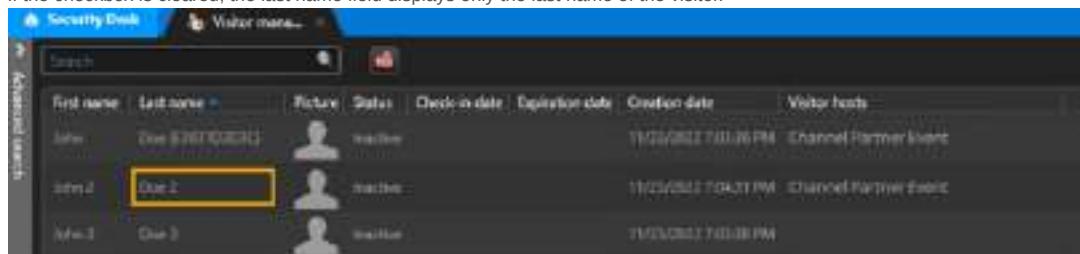
- If the checkbox is selected, the last name field displays the last name of the visitor and the QR code value. This checkbox is selected by default.

The checkbox must be selected for a QR code scanner to successfully scan and locate a pre-registered visitor in Security Desk.



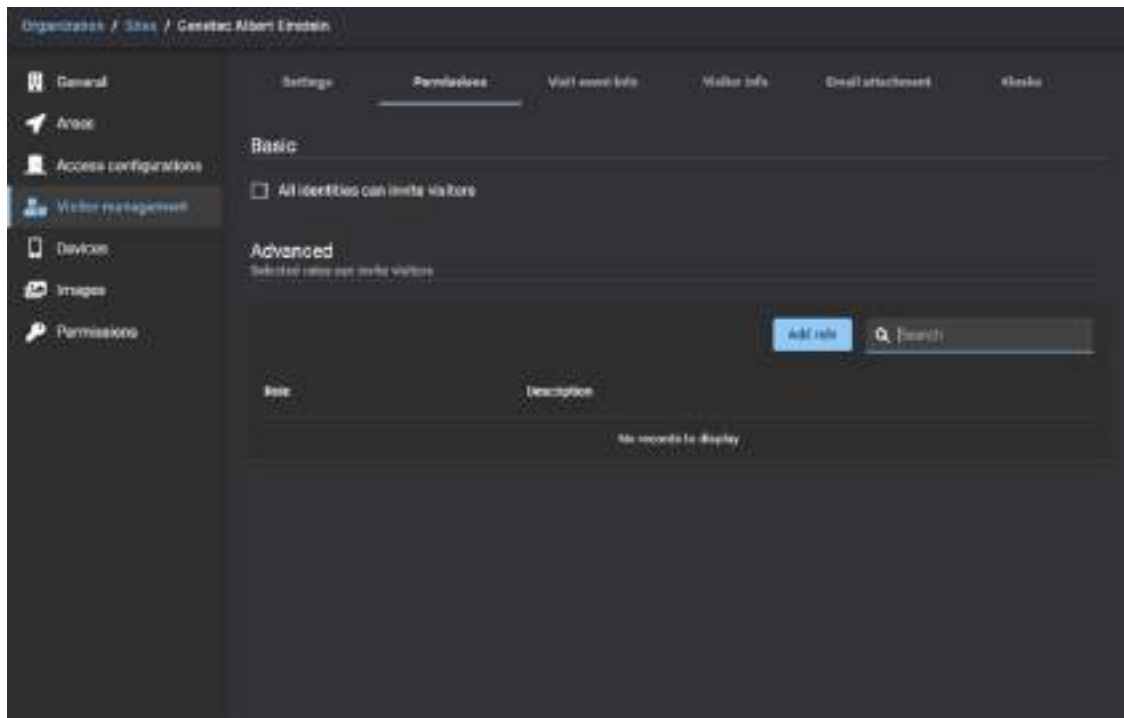
Tip: You can use a Zebra QR code scanner to enter the QR code in the Last name field for you. In the Visitor management task in Security Desk, click in the Search field, scan the QR code and press Enter.

- If the checkbox is cleared, the last name field displays only the last name of the visitor.



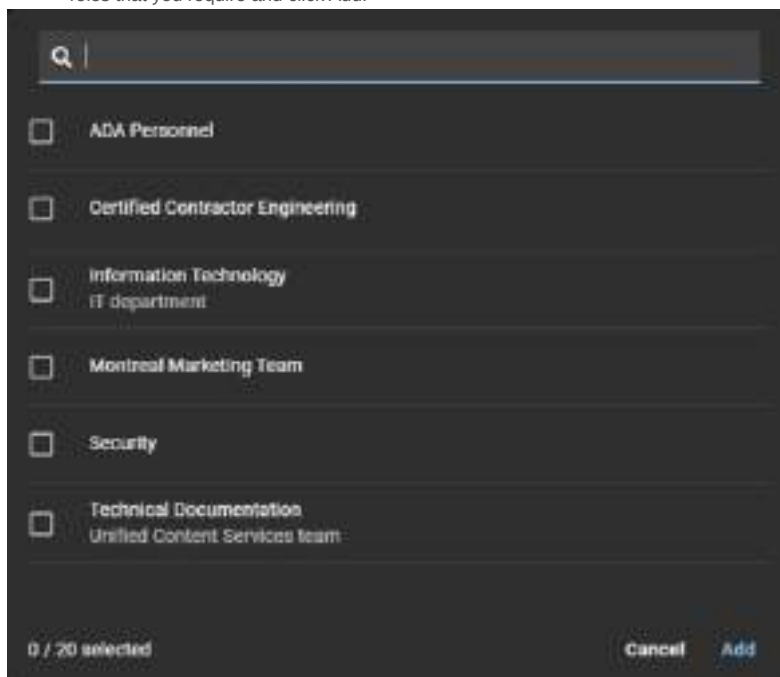
NOTE: When the registration code option is changed, only visitors created after the change are modified, previously created visitors remain unchanged.

5. (Optional) Click the Permissions tab.



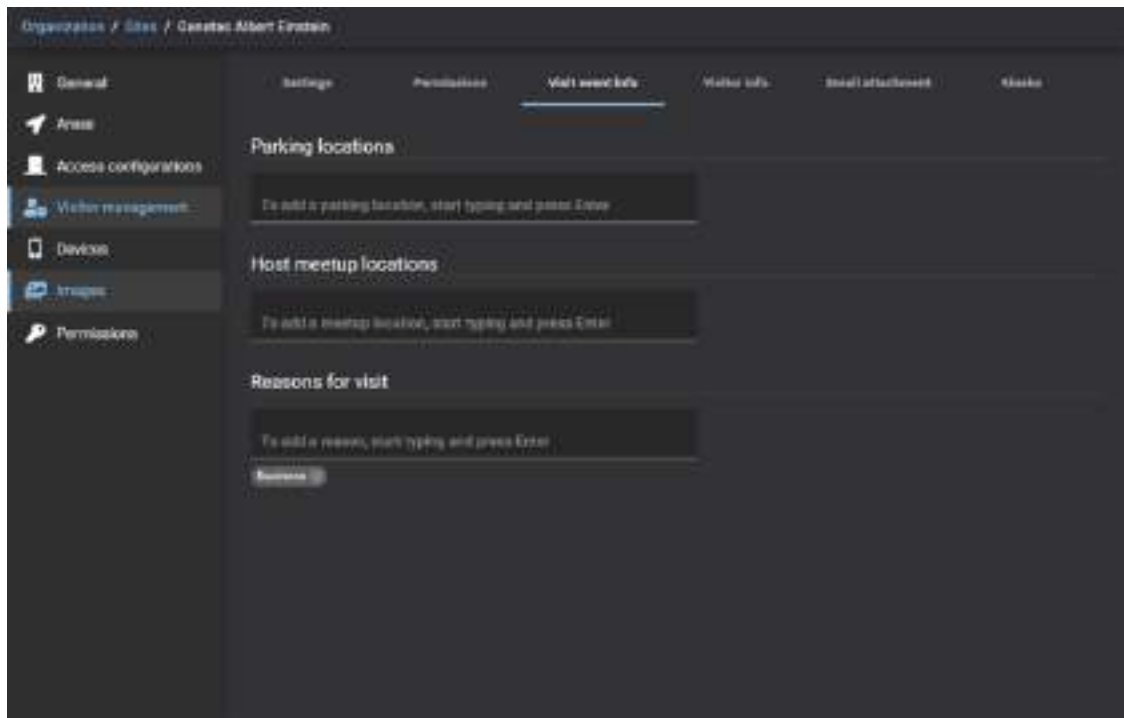
Do one of the following:

- In the Basic section, select the All identities can invite visitors checkbox if you want all identities to be able to invite visitors to this site.
- In the Advanced section, click Add role if you want to use roles to manage who can invite visitors to this site. You can then search for or select the roles that you require and click Add.



Tip: When adding new role permissions, advise role members to log off and log on, if they want to load the new visitor invite permissions immediately.

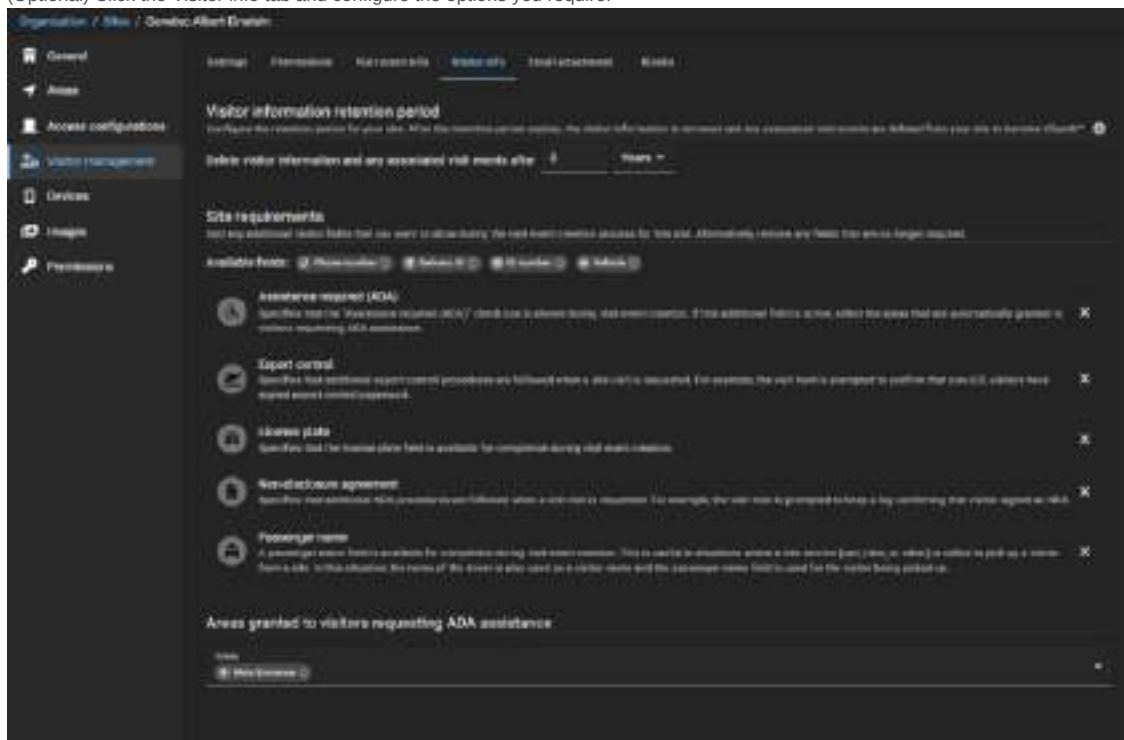
6. (Optional) Click the Visit event info tab and configure the options you require:



- In the Parking locations section, add parking locations.
- In the Host meetup locations section, add meetup locations.
- In the Reasons for visit section, add the typical reasons for visits to your site.

For example, customer meeting, partner meeting, job interview, delivery, taxi pickup, Uber pickup, lift pickup, and so on.

- (Optional) Click the Visitor info tab and configure the options you require:

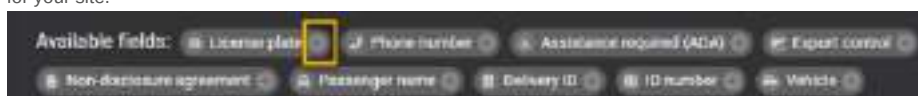


- In the Visitor information retention period section, select a retention period in days, months, or years.

The default retention period is 1 year and the maximum is 3 years.

NOTE: The retention period is configurable by site to comply with the different data laws that might apply in your region.

- In the Site requirements Available fields section, click  to add each additional field that you want to include during the visit event creation process for your site.



License plate

If selected, a license plate field is provided when a site visit is requested.

Phone number

If selected, a phone number field is provided when a site visit is requested.

Genetec ClearID®; User Guide

Displayed in the header

Assistance required (ADA)

If selected, an Areas granted to visitors requesting ADA assistance section is displayed.

NOTE: This assistance option is used to comply with the Americans with Disabilities Act (ADA).

Export control required

If selected, additional export control procedures are followed when a site visit is requested. For example, the visit host is prompted to confirm that non-U.S. visitors have signed export control paperwork.

Non-disclosure agreement

If selected, additional NDA procedures are followed when a site visit is requested. For example, the visit host is prompted to keep a log confirming that the visitor signed an NDA.

Passenger name

If selected, a passenger name field is provided when a site visit is requested. This passenger name field is useful in situations where a ride service (taxi, Uber, or other) is called to pick up a visitor from a site. In this situation, the name of the driver is also used as a visitor name and the passenger name field is used for the visitor being picked up.

Delivery ID

If selected, a delivery ID field is provided when a site visit is requested.

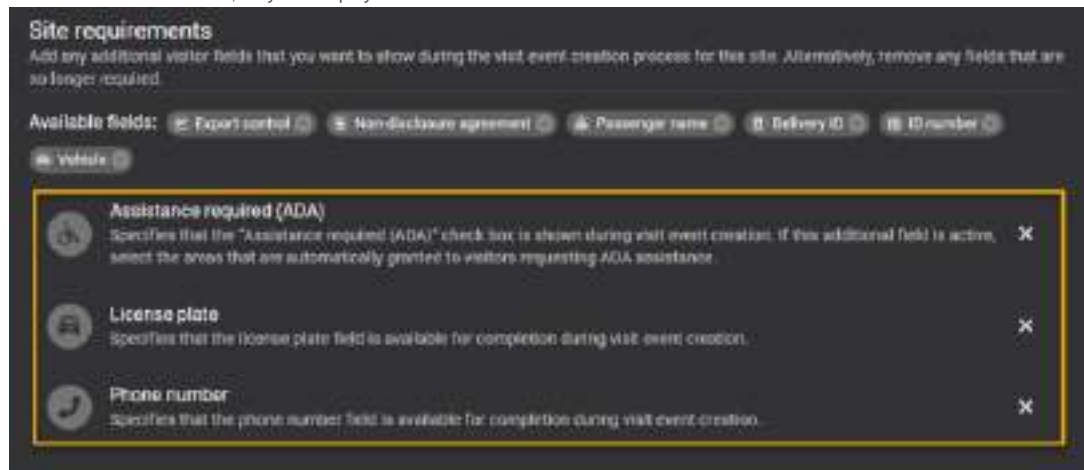
ID number

If selected, an ID number field is provided when a site visit is requested.

Vehicle

If selected, an extra expected vehicle details field is provided when a site visit is requested.

NOTE: As fields are added, they are displayed in the Available fields later in the section.



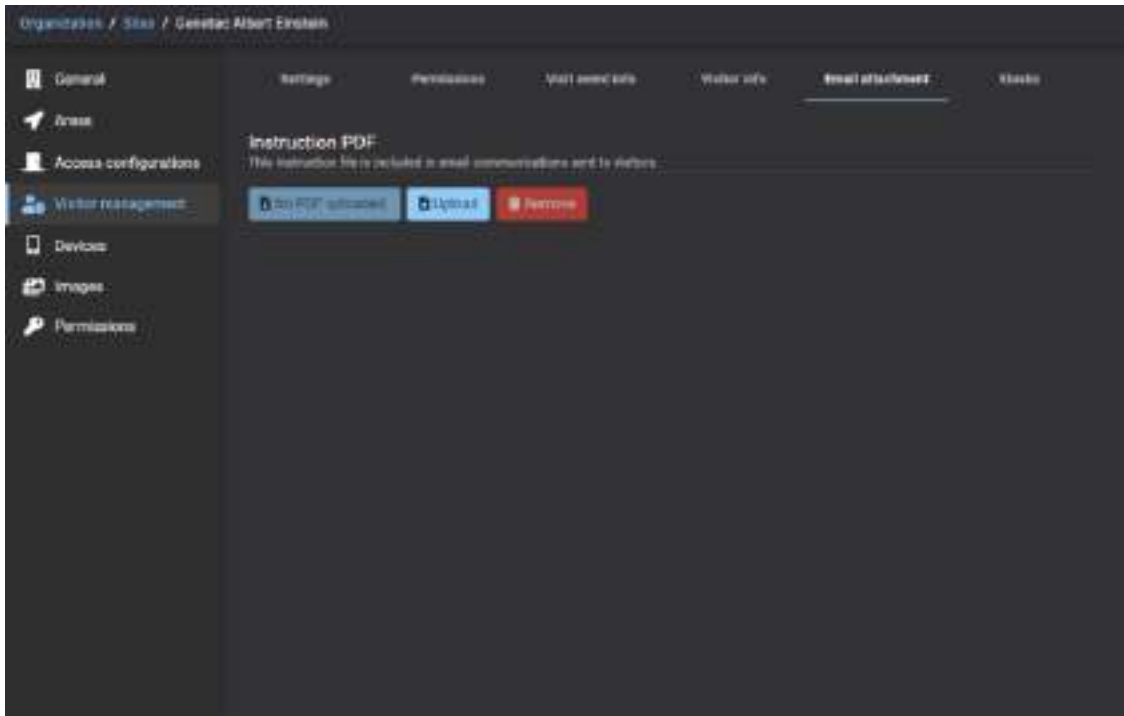
- c. (Optional) If you added Assistance required (ADA) to your site requirements, in the Areas granted to visitors requesting ADA assistance section, add areas that should automatically be granted to visitors requesting ADA assistance.

NOTE: When an employee invites a visitor that requires accessibility assistance to the site, the visitor is automatically added to the list of ADA areas.

For example, If there is a special door for wheelchair access, the people responsible for the site or facilities add that door for wheelchair access in a specific area and add the area to the list of areas granted to visitors that request ADA assistance. If a visitor checks in with ADA enabled, ClearID grants the visitor access to this door, but not other visitors.

- d. (Optional) Click  to remove any visitor fields that are no longer required.

8. Click the Email attachment tab and select the options you require:



Instruction PDF

This instruction file is used if you want to automatically include a Visit Instructions File PDF in email communications with visitors. For example, location details, site map, travel instructions, and so on. Regardless of the uploaded file name, the downloadable instruction file is saved as VisitInstructionsFile.pdf.

No PDF uploaded

Indicates that no Instruction PDF has been uploaded yet.

VisitInstructionsFile.pdf

Click to download a copy of the VisitInstructionsFile.pdf.

NOTE: This button is only visible and active after an Instruction PDF has been uploaded.

Upload

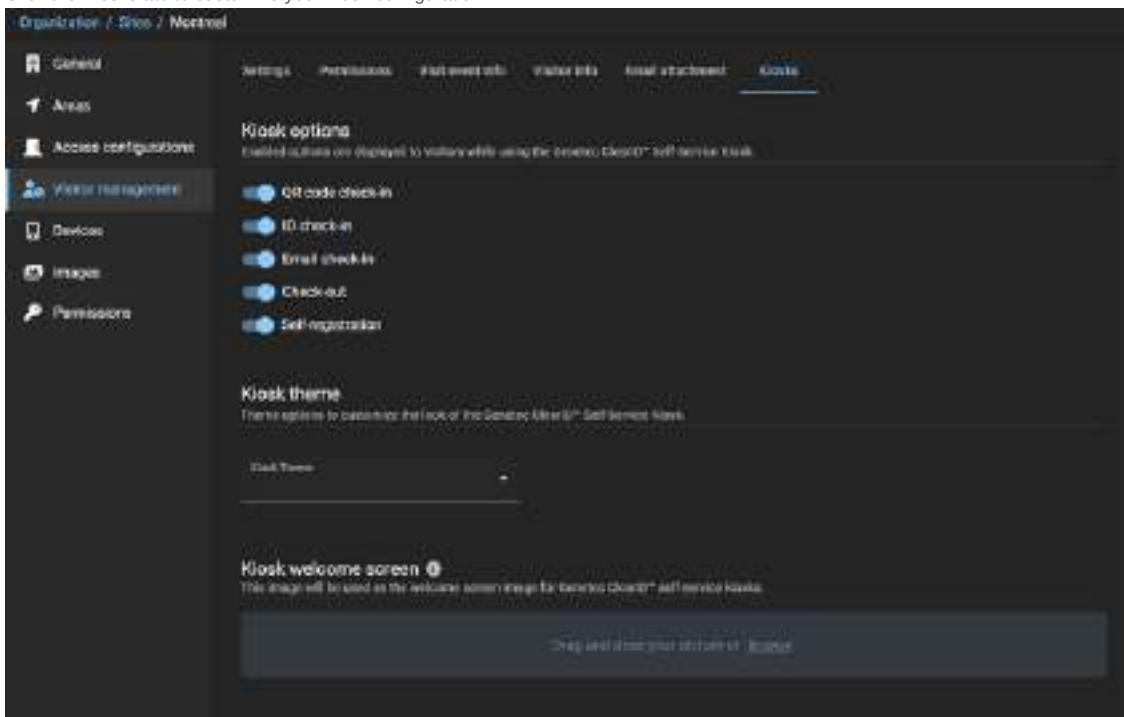
Click to upload a PDF instruction file.

Best Practice: If your instruction file is a word document, click Save as Adobe PDF before uploading to ensure that visitors cannot modify the procedure.

Remove

Click to remove a Visit Instructions File PDF from email communications with visitors.

9. Click the Kiosks tab to customize your kiosk configuration.

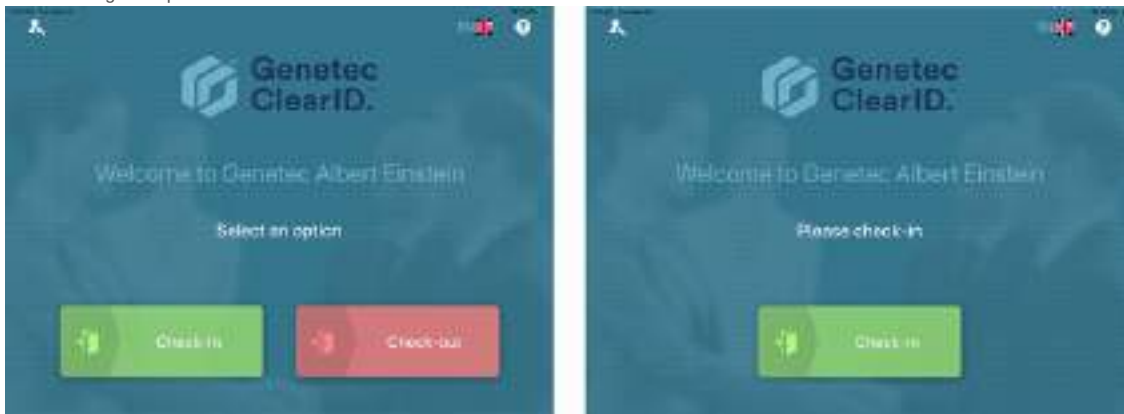


10. (Optional) Customize the Kiosk options.

These options customize the choices that are displayed to your visitors on your ClearID Self-Service Kiosk during the check-in or check-out process.

NOTE: The self-registration option is only displayed when all other check-in options are not applicable.

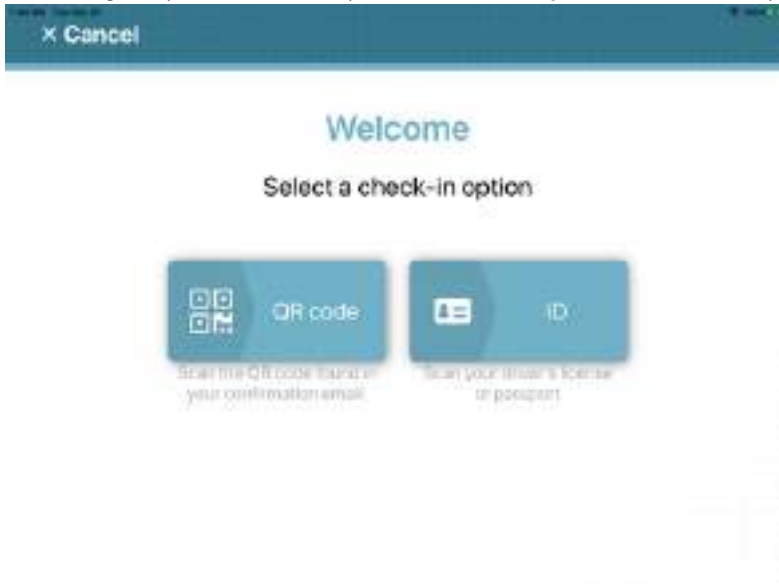
The following example shows the initial check-in or check-out screen customized for two different scenarios.



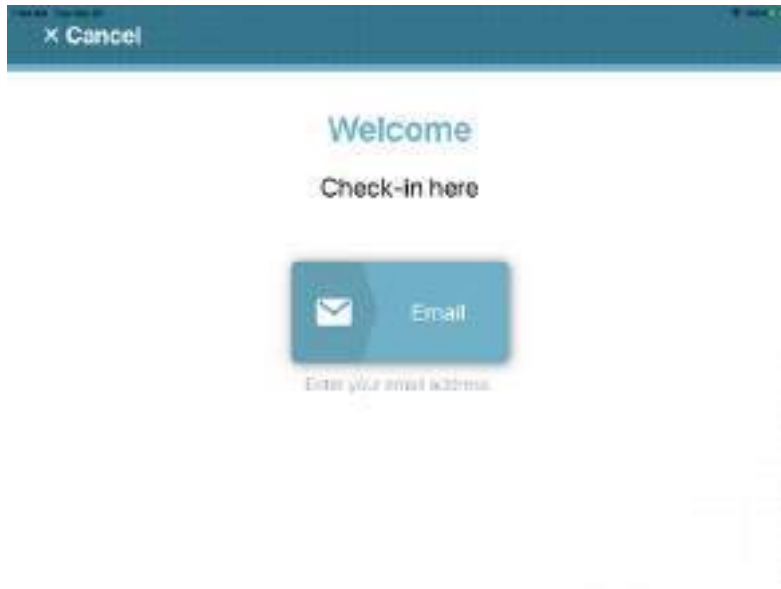
The following example shows the Kiosk options customized with QR code, ID, and Email check-in options enabled.



The following example shows the Kiosk options customized with QR code and ID check-in options enabled.



The following example shows the Kiosk options customized with only the Email check-in option enabled.



11. (Optional) Customize the Kiosk theme.

a. In the Kiosk theme section, choose a theme from the following:

ClearID

The ClearID theme (HEX color code 35768D) has no accent color.

White

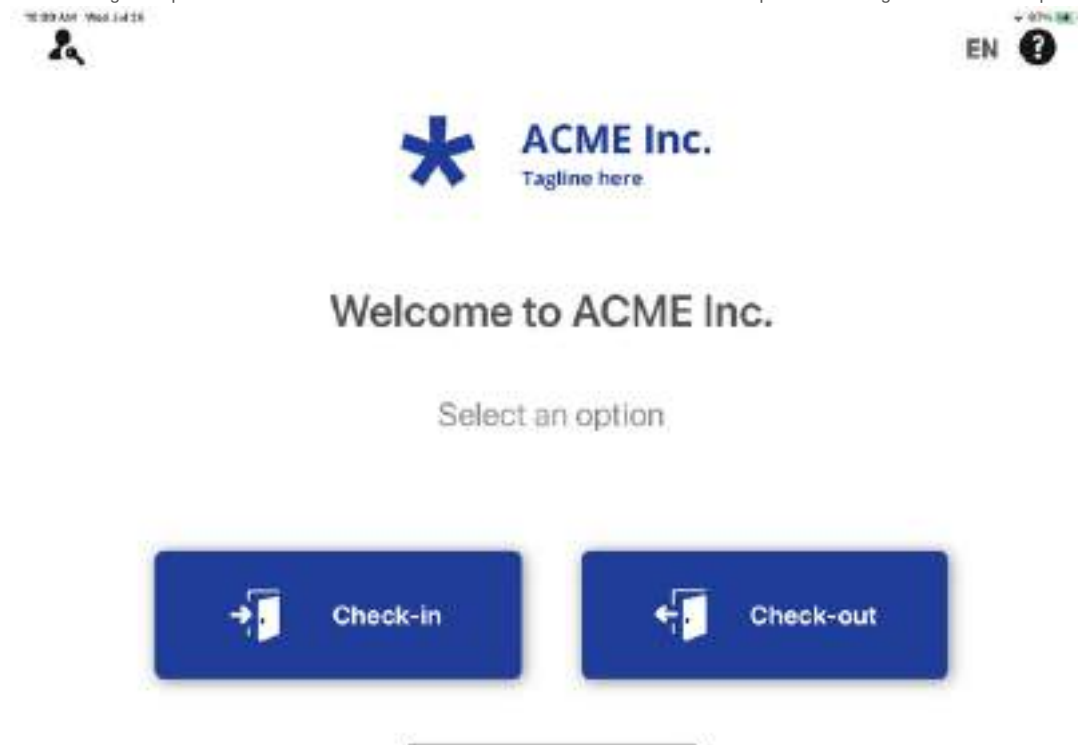
The white theme includes extra controls to pick an accent color. For example, to align with your corporate branding.

b. If you chose the White kiosk theme, select an accent color.

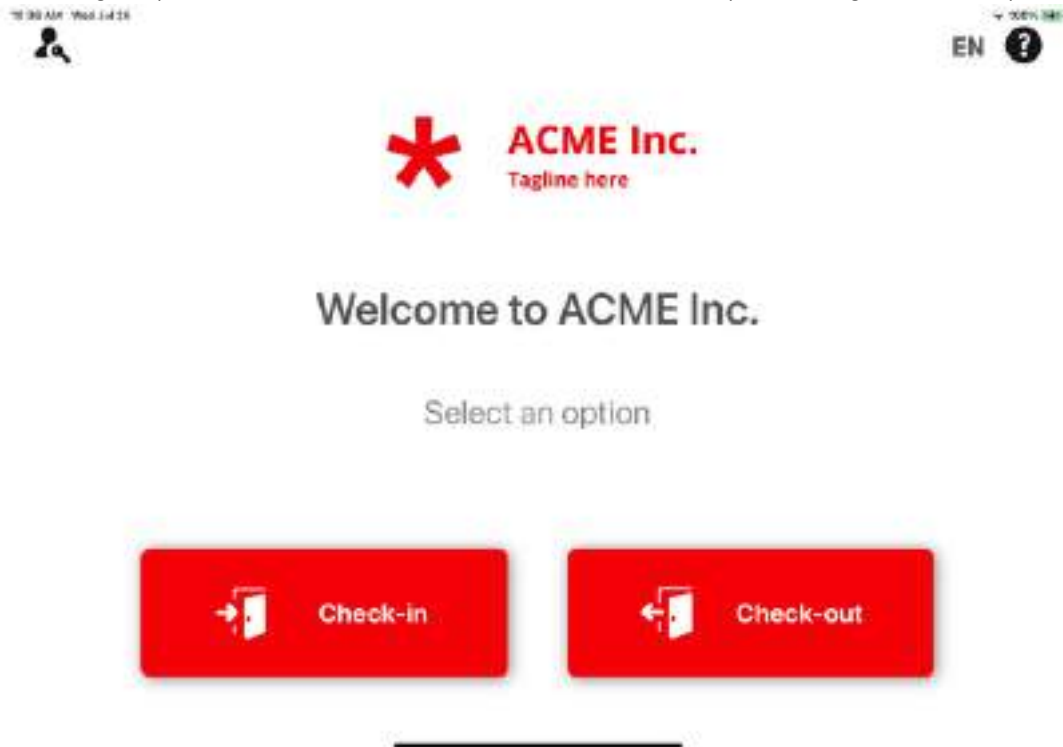


The accent color is applied to the buttons displayed on the ClearID Self-Service Kiosk.

The following example shows the white theme with blue accent color to match the blue corporate branding seen in the example.



The following example shows the white theme with red accent color to match the red corporate branding seen in the example.



12. (Optional) Customize the Kiosk welcome screen.

- a. In the Kiosk welcome screen section, drag and drop your picture or browse to select a Kiosk welcome screen image. This image is used as the welcome screen *company name* or *logo* for the kiosk.

The following example shows the welcome screen with a custom logo image.



13. Click Save.

NOTE: Kiosk options changes are synchronized with your kiosk every 60 seconds.

Results

Visitor management is enabled for the site.

After you finish

Submit an access request or visit request for this site.

Parent topic: Creating sites in ClearID

Browse

- [Introduction to the ADA](#)
- [Visit Instructions file \(Example PDF\)](#)

Browse

- [About workflows in ClearID](#)
- [Inviting visitors in ClearID](#)
- [About ClearID Self-Service Kiosk check-in](#)
- [Enabling QR code credentials for visitors in ClearID](#)

7.2.2.1 | [Viewing sites where a user can invite visitors](#)

[Creating sites in ClearID](#) >

An account administrator might need to view the list of sites where a user can invite visitors so that they can verify or update access if required.

Before you begin

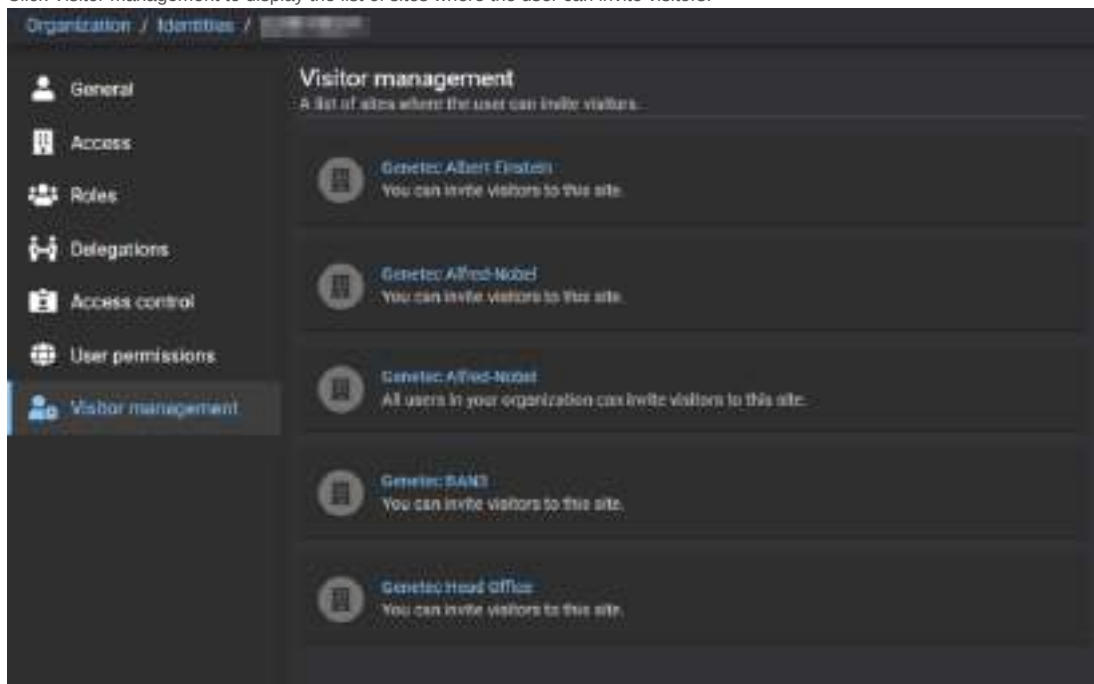
- [Configure your visitor management settings.](#)
- [Add your role members.](#)

What you should know

- Only account administrators can view the list of sites where a user can invite visitors or grant user permissions to invite visitors using roles.
- Users are automatically granted *Invite visitors* permissions for their home site by default.

Procedure

1. From the Home page, click [Organization](#) > [Identities](#).
2. Search for or select a user.
3. Click [Visitor management](#) to display the list of sites where the user can invite visitors.



Parent topic: [Enabling visitor management for sites in ClearID](#)

Browse

- [Granting access to the ClearID web portal](#)

7.3 | [Modifying sites in ClearID](#)

After you add your sites, you can modify the settings of each site individually. An *Account administrator* or *Site owner* can modify the *Site owners*, site properties, and change visitor management options for the site.

Before you begin

Create your sites.

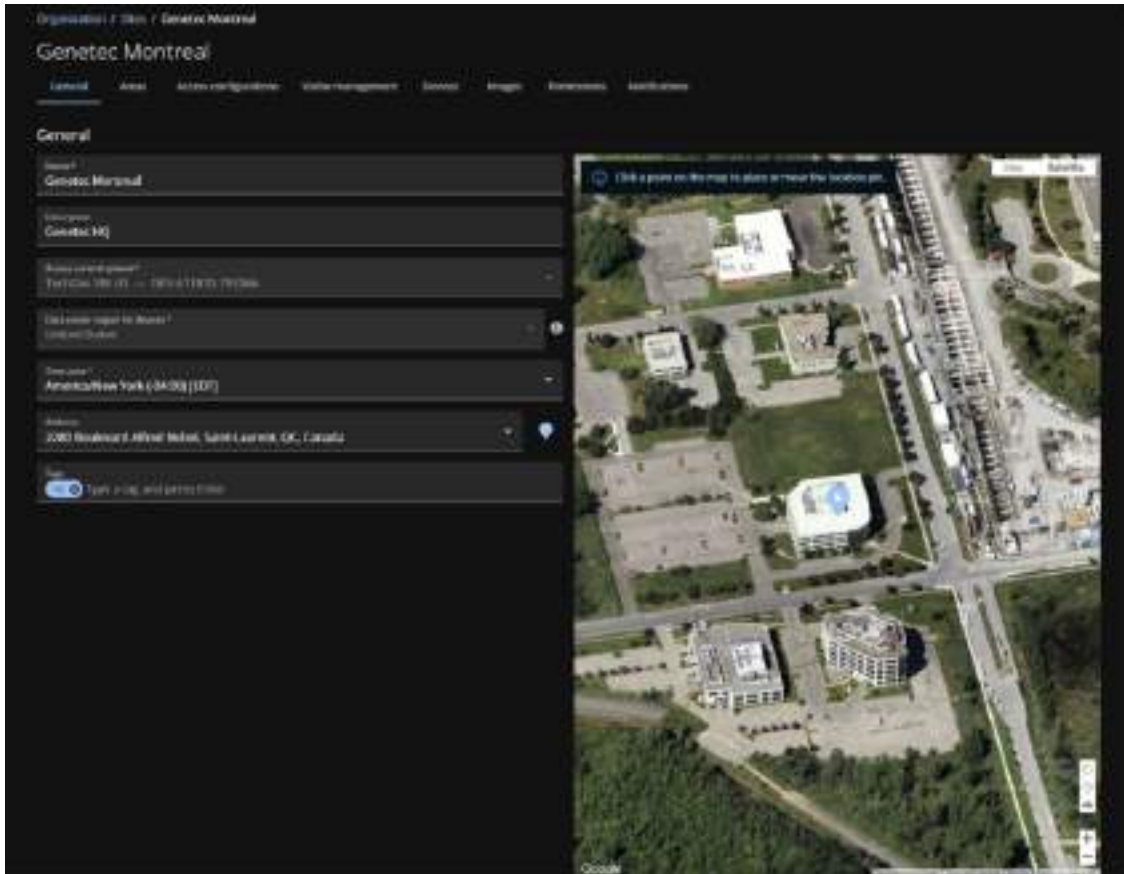
What you should know

To modify sites in Genetec ClearID™, you must be an *Account administrator* or *Site owner*.

- A *site* is associated with a Security Center access control system.
- Multiple sites can be associated with the same Security Center access control system.

Procedure

1. Click Organization > Sites.
2. Search for a site using the search field or select a site from the Site list.



3. On the General page, modify the fields as required.
4. On the Notifications page, modify the fields as required.
5. Click Save.

Results

Your site settings have been changed.

Browse

- [Creating sites in ClearID](#)

7.4 | Setting a maximum duration for site access in ClearID

To enforce a limit for identities with temporary access, you can set a site access duration. When the maximum duration limit is reached, their access expires.

What you should know

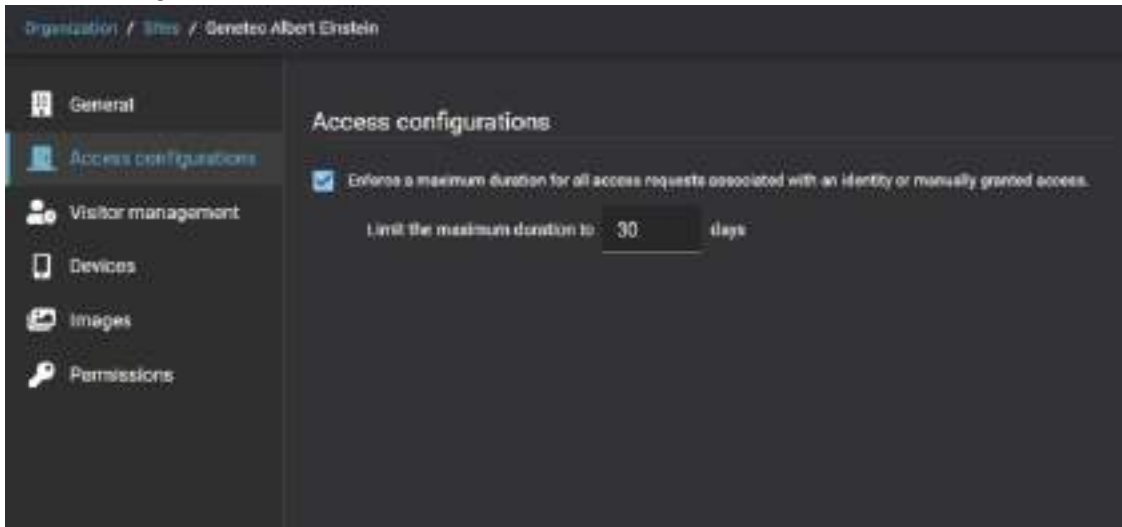
If the maximum duration for site access function has been activated for your account, the maximum duration limit for site access is enabled by default.

- To set a maximum duration period for site access in Genetec ClearID™, you must be a site owner.
- This access duration period only applies to individual identities or access that was manually granted.
- This access duration period does not apply to role access.

Tip: Use role groups when you have people who require permanent access to a site.

Procedure

1. Click Organization > Sites.
2. Search for and select a site.
3. Click Access configurations.



- a. Select the Enforce a maximum duration for all access requests associated with an identity or manually granted access checkbox.
- b. In the Limit the maximum duration to field, enter the maximum duration in days.
You can enter a value in days from 1 to 365. The default value is 30 days.

Browse

- [Adding roles in ClearID](#)
- [Adding role members in ClearID](#)
- [Requesting access in ClearID](#)

7.5 | Configuring access request documents for sites in ClearID

For sites with extra security measures or requirements, *Site owners* can make it mandatory for employees to upload supporting documents like copies of drivers licenses or certifications when requesting access to areas.

Before you begin

Familiarize yourself with [access request workflows](#).

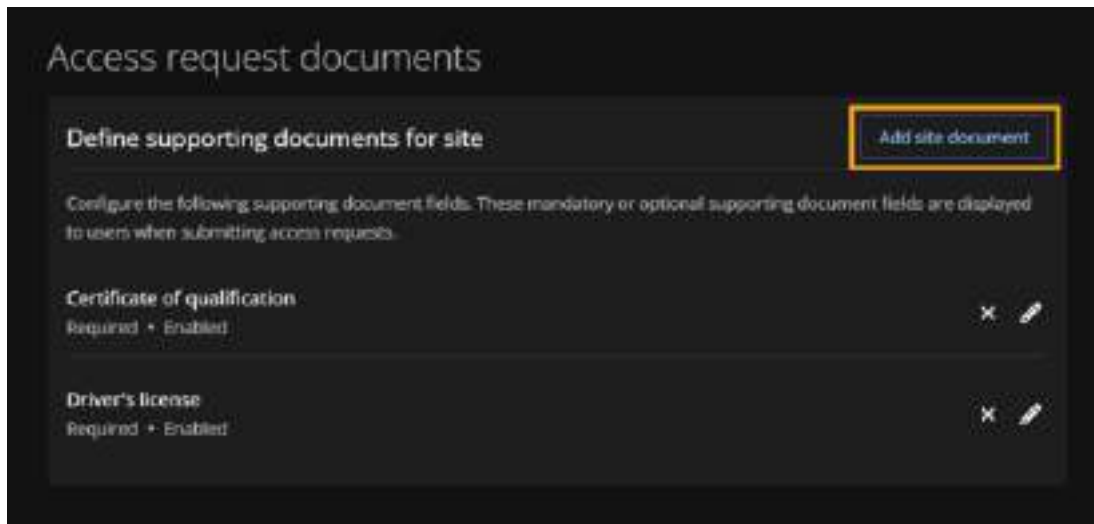
What you should know

- You must be a *Site owner* to configure mandatory or optional supporting documents for access requests at the site level.
- You can configure up to 20 supporting document types per site.

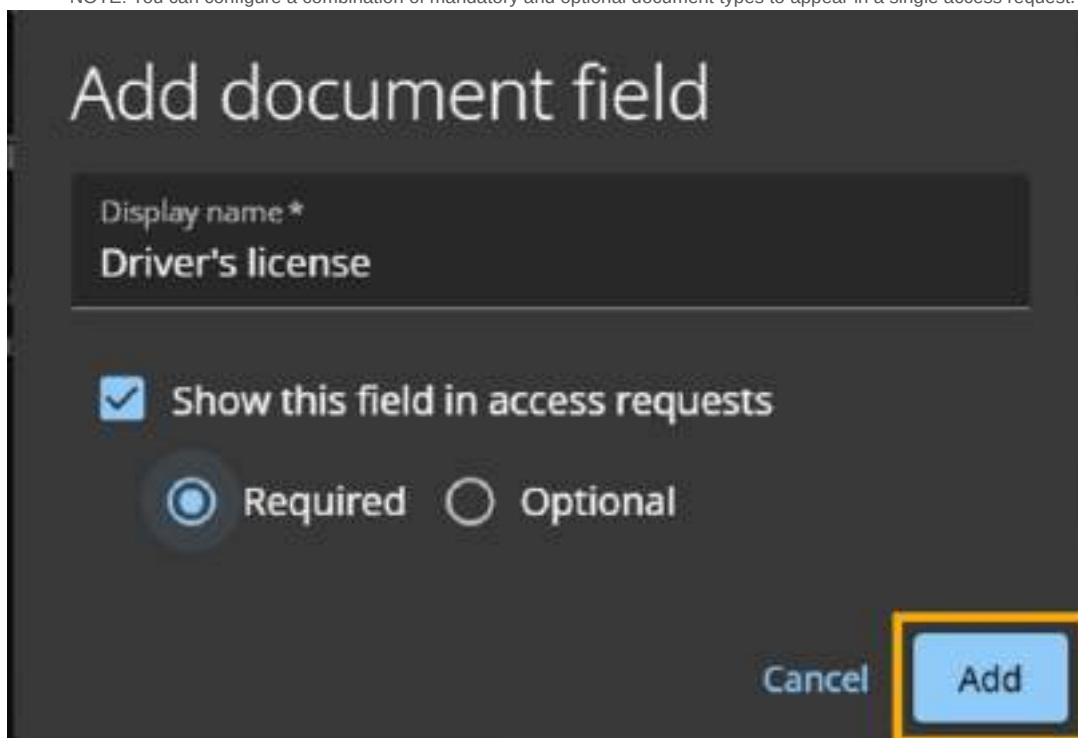
IMPORTANT: All areas inherit supporting documents configured at the site level. If needed, site owners can remove site level supporting document configurations from an area by accessing [area access request settings](#).

Procedure

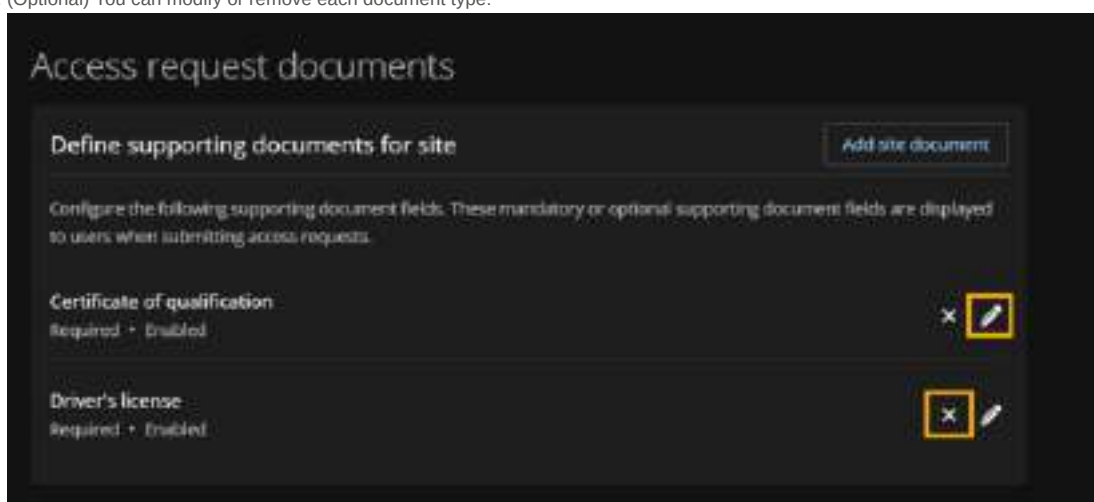
1. In the Genetec ClearID™ web portal, click Organization > Site > Access configurations.
2. Under Define supporting documents for site, click Add site document.



- a. In the Display name field, enter a name for the document type.
 - b. Select Show this field in access requests to display the document field in access requests for the site.
Tip: When the checkbox is cleared, the document type remains available in draft mode.
 - c. Choose whether or not uploading the document is mandatory when submitting an access request by clicking the Required or Optional radio button.
- NOTE: You can configure a combination of mandatory and optional document types to appear in a single access request.



3. Click Add.
4. (Optional) You can modify or remove each document type:



- a. Click  to modify the configuration of a supporting document.

- b. Click  to remove a configured supporting document.

7.6 | Customizing email notifications for sites in ClearID

To communicate specific requirements with email recipients, *Account administrators* and *Site owners* can customize the header and footer text of email notifications sent out by Genetec ClearID™.

What you should know

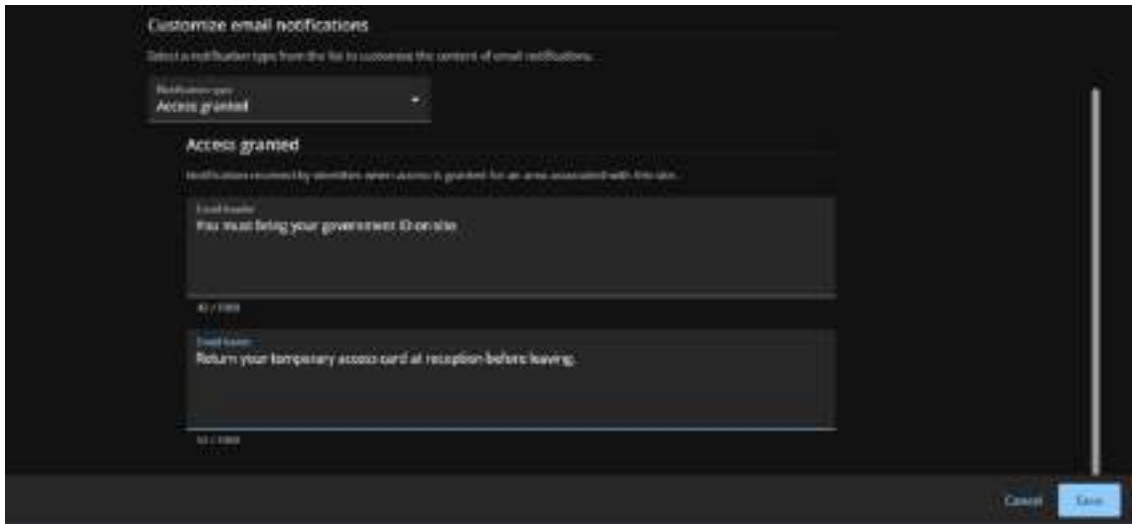
You can customize the header and footer text for two types of email notifications:

- Access granted notifications
- Visitor confirmation notifications

Procedure

1. Click Organization > Sites > Notifications.
2. From the Notification type list in the Customize email notifications section, select the type of email you want to customize.
 - a. In the Email header field, type the header text. For example, use the custom text fields to communicate equipment or documentation requirements to visitors or steps to complete before accessing an area.
 - b. In the Email footer field, type the footer text.

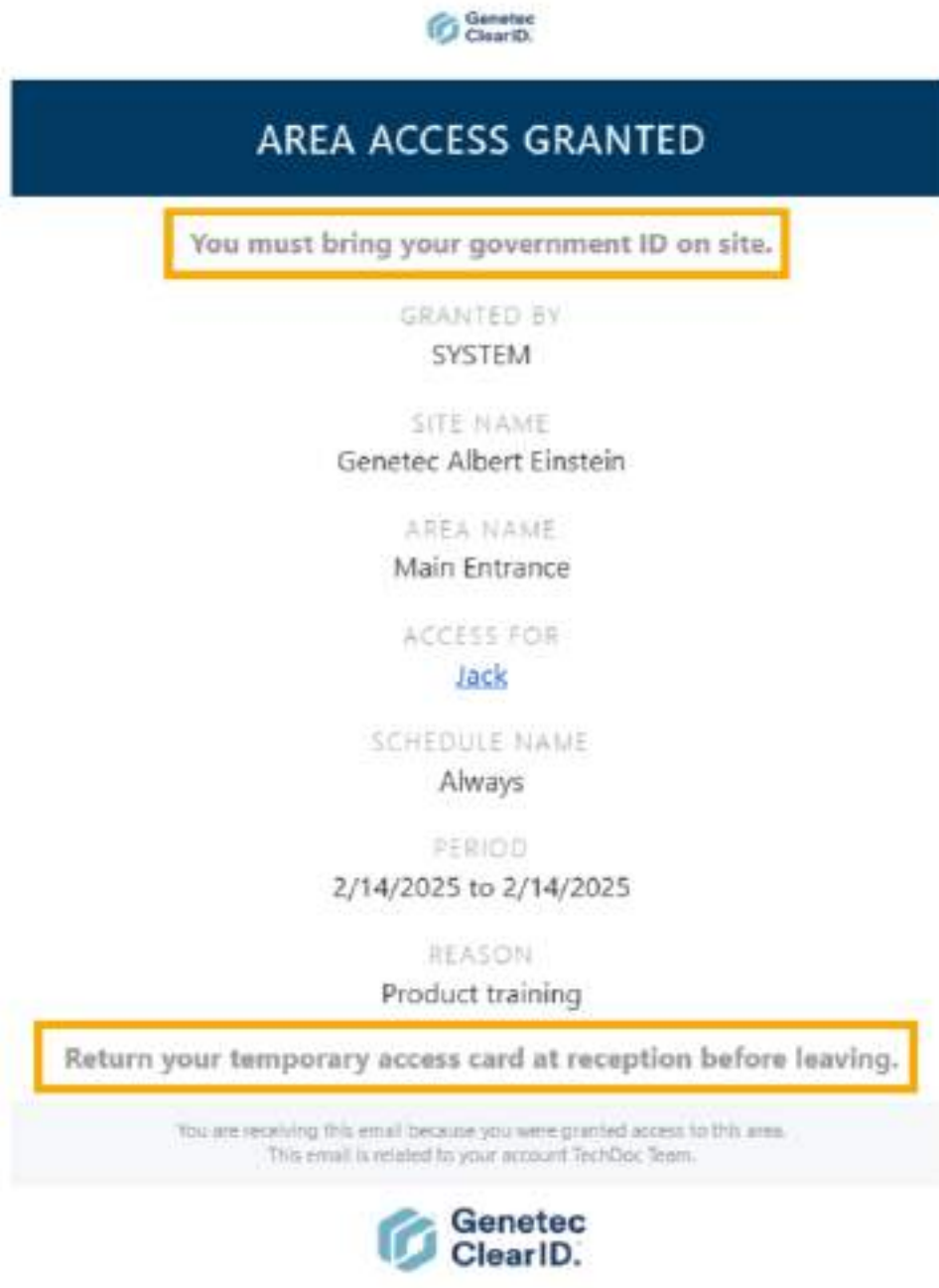
NOTE: Custom text in the header and footer of notification emails is limited to 1,000 characters.



The screenshot shows a web interface titled "Customize email notifications". Below the title, it says "Select a notification type from the list to customize the content of email notifications." A dropdown menu labeled "Notification type" has "Access granted" selected. Below this, the "Access granted" section is shown. It includes a "Email header" field with the text "You must bring your government ID on site" and a "42 / 1000" character count. Below that is an "Email footer" field with the text "Return your temporary access card at reception before leaving." and a "42 / 1000" character count. At the bottom right, there are "Cancel" and "Save" buttons.

3. Click Save.

Email notifications sent out by ClearID use your customized text in the header and footer.



7.6.1 | Customizing ClearID email notification branding

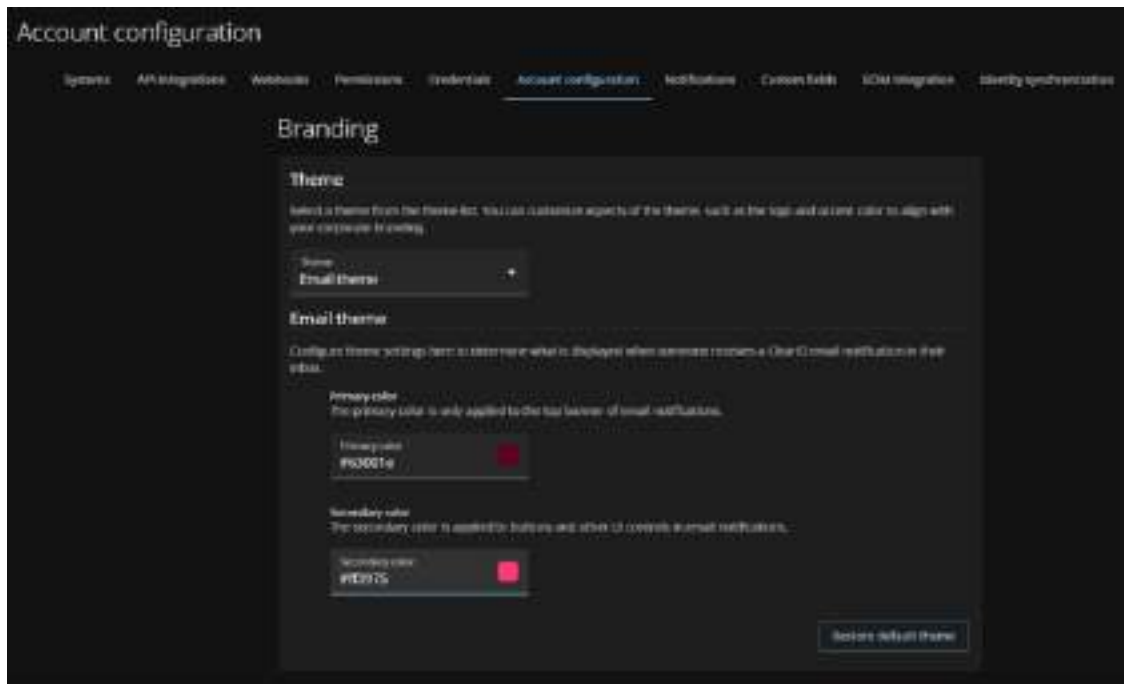
As an *Account administrator*, you can customize the color scheme of Genetec ClearID™ email notifications to align with your company's branding.

What you should know

You must be an *Account administrator* to customize email notification branding.

Procedure

1. In the ClearID web portal, click Administration > Account configuration.
2. In the Branding section, select Email theme from the Theme list.

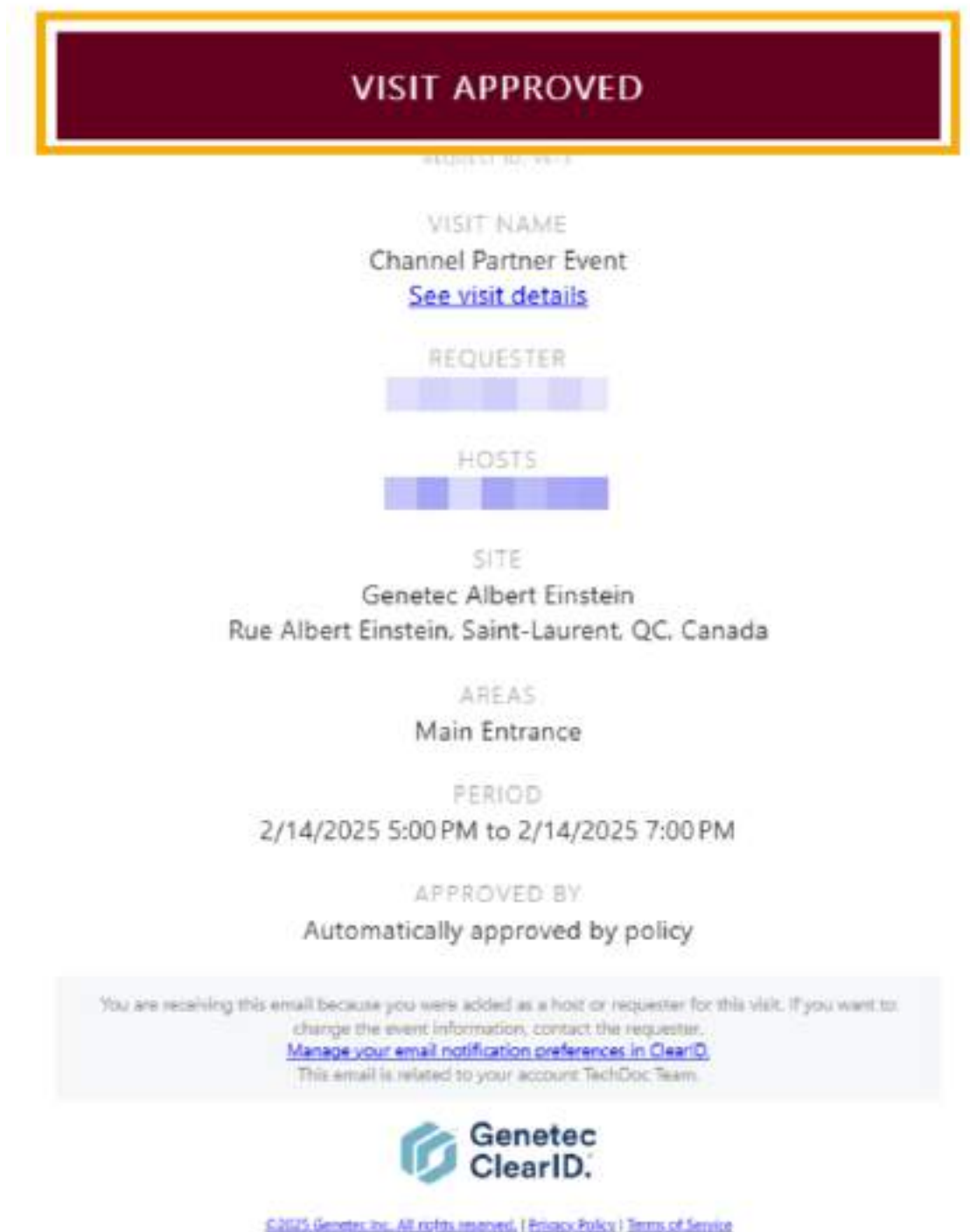


3. In the Email theme section, configure the colors for email notifications:
 - a. In the Primary color field, use the color picker to select a primary color to apply to the top banner of email notifications.
 - b. In the Secondary color field, use the color picker to select a secondary color to apply to buttons and other UI controls in email notifications.

Tip: You can reset the email theme colors to default by clicking the Restore default theme button.
4. Click Save.

Results

Customized branding is applied to the top banner, buttons, and UI controls of email notifications sent by ClearID.



Parent topic: Customizing email notifications for sites in ClearID

7.7 | About access reviews in ClearID

An access review is the process of performing an access review for an area, role, or identity to confirm that the access is still required and valid. To ensure security compliance and audit readiness you can schedule your access reviews to occur automatically.

Traditionally, security personnel manually export list of access and send to area owners to review twice a year, or every quarter.

In Genetec ClearID™ these access reviews can be scheduled (automated) or initiated manually. A site manager or owner is responsible for configuring access review frequency or manually initiating access reviews to ensure that the review process occurs on time.

- Site owners: Access reviews are displayed in the Access reviews report.
- Area managers or role managers: Area access reviews are displayed in My Tasks and notification emails.
- Supervisors: Identity access reviews are displayed in My Tasks and notification emails.

NOTE: Only site owners can access the Access review reports. Area managers can only access reviews for areas that they manage. Supervisors can only access reviews for their direct reports.

You cannot schedule a review for a site that has no areas. If a role or group is associated with an area or room, the role or group becomes part of the area review automatically. All Completed reviews are retained for audit and tracking purposes.



Scheduled access reviews

You can schedule site access reviews to occur yearly, monthly, weekly, or now to suit your needs.

- A site access review for a *Server Room* area could be scheduled to occur Yearly. For example, at quarterly intervals, on the first day of the month at 08:00.
- A site access review for a *Data Center* area could be scheduled to occur Monthly. For example, on the first day of every month at 08:00.

Manual access reviews

You can start an access review manually using the Now schedule when required, to ensure security compliance and audit readiness. Typically manual access reviews are used to test reviews in preparation for an annual review or scheduled reviews to check that all participants are properly set, or to force a review after an incident.

Access review email notifications

Access review email notifications are sent to relevant approvers to indicate that an area or role access review is pending. Site owners do not receive any email notifications.



Access review pending email notification

- When the COMPLETE THE REVIEW hyperlink is clicked, the access review detailed in the email notification is displayed and ready for review.
- When an area manager or role manager clicks the See all your access reviews hyperlink, the My access reviews page is displayed. This view only displays access reviews relevant to the approver.

Access review email notification reminders are sent every 7 days. Access review email notifications are sent from noreply@clearid.io. Check your spam or junk folder if email notifications are not received.

The status of incomplete access reviews are automatically updated to the Expired state when the incomplete access review is replaced by a newer scheduled review with the same name or when the Enforce an expiration for access reviews option is active and the expiration period has been exceeded.

All Completed reviews are retained for audit and tracking purposes. No changes can be made to an access review after it has been completed.
Browse

- [Access Reviews Feature Note \(2 pages\)](#)

7.8 | Setting up automatic expiration for access reviews

To ensure that reviewers only review current access information, you can specify an expiration period for access reviews. Failure to set an expiration could result in reviewers reviewing outdated information.

Before you begin

[Learn about access reviews.](#)

What you should know

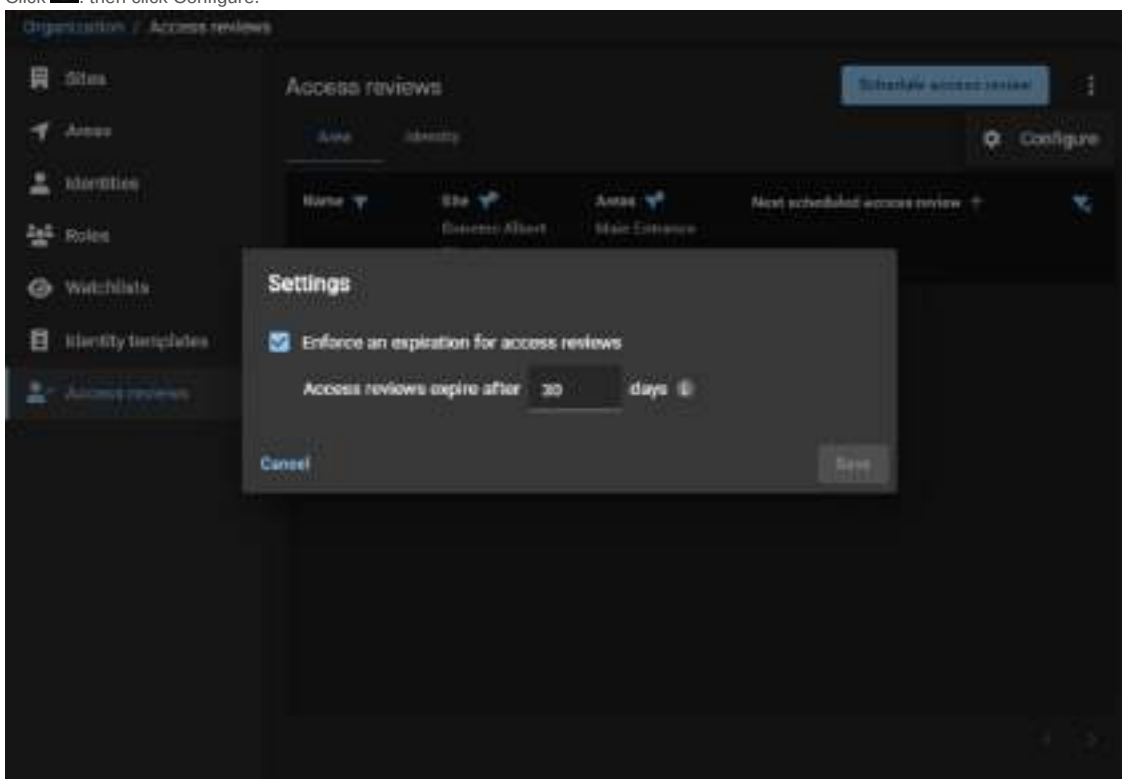
Only an account administrator can configure the expiration settings for access reviews.

Best Practice: The access reviews expiration setting is enabled by default and the default expiration period is set at 30 days.

- The expiration duration set for access reviews applies to all access reviews in the system.
- The new expiration setting is only applied to access reviews created after the setting is enabled or modified.
- When the access reviews expire, their status is set to Expired.
 - Access reviews displayed in My tasks are then changed to Completed with the status Expired.

Procedure

1. From the homepage, click Organization > Access reviews.
2. Click  then click Configure.



3. In the Settings dialog, select or enter the expiration duration that you require for your organization.
Tip: Pick an expiration interval that matches the access reviews requirement for your organization. Also bear in mind any audit or legal requirements that might be applicable.
4. (Optional) If your organization does not want to enforce expiration for access reviews, clear the Enforce an expiration for access reviews checkbox.
5. Click Save to confirm your changes.

After you finish

[Set up your access reviews.](#)

7.9 | Setting up area access reviews in ClearID

To ensure security compliance and audit readiness, you can set up area access reviews to occur at scheduled intervals. You can also start an area access review manually if required.

Before you begin

- Make sure that the site has areas defined.
- Make sure that the site is not already part of another review.

What you should know

- Only a site owner can set up area access reviews.

Best Practice: Schedule your site access reviews so that they are automatically triggered the day, week, or month before corporate audits or site safety checks to ensure your security compliance and audit readiness.

Procedure

In the Genetec ClearID™ web portal, do the following:

- [Schedule your area access reviews](#)

Results

Your area access reviews have now been set up.

After you finish

Do one or more of the following to complete your area access reviews when required:

- [Complete an area access review \(site owner\)](#)
- [Complete an area access review \(area owner\)](#)

Browse

- [Reviewing area access in ClearID](#)

Browse

- [Access Reviews Feature Note \(2 pages\)](#)

7.9.1 | Scheduling area access reviews in ClearID

To ensure security compliance and audit readiness, you can set up area access reviews to occur at scheduled intervals.

Before you begin

- Make sure that the site has areas defined.
- Make sure that the site is not already part of another review.

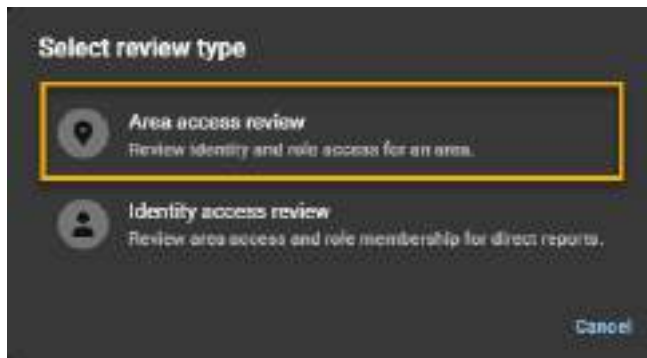
What you should know

- Only a site owner can schedule area access reviews.
- Site owners can define a review schedule for one or multiple areas under their site.

Best Practice: Schedule your site access reviews so that they are automatically triggered the day, week, or month before corporate audits or site safety checks to ensure your security compliance and audit readiness.

Procedure

1. From the homepage, click Organization > Access reviews.
2. Click Schedule access review.
3. In the Select review type dialog, select Area access review.



4. In the Site access review schedule dialog, select the options that you require.

a. Enter a Name for your area access review.

b. Select the Trigger site reviews frequency that you require and configure the options.

NOTE: The options that are displayed vary depending on the Trigger site reviews frequency that you select.

Yearly

Specifies a site access review that occurs yearly.

Monthly

Specifies a site access review that occurs monthly.

Weekly

Specifies a site access review that occurs weekly.

Now

Specifies a site access review that occurs immediately.

For example, an access review could be started manually using the *Now* schedule. Typically manual access reviews are used to test reviews before an annual review or scheduled reviews to check that all participants are properly set, or to force a review after an incident.

c. If you selected Yearly, select the day and month or months that you want the site access review scheduled.

d. If you selected Monthly, select the day that you want the site access review scheduled.

e. If you selected Weekly, select the day or days that you want the site access review scheduled.

f. Select the time that you want the site access review scheduled.

NOTE: The time shown in the Site access review schedules dialog options and all scheduled review times uses the time zone of the site.

g. Search for or select the site that you want to include in your site access review.

h. Search for or select the areas that you want to include in your site access review.

i. (Optional) In the Notes field, you can add more details as needed.

The Notes field is used to enter more detailed information about the site access review. This field is typically used when the site performs security reviews. For example, an ISO 27001 review or a SOC 1 or SOC 2 audit report.

The following example shows a site access review for a *server room* area scheduled to occur Yearly at quarterly intervals, on the first day of the month at 08:00.

Server room (quarterly access reviews)

Site access review schedule

Name *

Server Room (Quarterly Access Reviews)

Trigger site reviews

Yearly

Monthly

Weekly

Now

On the

1st

▼

day of

☒ January

☐ February

☐ March

☒ April

☐ May

☐ June

☒ July

☐ August

☐ September

☒ October

☐ November

☐ December

at

08

▼

00

▼

America/Toronto
(EST -05:00)

Site *

Genetec Head Office

▼

Area *

Server Room

+ Add more

Type to search...

▼

Notes

Close

Create

The following example shows a site access review for a *data center* area scheduled to occur Monthly, on the first day of every month at 08:00.
Data center (monthly access reviews)

Site access review schedule

Name *

Data Center (Monthly Access Reviews)

Trigger site reviews

Yearly

Monthly

Weekly

Now

On the

1st

▼

day of every month

at

08

▼

00

▼

America/New York
(EST -05:00)

Site *

Genetec Montreal

▼

Area *

Data Center

+ Add more

Type to search...

▼

Notes

Close

Create

The following example shows a site access review for a *data center* and *server room* area scheduled to occur Now.

Data center and server room (manual access review scheduled now)

Site access review schedule

Name *

Access review test

Trigger site reviews

Yearly

Monthly

Weekly

Now

Site *

Genetec Montreal

Area *

Data Center

Server Room

Add more

Type to search...

Close

Create

NOTE: Access reviews that are configured with a schedule of Now are not displayed on the scheduled Access reviews page. Instead, they are immediately displayed in the My tasks view of the relevant reviewers.

5. Click Create.

The scheduled access reviews are displayed in the Access reviews page.

Organization / Access reviews

Access reviews

Schedule access review

Area

Security

Name	Site	Area	Next scheduled access review	
Data Center (Monthly Access Reviews)	Genetec Montreal	1 area	January 1, 2023 at 8:00 AM (Monthly)	X
Server Room (Quarterly Access Reviews)	Genetec Montreal	1 area	January 1, 2023 at 12:00 PM (Quarterly)	X

6. (Optional) Click an area access review in the list to see the schedule details.
- a. Click Go to access reviews report to display all access reviews.

Results

Your site area access reviews have now been scheduled.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Do one or more of the following to complete your access reviews when required:

- Complete an area or role access review (site owner)
- Complete an area or role access review (area owner)

Parent topic: [Setting up area access reviews in ClearID](#)

7.10 | Setting up identity access reviews in ClearID

To ensure security compliance and audit readiness, you can set up identity access reviews to occur at scheduled intervals.

Before you begin

- Make sure that the supervisor has direct report identities defined.

What you should know

- Only an account administrator can set up identity access reviews.

Best Practice: Schedule your identity access reviews so that they are automatically triggered before corporate audits or site safety checks to ensure your security compliance and audit readiness.

Procedure

In the Genetec ClearID™ web portal, do the following:

- [Schedule your identity access reviews](#)

Results

Your access reviews have now been set up.

After you finish

[Complete an identity access review \(supervisor\)](#)

7.10.1 | Scheduling identity access reviews in ClearID

To ensure security compliance and audit readiness, you can set up identity access reviews to occur at scheduled intervals. These identity access reviews are performed based on a list of selected roles.

Before you begin

- Make sure that the roles to be reviewed have already been defined.
- Make sure that all the required identities have been associated with the correct roles.

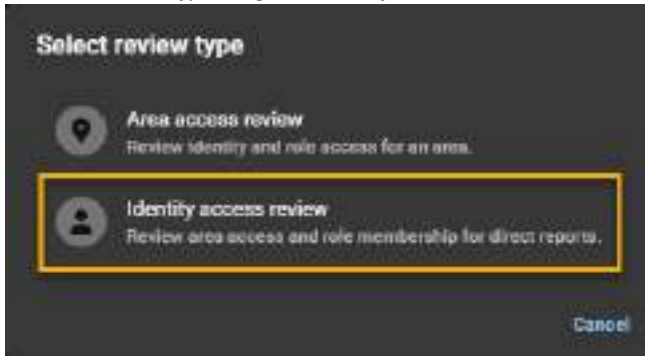
What you should know

- Only an account administrator can schedule identity access reviews.
- For Identity access reviews, only Yearly schedules are supported.
- You can schedule up to five identity access reviews at a time, and each review can include a maximum of 20 roles.

Best Practice: Schedule your identity access reviews so that they are automatically triggered before corporate audits or site safety checks to ensure your security compliance and audit readiness.

Procedure

1. From the homepage, click Organization > Access reviews.
2. Click Schedule access review.
3. In the Select review type dialog, select Identity access review.



4. In the Identity access review schedule dialog, select the options that you require.
 - a. Enter a Name for your identity access review.

For example, You might enter Contractor access review for electricians or Data center identity access review for your direct reports that need access to a data center.
 - b. Select the Trigger identity reviews options that you require.
 - Select the day and month that you want the identity access review scheduled.
 - Select the time that you want the identity access review scheduled.

NOTE: The time shown in the Identity access review schedules dialog options and all scheduled review times use the UTC time zone.
 - c. Select the Roles that you want to include in your Identity access review.

Identity access reviews will be generated for all identities in that role (active and inactive status). Inactive identities are clearly identified in the review.
 - d. (Optional) If you selected Yearly, in the Notes field, you can add more details as needed.

The Notes field is used to enter more detailed information about the identity access review. This field is typically used when a supervisor performs security reviews. For example, an ISO 27001 review or a SOC 1 or SOC 2 audit report.

The following example shows an identity access review for *Electrical contractors* role scheduled to occur Yearly, on the first day of January at 12:00.

Identity access review (yearly access reviews)

Identity access review schedule

None*

Electrical Contractor Identities review (1st review of the year)

Trigger identity reviews

Yearly

On the

1st +

day of

☒ January

☐ April

☐ July

☐ October

☐ February

☐ May

☐ August

☐ November

☐ March

☐ June

☐ September

☐ December

at

12 +

00 +

UTC (-05:00)

Rules*

Electrical contractors

+ Add more

Type to search...

1 / 30

None

Yearly identities review

Close

Create

- 5. Click Create.
- 6. (Optional) Click an identity access review in the list to see the schedule details.
 - a. Click Go to access reviews report to display all access reviews.

Results

Your identity access reviews have now been scheduled.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Do the following to complete your access reviews when required:

- Complete an identity access review (supervisor)

Parent topic: Setting up identity access reviews in ClearID

7.11 | Modifying access reviews in ClearID

After you have set up and scheduled your area or identity access reviews, you can modify or delete them if required.

Before you begin

- [Scheduling area access reviews in ClearID](#)
- [Scheduling identity access reviews in ClearID](#)

What you should know

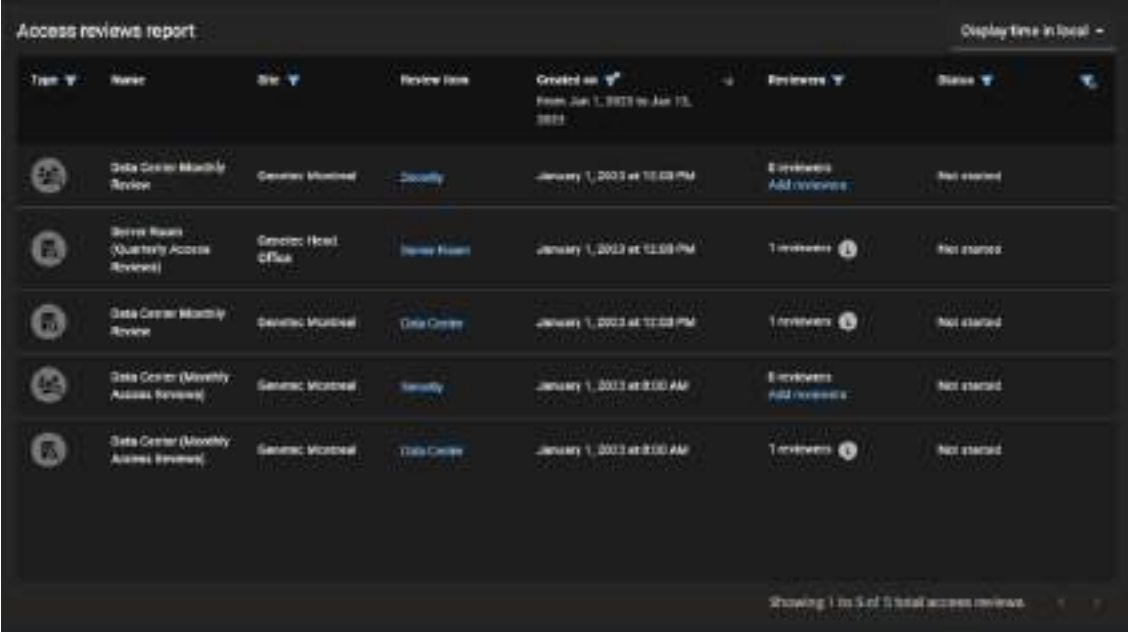
- Only a site owner can modify area access reviews.
- Only an account administrator can modify identity access reviews.

Procedure

1. If you need to make any changes or delete an identity access review schedule, click Organization > Access reviews.
2. To modify an area access review schedule, click the Area tab.
3. To modify an identity access review schedule, click the Identity tab.
4. Click a review in the list and make any changes that you require then click Save.
5. (Optional) To delete an access review, click  next to the review you want to delete then click Remove to confirm the deletion.

7.12 | About access reviews report in ClearID

In Genetec ClearID™, an access reviews report is a list of access reviews. The report includes information about area, role, or identity access reviews and the current review status (not started, started, in progress, completed, or expired).



Type	Name	Site	Review Date	Created on	Reviewers	Status
Area	Data Center Monthly Review	Genetec Montreal	Monthly	January 1, 2023 at 10:00 PM	2 reviewers Add reviewers	Not started
Area	Server Room (Quarterly Access Reviews)	Genetec Host Office	Quarterly	January 1, 2023 at 12:00 PM	1 reviewer Add reviewers	Not started
Area	Data Center Monthly Review	Genetec Montreal	Data Center	January 1, 2023 at 11:00 PM	1 reviewer Add reviewers	Not started
Area	Data Center (Monthly Access Reviews)	Genetec Montreal	Monthly	January 1, 2023 at 8:00 AM	8 reviewers Add reviewers	Not started
Area	Data Center (Monthly Access Reviews)	Genetec Montreal	Data Center	January 1, 2023 at 8:00 AM	1 reviewer Add reviewers	Not started

Showing 1 of 5 of 5 total access reviews

Access reviews report

The access reviews report is used for the following:

- Site owners: To check the status of site access reviews for areas or roles.
- Supervisors: To check the status of identity access reviews (for their direct reports).
- Audits: To provide information to auditors.

Column filters can be used to help refine the report search results by review type, site, created on, reviewers, and status.

For example, you could filter for completed reviews, then select a review and choose Print (hardcopy) or Print > Destination > Save as PDF (softcopy). The hardcopy or softcopy can then be shared with auditors or other members of your organization.

Who can see what?

- Area managers or role managers only see the filters that are relevant to area or role reviews.
- Supervisors only see their direct reports.
- Administrators see everything.

Browse

- [Checking the status of access reviews in ClearID](#)

7.13 | Checking the status of access reviews in ClearID

A site owner is responsible for checking the status of access reviews to ensure that the organization is security-compliant, audit ready, and that the review processes occurs on time. A supervisor can also check the status of identity access reviews for their direct reports.

Before you begin

Set up your access reviews.

What you should know

- Only a site owner can view the complete Access reviews report to check the status or progress of an area or role access review for their site.
- An area manager or role manager only sees their reviews in a My access reviews version of the report.
- A site owner who is not an area owner or manager, or a role owner or manager does not see any access reviews in Dashboard > My tasks.
- Filters: When no types, sites, or reviewers are selected, all results are displayed in the report.

Procedure

1. From the Dashboard, click Reports > Access reviews.

Team	Name	Site	Review type	Created on	Reviewers	Status
	Data Center Monthly Review	Security Montreal	Security	January 1, 2023 at 10:03 PM	8 reviewers Add reviewers	Not started
	Server Room (Quarterly Access Reviews)	Security Montreal	Server Room	January 1, 2023 at 12:03 PM	1 reviewer	Not started
	Data Center Monthly Review	Security Montreal	Data Center	January 1, 2023 at 12:03 PM	1 reviewer	Not started
	Data Center (Monthly Access Reviews)	Security Montreal	Security	January 1, 2023 at 8:00 AM	8 reviewers Add reviewers	Not started
	Data Center (Monthly Access Reviews)	Security Montreal	Data Center	January 1, 2023 at 8:00 AM	1 reviewer	Not started

Showing 1 to 5 of 5 total access reviews

Tip: If any review shows 0 reviewers in the Reviewers column, you can click the Add reviewers hyperlink to add them immediately. This situation typically occurs when there are no owners or managers defined.

2. In the Access reviews report page, select the display time that you require from the following options:

Display time in local

Show report times using the local system time from the computer of the logged-in user.

Display time in UTC

Show report times using Coordinated Universal Time (UTC).

3. In the Created on column, select one of the options, or click Date range and specify a date and time range to display a list of access reviews.

☐ Last 24 hours

☐ Last 7 days

☐ Last 30 days

☐ Last 90 days

☐ Last 365 days

☒ Date range

From * 01/18/2022 To * 10:15 AM

To * 01/18/2023 To * 10:15 AM

Time period limited to a maximum of one year

4. (Optional) If the list is long, configure additional report column filters to narrow report results as required.
 - a. In the Type column, select one or more review types as required:
 - Area access review**
Displays area access reviews.
 - Role access review**
Displays role access reviews.
 - Identity access review**
Displays identity access reviews.
 - b. In the Site column, enter a search string or select one or more sites from the list.
 - c. In the Reviewers column, enter an access reviewer's name or email to show reviews that they are associated with.
 - d. In the Status column, select the status options that you want to display when checking the access review.

NOTE: The status of incomplete access reviews are automatically updated to the Expired state when the incomplete access review is replaced by a newer scheduled review with the same name or when the Enforce an expiration for access reviews option is active and the expiration period has been exceeded.
 - e. (Optional) Click  to reset filter selections.
5. In the Review item column, click a hyperlink to check the details of the access review or to complete the review.
6. (Optional) You can see the list of reviewers by clicking the info icon () next to reviewers.
7. (Optional) If you selected an area access review, click hyperlinks in the Review item column to display additional information about the access review.
8. (Optional) If you selected an access review, click Continue review to complete the access review now.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Do one or more of the following to complete your access reviews when required:

- Complete an area access review (site owner)
- Complete an area access review (area owner)
- Complete an identity access review (supervisor)

Browse

- [About access reviews report in ClearID](#)

7.14 | Completing an area access review (site owner) in ClearID

To ensure security compliance or audit readiness you can perform access reviews to check who has access to an area or role. These periodic reviews are completed by a site owner.

Before you begin

[Set up your site access reviews.](#)

What you should know

- No changes can be made to an access review after it has been completed.
- All Completed reviews are retained for audit and tracking purposes.

Procedure

To complete an area access review:

1. From the Home page, click Reports > Access reviews.
2. (Optional) Configure report column filters as required.
3. In the Access reviews report section, select the area access review that you require.

Access reviews report Display time in local -

Type	Name	Site	Review item	Created on From Jan 1, 2023 to Jan 15, 2023	Reviewers	Status
	Data Center Monthly Review	Genetec Montreal	Security	January 1, 2023 at 10:08 PM	0 reviewers Add reviewers	Not started
	Service Room (Quarterly Access Reviews)	Genetec Head Office	Service Room	January 1, 2023 at 12:08 PM	1 reviewer	Not started
	Data Center Monthly Review	Genetec Montreal	Data Center	January 1, 2023 at 11:08 PM	1 reviewer	Not started
	Data Center (Monthly Access Reviews)	Genetec Montreal	Security	January 1, 2023 at 9:00 AM	0 reviewers Add reviewers	Not started
	Data Center (Monthly Access Reviews)	Genetec Montreal	Data Center	January 1, 2023 at 9:00 AM	1 reviewer	Not started

Showing 1 to 5 of 5 total access reviews

- Click an area hyperlink in the Review item column to begin the access review.
- Click Continue review.

4. In the Details section of the area access review, check the summary details.

Access review for Data Center

Summary Access Review

0 / 9

This access review is a snapshot of identity or role access for Data Center as of September 29, 2023, 1:43 PM / any modifications (identity or role access added or removed) made after this date and time will not be reflected in this access review.

Access review summary
This access review wizard guides you through the process of reviewing identity or role access.

Created by Jamie Myles on September 29, 2023, 1:43 PM

1 reviewer

Close and continue later Next

- Click to see the reviewer details.
- (Optional) Click Close and continue later to pause the review for a later time.
- Click Next to continue to the next section of the access review wizard.

5. In the Access section of the access review, review the access.

Access review for Data Center

Summary **Access** 0/5 Review

Access: 0/5 completed
5 identities or roles have access to this area. Verify that the identity or role access is still valid. Revoked access will be removed after the review is completed.

Approve all remaining ☐ Show already reviewed

Identity	Access	Actions
IT department	September 19, 2023 to Forever - Always Authorized by James Myers on September 14, 2023 (General access - always)	☒ ☐
John Doe	September 19, 2023 to November 15, 2023 - Always Authorized by James Myers on September 14, 2023 (General access)	☒ ☐
Security	September 19, 2023 to Forever - Always Authorized by James Myers on September 14, 2023 (General access - always)	☒ ☐
Superuser (read-only)	September 19, 2023 to November 15, 2023 - Always Authorized by James Myers on September 14, 2023 (General access)	☒ ☐
Test Cloud (read-only)	September 19, 2023 to November 15, 2023 - Always Authorized by James Myers on September 14, 2023 (General access)	☒ ☐

Close and continue later Back Next

- Click Keep access (☒) to confirm that access is still valid.
Tip: Use Approve all remaining to speed up approval process when the list is long, then remove any access that is no longer required.
 - Click Remove access (☐) to remove access that is no longer required.
 - (Optional) Select Show already reviewed to go back and make modifications.
 - Click Next to continue to the next section of the access review wizard.
6. In the Review section of the access review, verify that the review details are correct.

Access review for Data Center

Summary **Access** 5/5 Review

☒ No changes can be made to this access review after it is completed. - ensure that all information is up to date and valid before completing the review.

Additional notes
Enter any additional information or comments relevant to this access review.

Changes summary

When this access review is completed, the following changes will be made:

- 5 identities or roles will have their access revoked from Data Center.
- A report will be created for this access review, which can be found in the Reports section.

Close and continue later Back Complete

- In the Additional notes section, add any notes that you require.
- Before you click Complete, review the changes summary immediately after the Additional notes section.

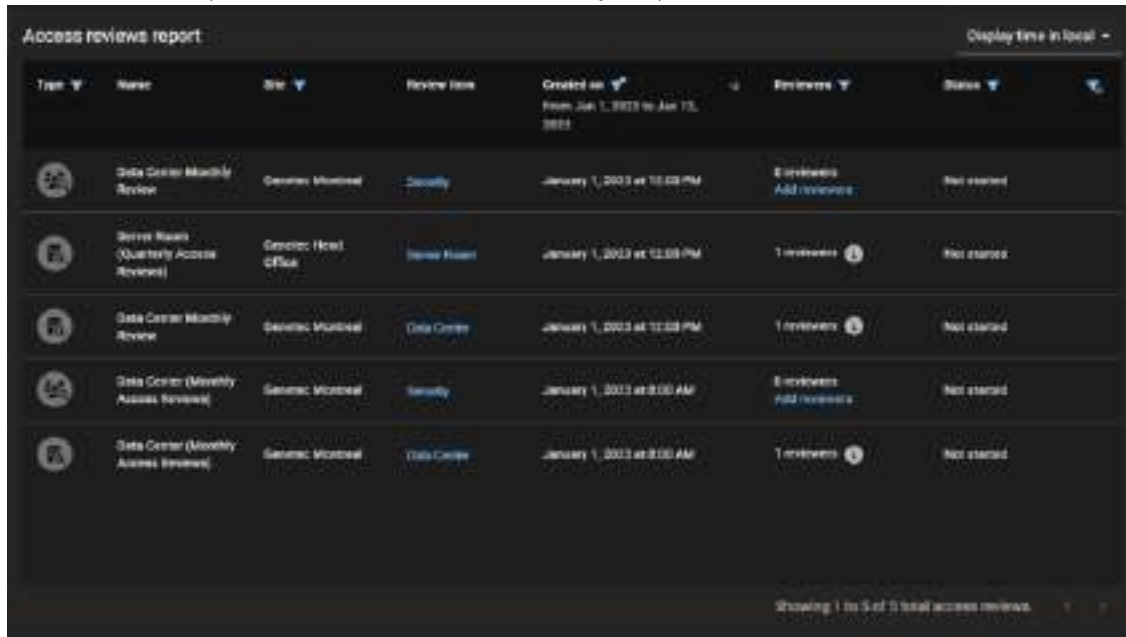
Genetec ClearID®; User Guide

Displayed in the header

- The changes summary displays information about any identity or role changes that will occur when you click Complete.
- (Optional) If any of the information looks incorrect, click Back to return to previous sections and modify your changes.
 - If the Review section details are correct, click Complete.

To complete a role access review:

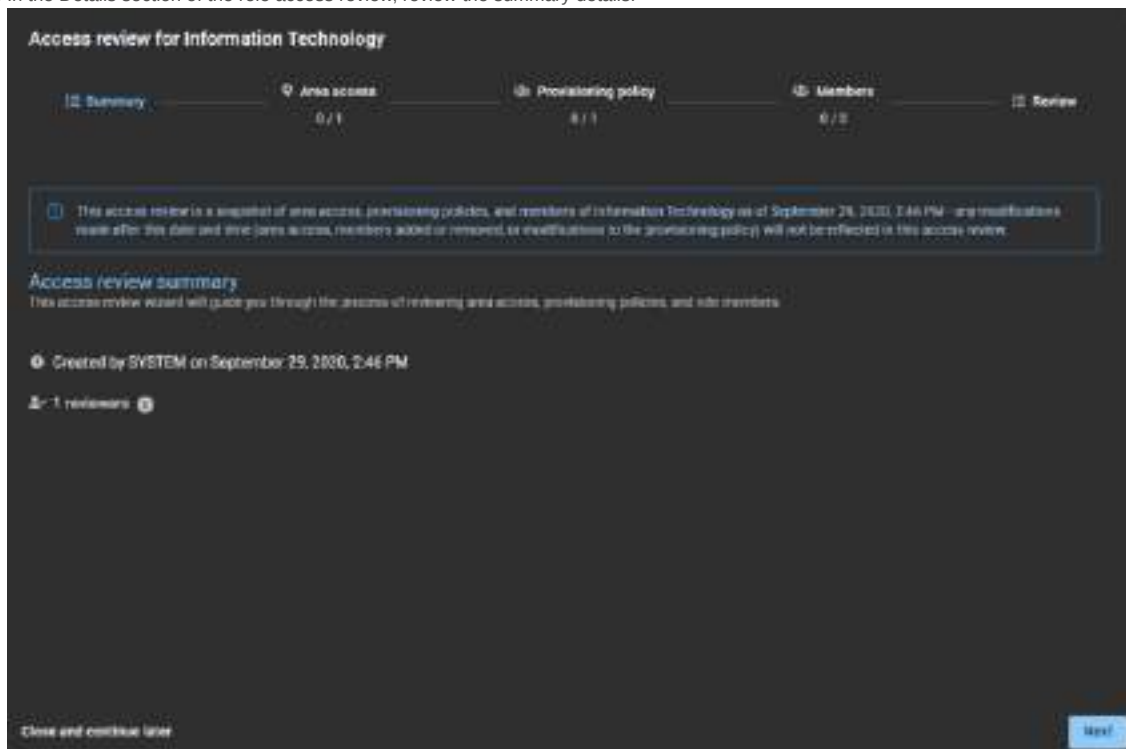
- From the Home page, click Reports > Access reviews.
- (Optional) Configure report column filters as required.
- In the Access reviews report section, select the role access review that you require.



Type	Name	Site	Review item	Created on	Reviewers	Status
	Data Center Monthly Review	Genetec Montreal	Security	January 1, 2023 at 10:03 PM	2 reviewers Add reviewers	Not started
	Server Room (Quarterly Access Reviews)	Genetec Head Office	Server Room	January 1, 2023 at 11:09 PM	1 reviewer	Not started
	Data Center Monthly Review	Genetec Montreal	Data Center	January 1, 2023 at 11:03 PM	1 reviewer	Not started
	Data Center (Monthly Access Reviews)	Genetec Montreal	Security	January 1, 2023 at 8:00 AM	2 reviewers Add reviewers	Not started
	Data Center (Monthly Access Reviews)	Genetec Montreal	Data Center	January 1, 2023 at 8:00 AM	1 reviewer	Not started

Showing 1 in 5 of 5 total access reviews

- Click a role hyperlink in the Review item column to begin the access review.
 - Click Continue review.
4. In the Details section of the role access review, review the summary details.



Access review for Information Technology

Summary | Area access | Provisioning policy | Members | Review

0 / 1 | 0 / 1 | 0 / 0

This access review is a snapshot of area access, provisioning policies, and members of Information Technology as of September 29, 2023, 2:46 PM – any modifications made after this date and time (area access, members added or removed, or modifications to the provisioning policy) will not be reflected in this access review.

Access review summary

This access review wizard will guide you through the process of reviewing area access, provisioning policies, and role members.

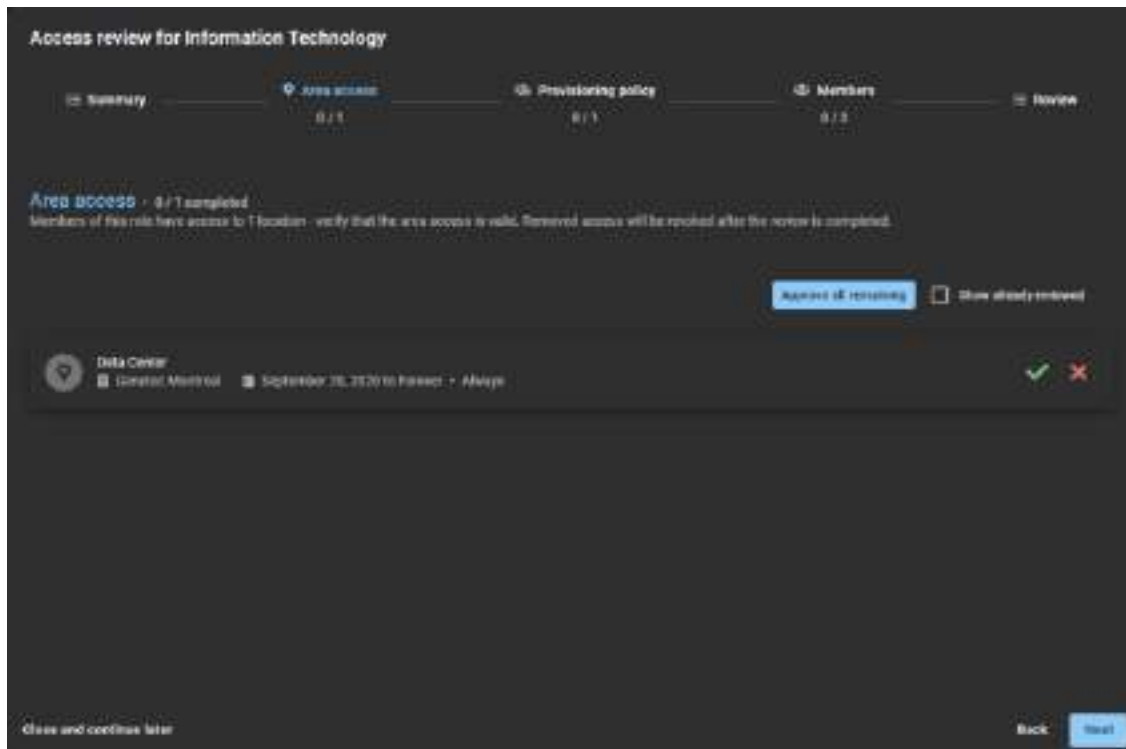
Created by SYSTEM on September 29, 2023, 2:46 PM

1 reviewer

Close and continue later

Next

- Click ⓘ to see the reviewer details.
 - (Optional) Click Close and continue later to pause the review for a later time.
 - Click Next to continue to the next section of the access review wizard.
5. In the Area access section of the role access review, review the access.



- a. Click Keep access (✓) to confirm that access is still valid.
Tip: Use Approve all remaining to speed up approval process when the list is long, then remove any access that is no longer required.
 - b. Click Remove access (✗) to remove access that is no longer required.
 - c. (Optional) Select Show already reviewed to go back and make modifications.
 - d. Click Next to continue to the next section of the access review wizard.
6. In the Provisioning policy section of the role access review, confirm that the policies are still valid.



- a. (Optional) Click view or edit the policy to open the Provisioning policy page to view or make changes to the policy.
 - b. Click Approve policy (✓) to confirm that policy is still valid.
 - c. Click Next to continue to the next section of the access review wizard.
7. In the Members section of the role access review, confirm that the members are still valid.

Access review for Information Technology

Summary 1 / 1 Area access 1 / 1 Provisioning policy 1 / 1 **Members 6 / 6** Review

Role members • 6 / 6 completed
The following members have been added to this role manually - verify that this information is up to date. Reported members will be removed from the role after the review is completed.

[Approve all remaining](#) ☐ Show already reviewed

	Supervisor Jaramila • jaramila.supervising@gmail.com Authorized by Josue Myles on September 20, 2023 (Temporary access added manually)		
	Yves David L. Myles • yves.lmylesm@gmail.com Authorized by Josue Myles on September 20, 2023 (Temporary access added manually)		
	Neil Jaramila • jaramila.neil@gmail.com Authorized by Josue Myles on September 20, 2023 (Temporary access added manually)		

Close and continue later Back Next

- Click Keep access () to confirm that access is still valid.
Tip: Use Approve all remaining to speed up approval process when the list is long, then remove any access that is no longer required.
- Click Remove access () to remove access that is no longer required.
- (Optional) Select Show already reviewed to go back and make modifications.
- Click Next to continue to the next section of the access review wizard.

8. In the Review section of the role access review, verify that the review details are correct.

Access review for Information Technology

Summary 1 / 1 Area access 1 / 1 Provisioning policy 1 / 1 **Members 6 / 6** **Review**

No changes can be made to this access review after it is completed - ensure that all information is up to date and valid before completing the review

Additional notes
Enter any additional information or comments relevant to this access review.

Additional notes

When this access review is completed, the following changes will be made:

- Information Technology will have its access revoked for 6 areas.
- No changes to the role provisioning policy.
- 6 members will be removed from Information Technology.
- A report will be created for this access review, which can be found in the Reports section.

Close and continue later Back Complete

- In the Additional notes section, add any notes that you require.
- Before you click Complete, review the changes summary immediately after the Additional notes section.
- (Optional) If any of the information looks incorrect, click Back to return to previous sections and modify your changes.
- If the Review section details are correct, click Complete.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Generate an access reviews report.
Browse

- Reviewing area access in ClearID

Browse

- Access Reviews Feature Note (2 pages)

7.15 | Completing an area access review (area manager or role manager) in ClearID

To ensure security compliance or audit readiness, you can perform access reviews to check who has access to an area or role. These periodic reviews are completed by an area manager or role manager.

Before you begin

Check your mail for an *Access Review Pending* email notification or look on the My tasks page for a pending review.

What you should know

- Area managers or role managers can complete an access review from the My tasks page of the Dashboard or from an email notification.
- No changes can be made to an access review after it has been completed.
- All Completed reviews are retained for audit and tracking purposes.
-

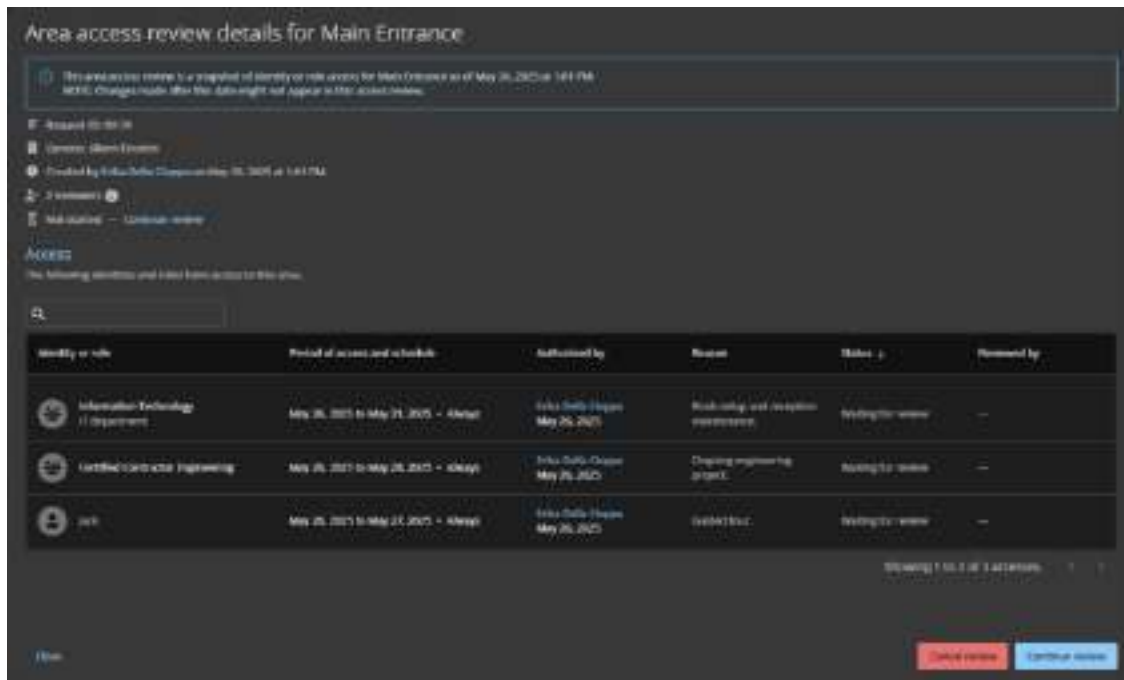
Procedure

To complete an area access review from the Dashboard page:

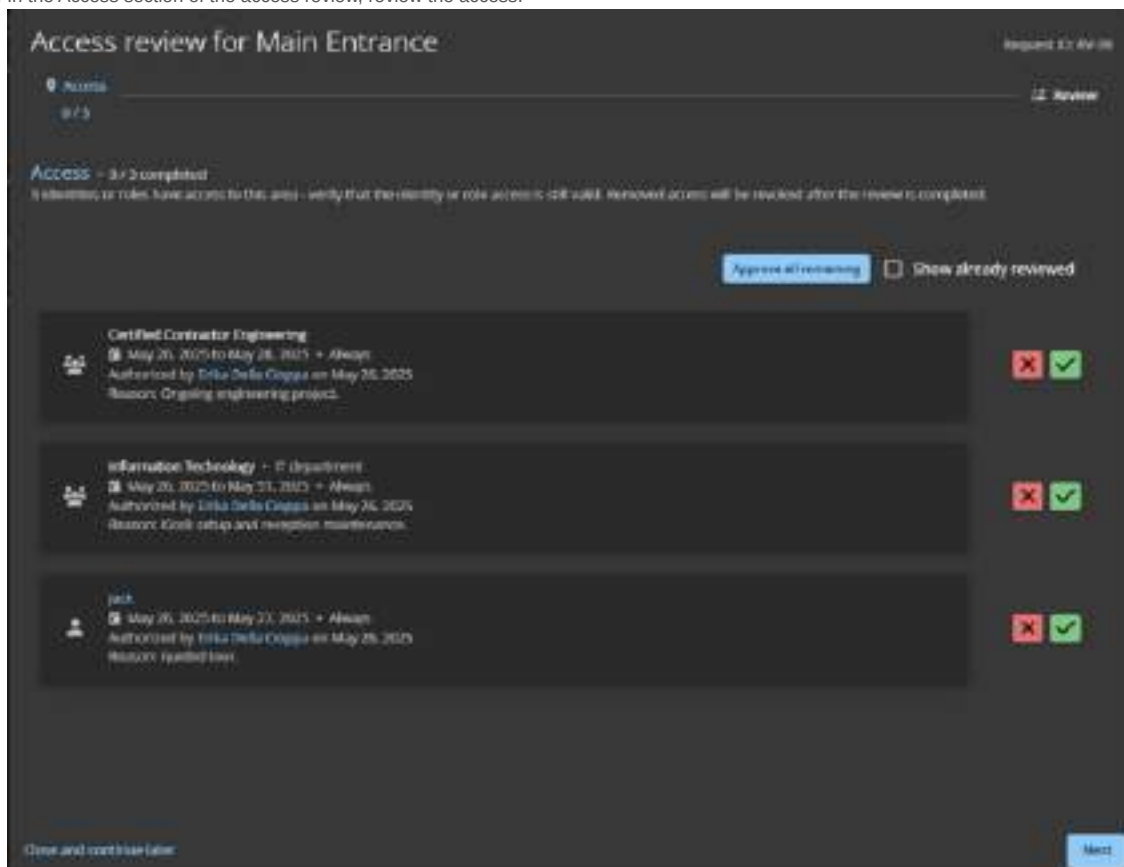
1. Click Dashboard > My tasks.
2. In the My tasks list, click the area that you require.



3. In the Details section of the area access review, check the summary details.



- a. Click  to see the reviewer details.
 - b. (Optional) Click Close and continue later to pause the review for a later time.
 - c. Click Next to continue to the next section of the access review wizard.
4. Click Continue review.
 5. In the Access section of the access review, review the access.



- a. Click Keep access () to confirm that access is still valid.
Tip: Use Approve all remaining to speed up approval process when the list is long, then remove any access that is no longer required.
 - b. Click Remove access () to remove access that is no longer required.
 - c. (Optional) Select Show already reviewed to go back and make modifications.
 - d. Click Next to continue to the next section of the access review wizard.
6. In the Review section of the access review, verify that the review details are correct.

Access review for Main Entrance

Report ID: 04-04

Alerts 3 of 3 Review

No changes can be made to this access review after it is completed. Ensure that all information is up to date and valid before completing the review.

Additional notes

Enter any additional information or comments relevant to this access review. The contents of additional information are not monitored by an administrator and are for audit viewing purposes only.

Add notes

When this access review is completed, the following changes will be made:

- 1 identity or role will have their access revoked from Main Entrance.
- A report will be created for this access review, which can be found in the Reports section.

Click and continue later Back Complete

- In the Additional notes section, add any notes that you require.
- Before you click Complete, review the changes summary immediately after the Additional notes section.
The changes summary displays information about any identity or role changes that will occur when you click Complete.
- (Optional) If any of the information looks incorrect, click Back to return to previous sections and modify your changes.
- If the Review section details are correct, click Complete.

To complete a role access review from the Dashboard page:

- Click Dashboard > My tasks.
- In the My tasks list, click the role that you require.

Genetec Dashboard

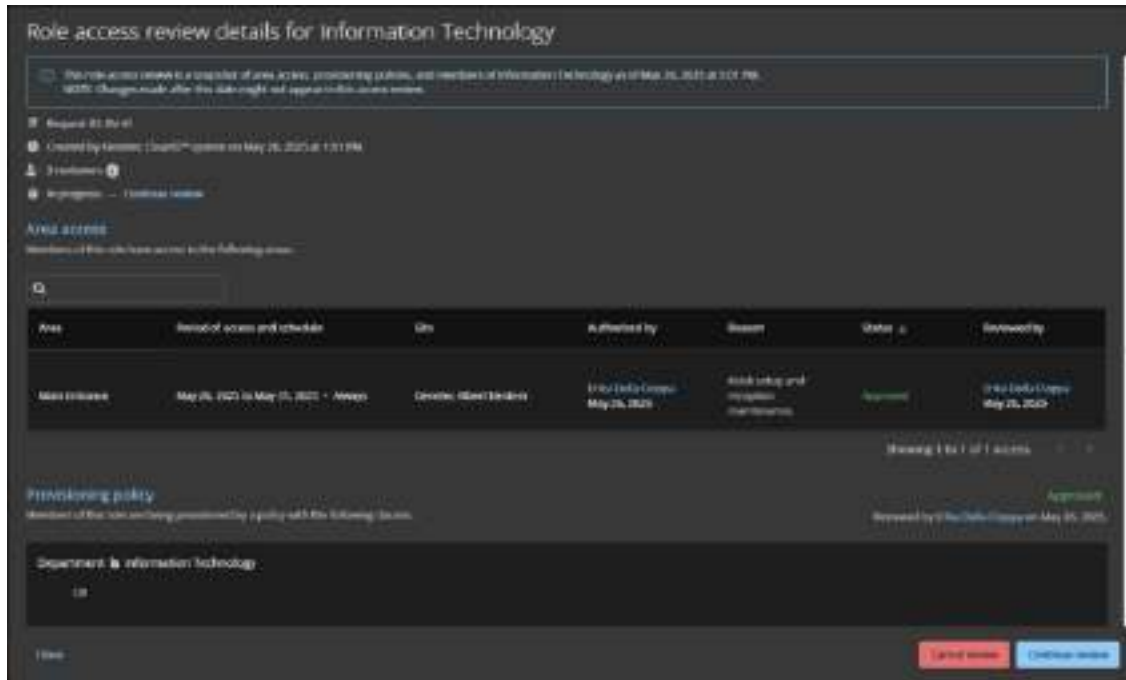
My tasks My tasks My tasks

Filtering

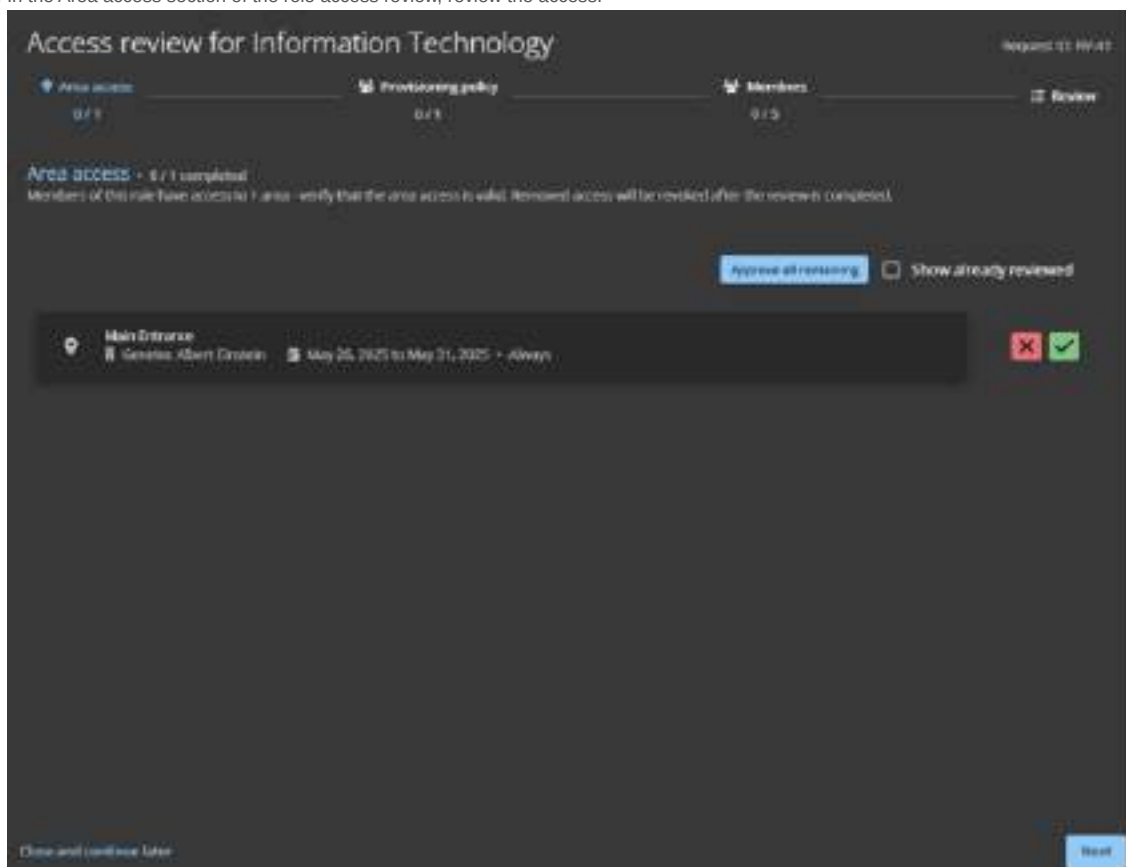
Type	Name	Description	Date updated
Information technology Role access review - 04-04	Role access	Genetec Main Entrance	17 Nov 2024
Controlled access Engineering Role access review - 04-04	Role access	Genetec Main Entrance	17 Nov 2024
Role access Information technology - 04-04	Information	Genetec Main Entrance	17 Nov 2024
Information technology Role access review	Role access	Genetec Main Entrance	16 Nov 2024

Create Role

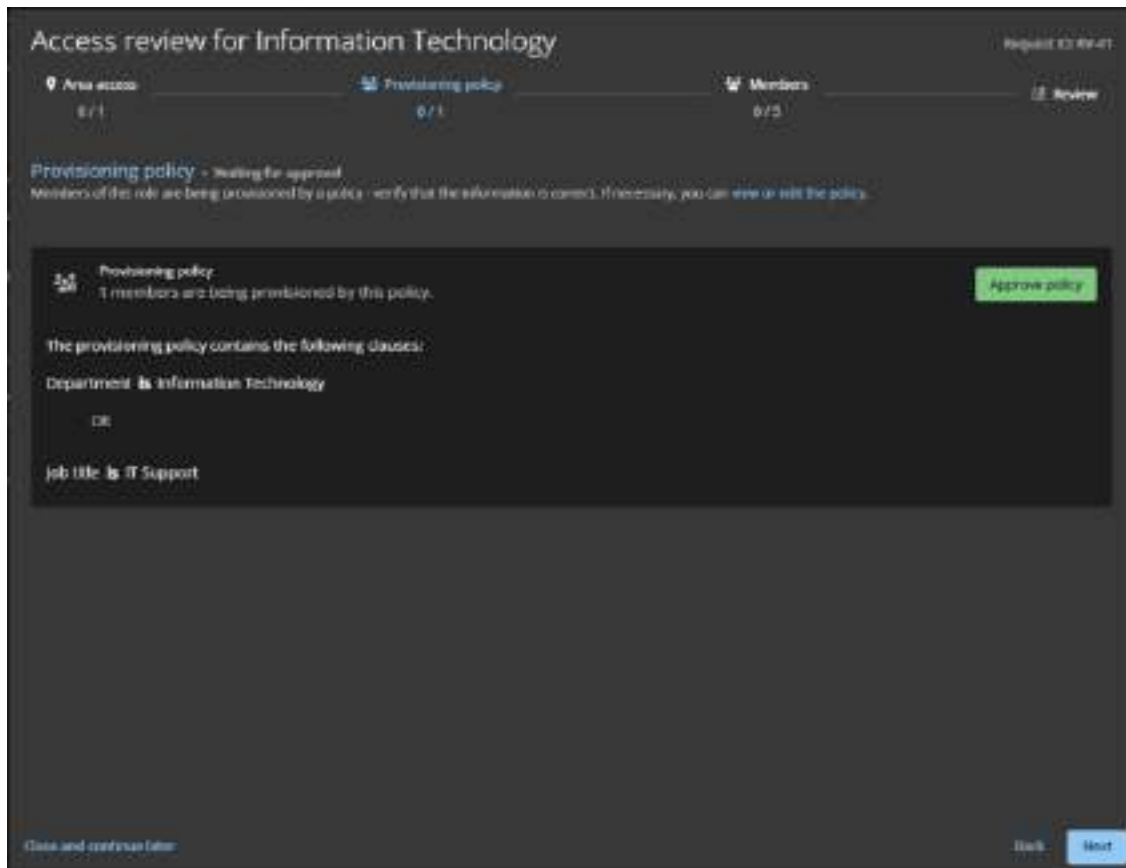
- In the Details section of the role access review, review the summary details.



- a. Click  to see the reviewer details.
 - b. (Optional) Click Close and continue later to pause the review for a later time.
 - c. Click Next to continue to the next section of the access review wizard.
4. Click Continue review.
 5. In the Area access section of the role access review, review the access.

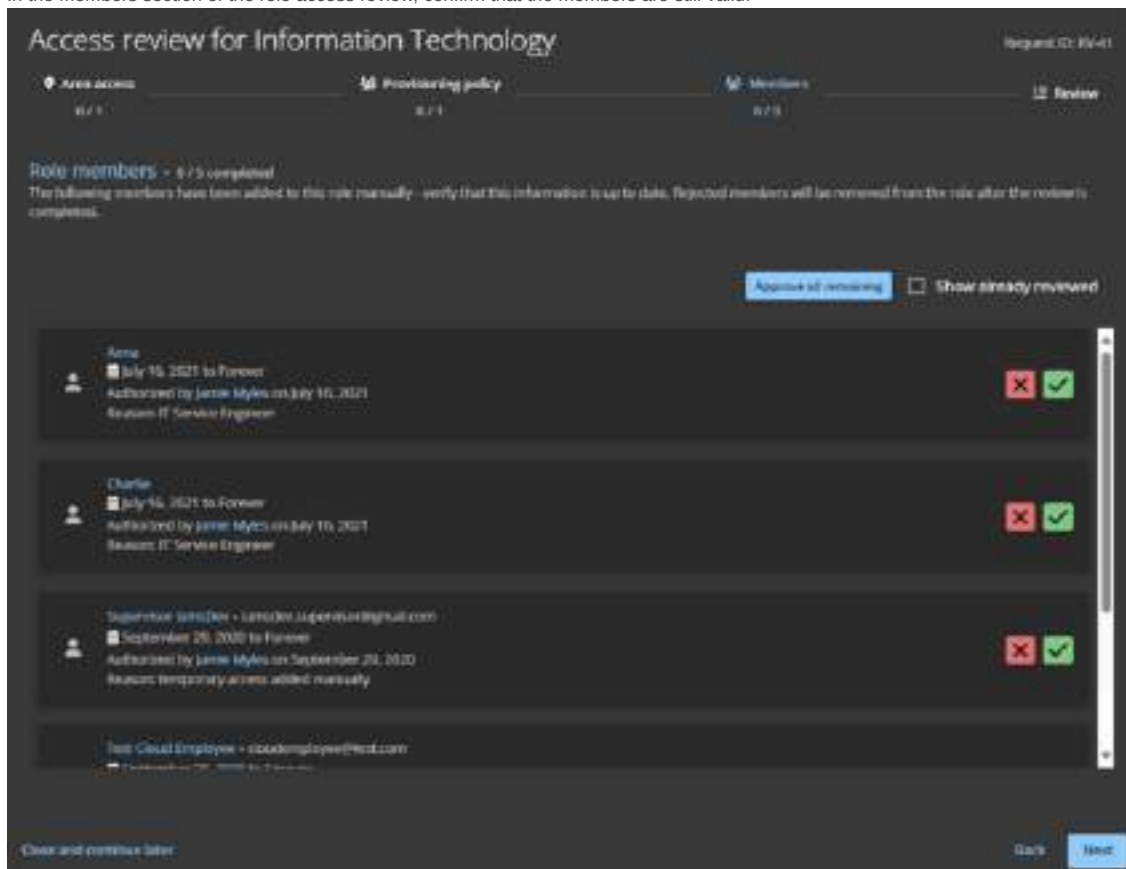


- a. Click Keep access () to confirm that access is still valid.
Tip: Use Approve all remaining to speed up approval process when the list is long, then remove any access that is no longer required.
 - b. Click Remove access () to remove access that is no longer required.
 - c. (Optional) Select Show already reviewed to go back and make modifications.
 - d. Click Next to continue to the next section of the access review wizard.
6. In the Provisioning policy section of the role access review, confirm that the policies are still valid.



- a. (Optional) Click view or edit the policy to open the Provisioning policy page to view or make changes to the policy.
- b. Click Approve policy (✓) to confirm that policy is still valid.
- c. Click Next to continue to the next section of the access review wizard.

7. In the Members section of the role access review, confirm that the members are still valid.



- a. Click Keep access (✓) to confirm that access is still valid.
Tip: Use Approve all remaining to speed up approval process when the list is long, then remove any access that is no longer required.
- b. Click Remove access (X) to remove access that is no longer required.
- c. (Optional) Select Show already reviewed to go back and make modifications.

d. Click Next to continue to the next section of the access review wizard.

8. In the Review section of the role access review, verify that the review details are correct.

Access review for Information Technology Report ID: RW-41

Area access 1 / 1 Provisioning policy 1 / 1 Members 5 / 5 [Review](#)

Warning: No changes can be made to this access review after it is completed. Ensure that all information is up to date and valid before completing the review.

Additional notes
Enter any additional information or comments relevant to this access review. The comments or additional information are not monitored by an administrator and are for audit viewing purposes only.

Additional notes

When this access review is completed, the following changes will be made:

- Information Technology will have access revoked for 0 users.
- No changes to the role provisioning policy.
- 3 members will be removed from Information Technology.
- A report will be created for this access review, which can be found in the Reports section.

[Close and continue later](#) [Back](#) [Complete](#)

a. In the Additional notes section, add any notes that you require.

b. Before you click Complete, review the changes summary immediately after the Additional notes section.

c. (Optional) If any of the information looks incorrect, click Back to return to previous sections and modify your changes.

d. If the Review section details are correct, click Complete.

After you finish

Generating an access review summary in ClearID

Browse

- [Access Reviews Feature Note \(2 pages\)](#)

7.16 | Completing an identity access review (supervisor) in ClearID

To ensure security compliance or audit readiness you can perform identity access reviews to check your direct reports areas and roles access. These periodic reviews are completed by a supervisor.

What you should know

- Supervisors can complete an identity access review from the My tasks page of the Dashboard or from an email notification.
- No changes can be made to an access review after it has been completed.
- All Completed reviews are retained for audit and tracking purposes.

Procedure

1. Click Dashboard > My tasks.
2. In the My tasks list, click the identity access review that you require.



3. Click Continue review.

4. In the Access control section, review the access control.



a. (Optional) If you want to extend the amount of time doors are unlocked (after access is granted) for cardholders with the property "extended grant time" turned on, select the Person requires extended grant time checkbox.

b. (Optional) Enter or select an Activation date MM/DD/YYYY and time HH:MM.AM for the cardholder.
If the activation fields are left blank the default current date and time are used.

c. (Optional) Enter or select an Expiration date MM/DD/YYYY and time HH:MM.AM for the cardholder.
When the expiration fields are blank, the cardholder never expires.

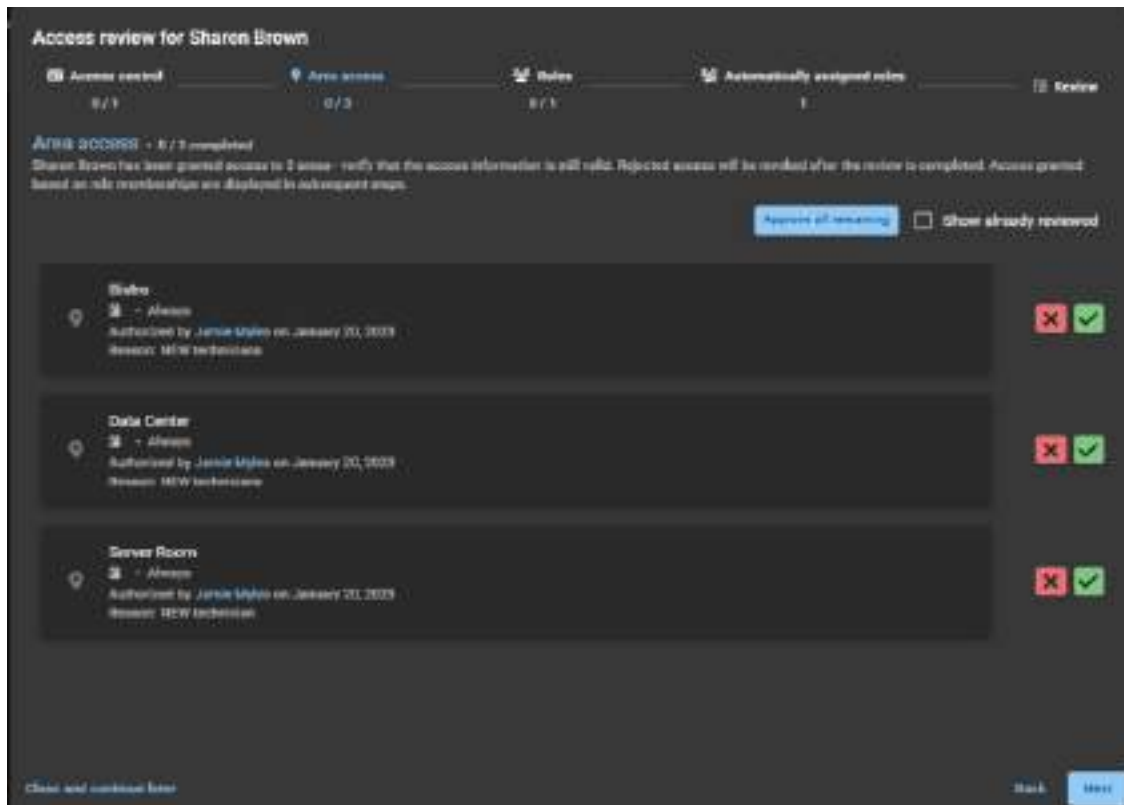
d. Click Approve to approve the access control settings.

NOTE: After an Activation date or Expiration date has been specified, you must include a time. Otherwise, the Approve button is disabled.

e. (Optional) If you change your mind about the settings, you can repeat the previous steps to make further modifications and then click Approve again.

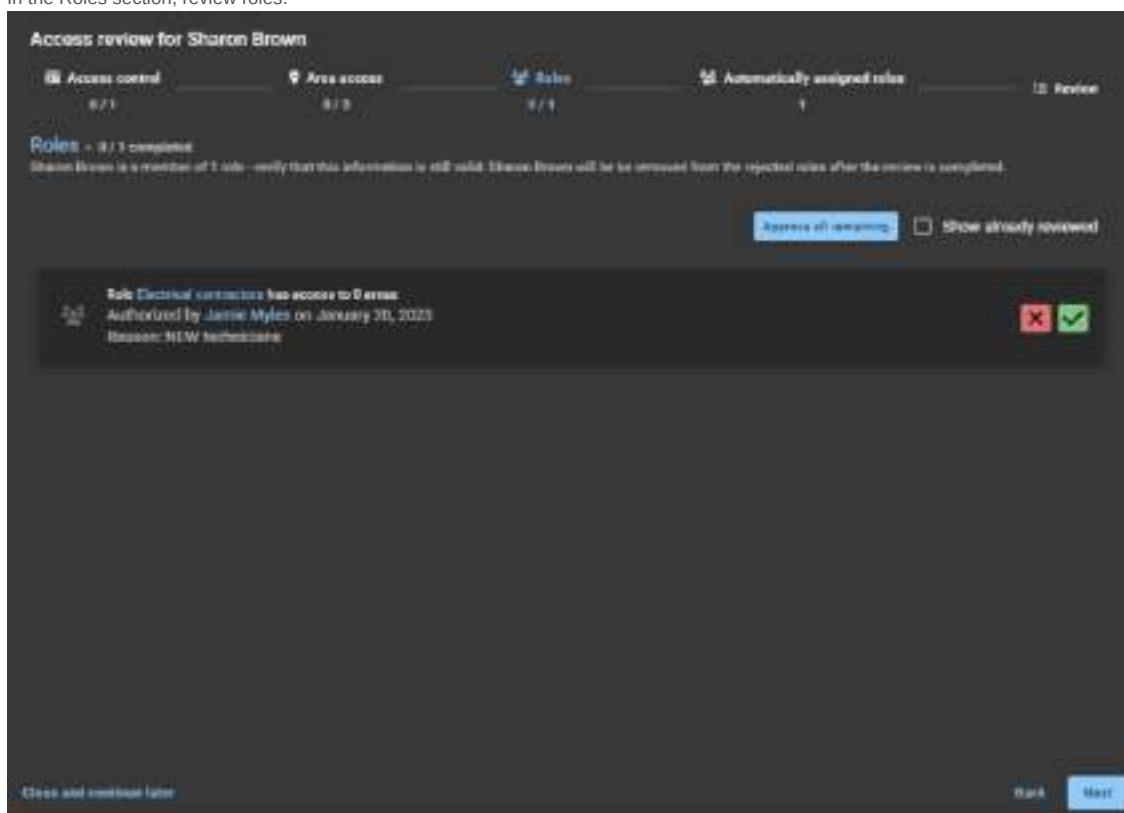
f. Click Next to continue to the next section of the access review wizard.

5. In the Area access section, review the area access.



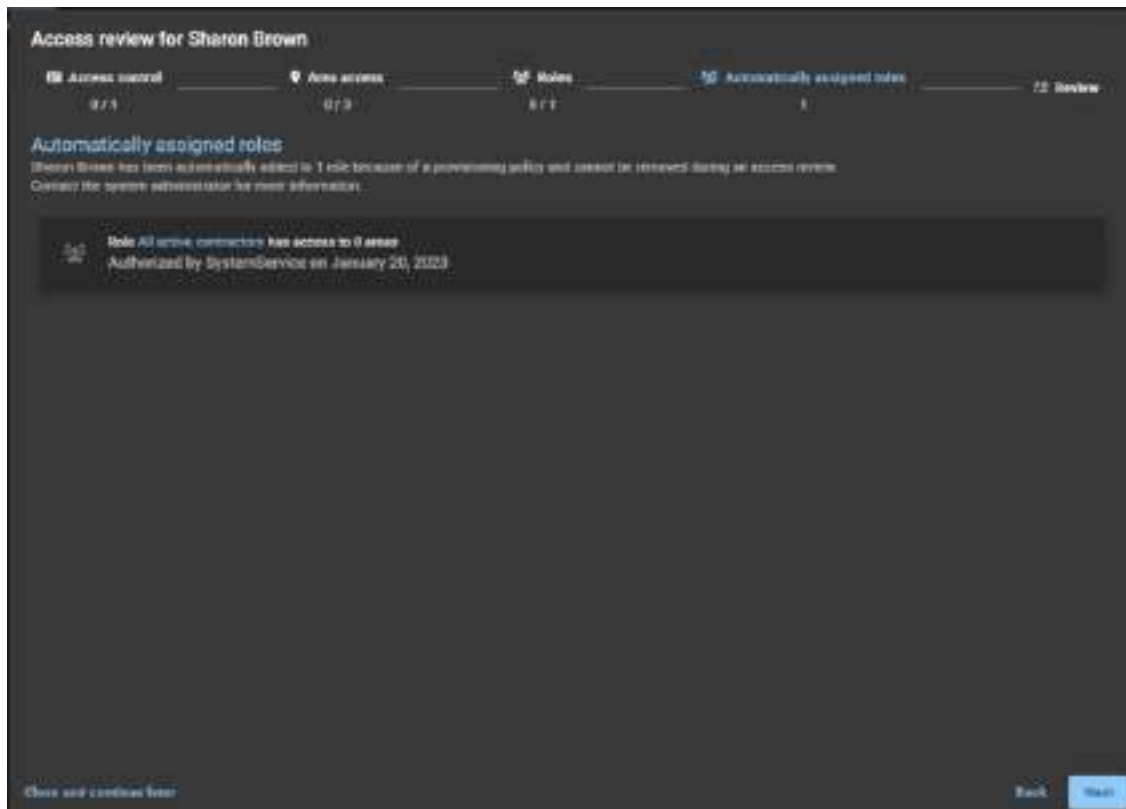
- a. Click Keep access (🟢) to confirm that access is still valid.
Tip: Use Approve all remaining to speed up approval process when the list is long, then remove any access that is no longer required.
- b. Click Remove access (🔴) to remove access that is no longer required.
- c. (Optional) Select Show already reviewed to go back and make modifications.
- d. Click Next to continue to the next section of the access review wizard.

6. In the Roles section, review roles.



- a. Verify the role information and either Keep access or Remove access as required.
- b. Click Next to continue to the next section of the access review wizard.

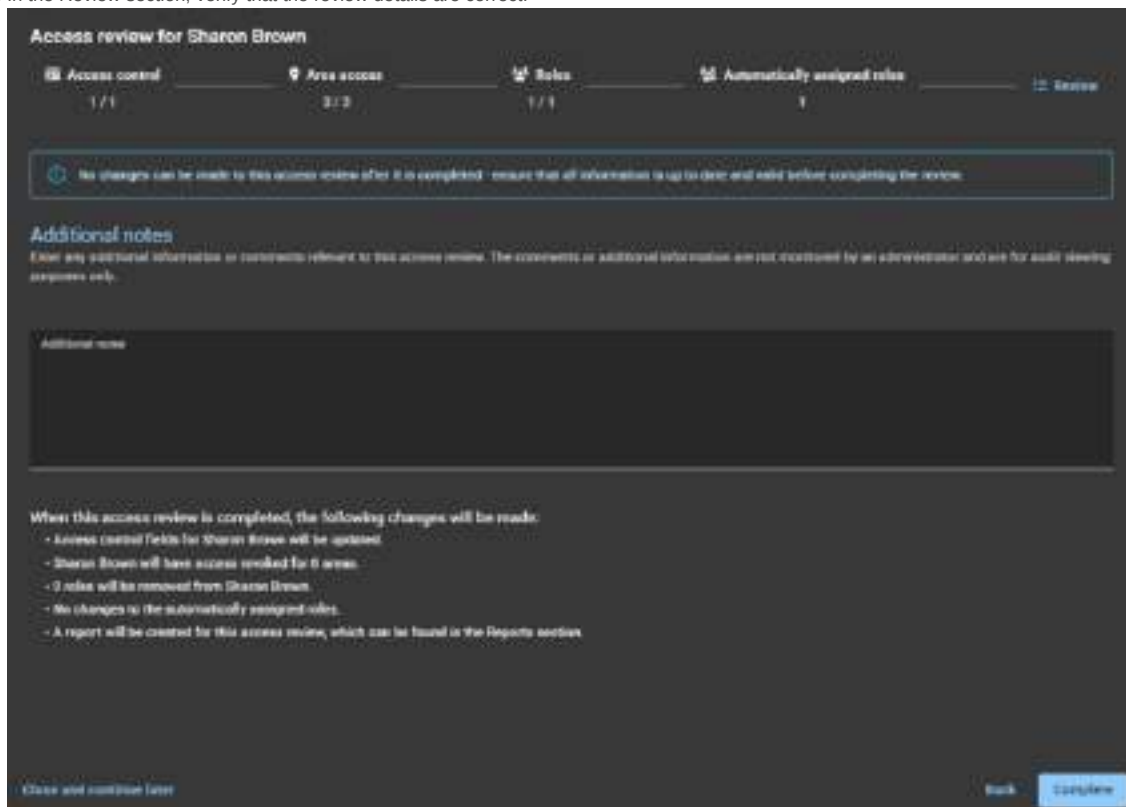
7. In the Automatically assigned roles section, review the automatically assigned roles.



The automatically assigned roles information here is useful context for a supervisor to review for accuracy and understand. It includes other access direct reports might have in addition to their manually assigned area access.

NOTE: Supervisors cannot modify any of this information because the roles were automatically assigned based on setup performed by an account administrator. If any automatically assigned roles information is no longer applicable, the account administrator should be contacted.

8. In the Review section, verify that the review details are correct.



- a. In the Additional notes section, add any notes that you require.
- b. Before you click Complete, review the changes summary immediately after the Additional notes section.
- c. (Optional) If any of the information looks incorrect, click Back to return to previous sections and modify your changes.
- d. If the Review section details are correct, click Complete.

9. Repeat this process as required for each identity listed in your My tasks dashboard inbox.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Generating an access review summary in ClearID

7.17 | Generating an access review summary in ClearID

You can generate an access review summary for any completed access review to share with an auditor or other members of your organization.

Before you begin

Complete your access reviews.

What you should know

You can only generate an access review summary for a single completed access review.

Procedure

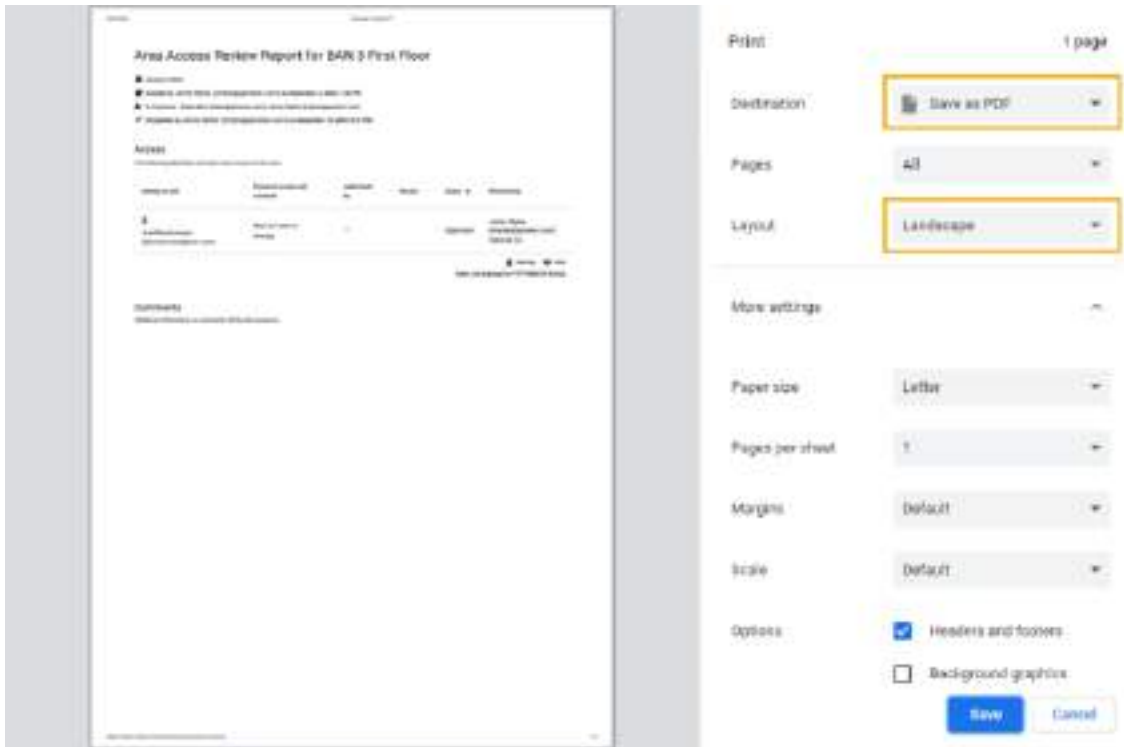
1. From the Home page, click Reports > Access reviews.
2. Configure report column filters to narrow report results as required.
 - a. Click the Status filter and select Completed.
 - b. In the Review item column, click the review item for the *completed* access review that you require.
3. Click Print.

NOTE: The layout Portrait option and the Background graphics checkbox option are not supported.

4. In the Print section, select an option from the Destination list.

Typically the report is either sent to a printer for a hardcopy output, or saved as a PDF so that it can be sent to auditors or shared by email. Other destination options are also available.

Best Practice: In the Layout list, select Landscape for the best viewing experience.



IMPORTANT: The options displayed in the Print dialog vary depending on your browser, your local computer and attached peripherals, and your organizations setup.

- (Optional) In the More settings section, select the Headers and footers option if you want to include the Date and the report Filename in the heading of the report.
- If you selected a printer, click Print and follow the on-screen prompts.
- If you selected Save as PDF, click Save and follow the on-screen prompts.

Tip: Use a file name that makes your access review reports easy to find during an audit or organization review. Include all useful information: area, role or group, and date. For example, Data Center - Access Review July 2020, Server Room - Access Review August 2020, or IT Department - Access Review Sept 2020. The default file name is <Area or Role name> - Access Review YYYY-MM-DD.pdf.

Results

Your report has now been printed or saved as a PDF for reference later.

After you finish

You can now share the access review report with an auditor or other members of your organization.

7.18 | About access requests report in ClearID

In Genetec ClearID™, an access requests report is a list of access requests for a specific site. The report includes information about the access request date, area requested, status, requested by, requested for, and period of access.

Access requests report

Access requests report

Download CSV

Display time in local +

Sanctus Head Office -

Request date	Area	Status	Requested by	Requested for	Access dates	
July 16, 2021, 3:36 PM	Server Room	Approved	Jessie	Avin	From July 16, 2021, 4:00 AM To August 1, 2021, 3:59 AM	
July 16, 2021, 7:06 PM	Server Room	Approved	Jessie	Charlie	From July 16, 2021, 4:00 AM To August 15, 2021, 3:59 AM	
July 16, 2021, 7:06 PM	2nd Floor	Waiting for approvals	Jessie	Charlie	From July 16, 2021, 4:00 AM To August 15, 2021, 3:59 AM	
December 15, 2020, 9:24 PM	2nd Floor	Canceled	Jessie	Test Cloud Employee	From December 15, 2020, 9:00 AM To January 1, 2021, 4:59 AM	
December 15, 2020, 9:24 PM	Server Room	Approved	Jessie	Test Cloud Employee	From December 15, 2020, 9:00 AM To January 1, 2021, 4:59 AM	
December 15, 2020, 8:07 PM	2nd Floor	Approved	Jessie	Charlie	From December 15, 2020, 8:00 AM To January 1, 2021, 4:59 AM	

1-17 of 17 total results

The access requests report is used by *area owners* and *site owners* to check the status of all access requests for a specific site and all the associated areas. The report can also be used to provide access request information to auditors.

Filters can be used to help refine the report search results by request date, area, status, requested by, requested for, and period of access. Browse

- [Checking the status of access requests in ClearID](#)

7.19 | Checking the status of access requests in ClearID

As *Area owners* and *Site owners* you can check the status of access requests at the site level for areas associated with a specific site. Using the Access request report, you can ensure that the organization is security-compliant, audit ready, and that the requests are processed in a timely fashion.

Before you begin

You must be an *Area owner* or *Site owner* to view the Access requests report and check the status or progress of access requests.

Procedure

1. From the Dashboard, click Reports > Access requests.
Tip: You can filter the results to suit different requirements. For example, to look for overdue requests, you can filter for Waiting for approvals in the Status column.

Request date	Area	Status	Requested by	Requested for	Access dates
July 16, 2021, 3:36 PM	Server Room	Approved	Janice	Anne	From July 16, 2021, 4:00 AM To August 1, 2021, 3:59 AM
July 16, 2021, 7:06 PM	Server Room	Approved	Janice	Charlie	From July 16, 2021, 4:00 AM To August 15, 2021, 3:59 AM
July 16, 2021, 7:06 PM	2nd Floor	Waiting for approvals	Janice	Charlie	From July 16, 2021, 4:00 AM To August 15, 2021, 3:59 AM
December 15, 2020, 9:24 PM	2nd Floor	Canceled	Janice	Test Cloud Employee	From December 15, 2020, 9:00 AM To January 1, 2021, 4:59 AM
December 15, 2020, 9:24 PM	Server Room	Approved	Janice	Test Cloud Employee	From December 15, 2020, 9:00 AM To January 1, 2021, 4:59 AM
December 16, 2020, 8:07 PM	2nd Floor	Approved	Janice	Charlie	From December 15, 2020, 9:00 AM To January 1, 2021, 4:59 AM

- In the Access requests report page, select the required display time format. Choose one of the following:

Display time in local

Show report times using the system time from the computer of the logged-in user.

Display time in UTC

Show report times using Coordinated Universal Time (UTC).

Display time in site time zone

Show report times using the time zone of the site.

- From the sites list, select the site for which you want to review access requests.
- In the Request date column, select one of the options, or click Date range and specify a date and time range to display a list of access reviews.
 - If you selected Date range, use the calendar picker to select the date range that you require.
NOTE: The time period for request date is limited to a maximum of 1 year.
 - (Optional) To sort the report results by Request date in ascending () or descending () order, click .
- In the Area column, click  to filter the results by area name.
 - Search for an area or select one or more check boxes to filter the results by the areas that you require.
 - Click the Area name hyperlink to display and verify the area details.

Tip: To revoke an access request, click the Area name hyperlink in the report, then click Access and click  next to a user.
- In the Status column, click  to filter the results by status.
 - Select one or more check boxes to filter the results by the statuses that you require (Submitted, Waiting for approvals, Denied, Approved, Canceled, or Completed).
 - (Optional) Click the Status hyperlink to display the access request.
NOTE: If you're an approver, you can Approve or Deny the pending access request while viewing the request.
- In the Requested by column, click  to filter the results by access requester.
 - Enter a user name or email address in the search field.
 - (Optional) Click the Requested by hyperlink to display summary details about the requester.
- In the Requested for column, click  to filter the results by access recipient.
 - Select one of the following:

All
Displays all identity and role access requests.

An identity
Select An identity, then enter an identity in the search field when you want to filter access requests for a specific identity.

A role
Select A role, then enter a role in the search field when you want to filter access requests for a specific role.
 - (Optional) Click the Requested for hyperlink to display summary details about the recipient.
- In the Period of access column, click  to filter the results using a date range.
- Click Download CSV, to download a copy of the access requests report in CSV format. The report can then be used for auditing purposes, to keep a physical copy, to attach to an audit request, to review offline, or to manipulate or consolidate data in a spreadsheet for other audiences.
 - Follow your browser prompts to complete downloading the exported file.

Genetec ClearID® User Guide

Displayed in the header

The file is exported as a .CSV file to the default download location for your browser. By default the exported file is created using the name of your site. For example, AccessRequest_yoursitename_fromdate_to_todate.csv (AccessRequest_Genetec_Montreal_2024-09-14.csv).

NOTE: The columns and entries in the CSV file can vary depending on the filters you've selected when you download the report.

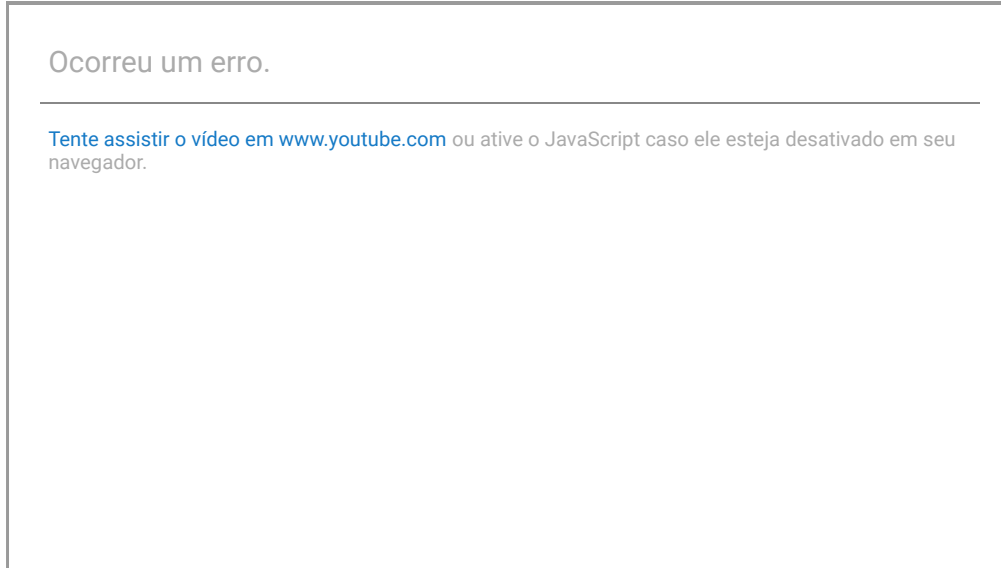
11. (Optional) Click  to reset filter selections.

Results

You have now checked the status of all access requests at a site level for all areas associated with a specified site.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.



After you finish

Approve or reject access requests as required:

- Approving area access requests in ClearID
- Rejecting area access requests in ClearID

Browse

- About access requests report in ClearID
- Requesting access in ClearID

7.20 | About site activity report in ClearID

In Genetec ClearID™, a site activity report is an audit trail of activities or events for a specific site. The report includes timestamp information, activity type, area, who activity was performed by, and a details section including reason information.

Site activity report

Site activity report

Download CSV

Display time in UTC

Genetec Head Office

Timestamp	Activity type	Area	Performed by	Details
August 13, 2021, 4:04 AM	Identity access removed	Server Room	System	Charlie has been removed from Server Room. Reason: Expired
August 1, 2021, 4:04 AM	Identity access removed	Server Room	System	Anna has been removed from Server Room. Reason: Expired
July 16, 2021, 3:38 PM	Identity access granted	Server Room	System	Anna granted access to Server Room. Reason: Contractor (highest access)
July 16, 2021, 2:06 PM	Identity access granted	Server Room	System	Charlie granted access to Server Room. Reason: System engineer requires access to Server room

1-4 of 4 total results

The site activity report is used by *site owners* to check audit trail events at a site level. The report can also be used to provide site activity information to auditors.

Filters can be used to help refine the report search results by timestamp, activity type, area, performed by, and details.

Browse

- Viewing a site activity report in ClearID

7.21 | Viewing a site activity report in ClearID

You can view a site activity report to review an audit trail of activities or events for a specific site.

Before you begin

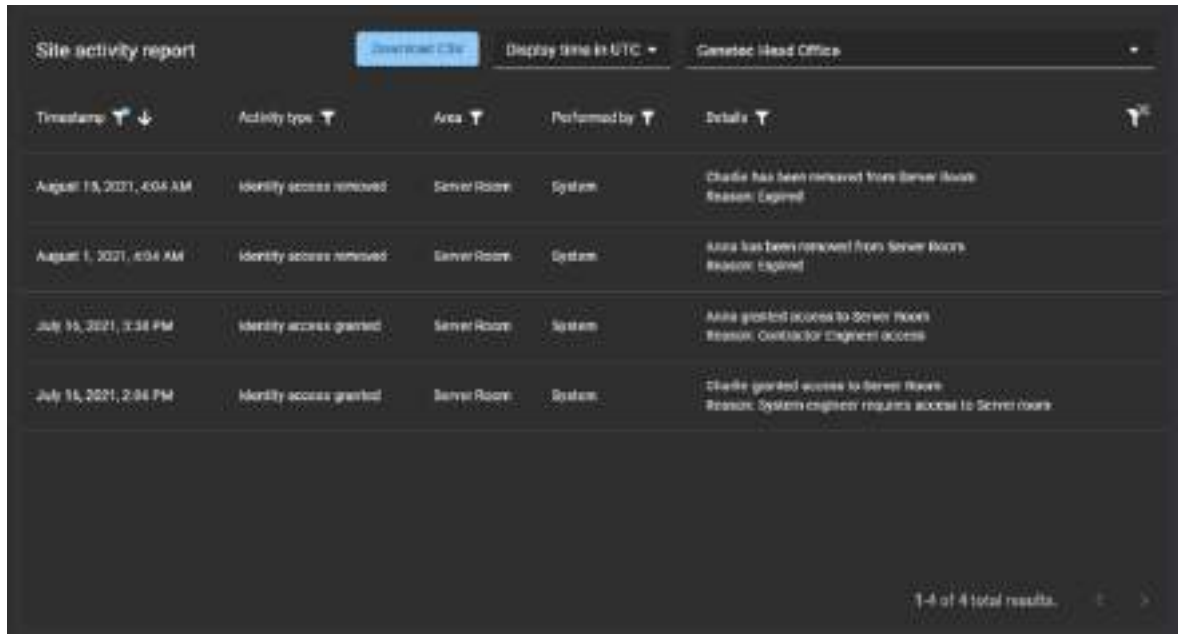
- Add area owners and managers
- Add role members
- Request access

What you should know

Only a site owner can view a Site activity report to review an audit trail of activities or events for a specific site.

Procedure

- From the homepage, click Reports > Site activity.



The screenshot shows the 'Site activity report' interface. At the top, there's a 'Download CSV' button and a 'Display time in UTC' dropdown menu. Below the header, there's a table with columns: Timestamp, Activity type, Area, Performed by, and Details. The table contains four rows of activity logs. At the bottom right, it says '1-4 of 4 total results.' with navigation arrows.

Timestamp	Activity type	Area	Performed by	Details
August 18, 2021, 4:04 AM	Identity access removed	Server Room	System	Charlie has been removed from Server Room Reason: Expired
August 1, 2021, 4:04 AM	Identity access removed	Server Room	System	Anna has been removed from Server Room Reason: Expired
July 16, 2021, 1:38 PM	Identity access granted	Server Room	System	Anna granted access to Server Room Reason: Contractor Engineer access
July 16, 2021, 2:04 PM	Identity access granted	Server Room	System	Charlie granted access to Server Room Reason: System engineer requires access to Server room

2. In the Site activity report page, select the display time that you require. Choose one of the following:

Display time in local

Report times are displayed using the system time from the computer of the logged in user.

Display time in UTC

Report times are displayed using Coordinated Universal Time (UTC).

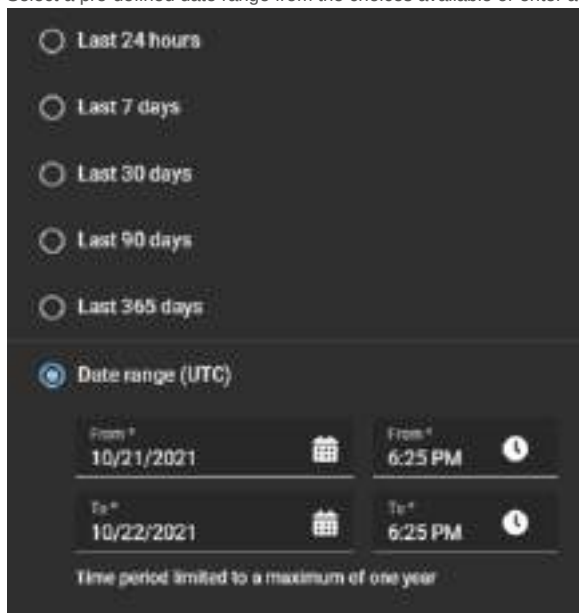
Display time in site time zone

Report times are displayed using the time zone of the site.

3. From the sites list, select the site that you require.

4. In the Timestamp column, click  to filter the results by date.

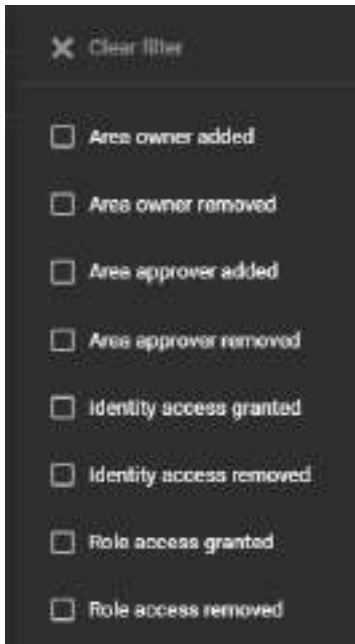
- a. Select a pre-defined date range from the choices available or enter a specific date range using the date range picker.



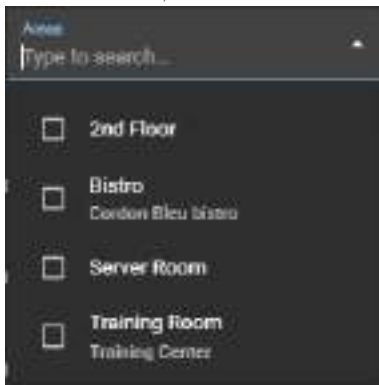
The screenshot shows a date range picker with radio buttons for 'Last 24 hours', 'Last 7 days', 'Last 30 days', 'Last 90 days', 'Last 365 days', and 'Date range (UTC)'. The 'Date range (UTC)' option is selected. Below it, there are two date pickers: 'From' with date '10/21/2021' and 'To' with date '10/22/2021'. There are also time pickers for 'From' and 'To' both set to '6:25 PM'. A note at the bottom says 'Time period limited to a maximum of one year'.

- b. (Optional) Use the sort icons ( and ) to display the results in descending or ascending order.

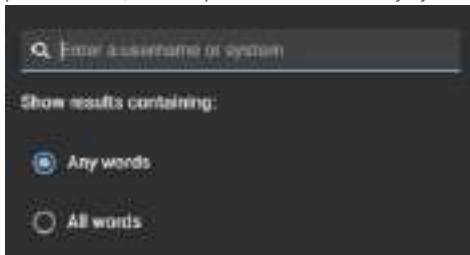
5. In the Activity type column, click  to filter the results by activity type.



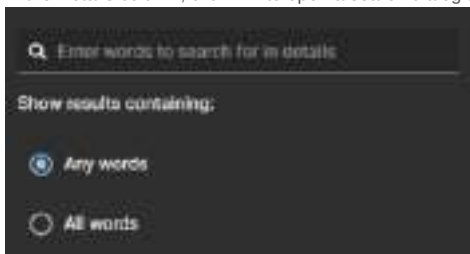
6. In the Area column, click  to filter the results by area.



7. In the Performed by column, click  to open a search dialog and filter the results by who performed an activity. For example, tasks performed by a particular user, or tasks performed automatically by the system.



8. In the Details column, click  to open a search dialog to search the details or reason using a search criteria.



9. Click Download CSV, to download a copy of the site activity report in CSV format. The report can then be used for auditing purposes, to keep a physical copy, to attach to an audit request, to review offline, or to manipulate or consolidate data in a spreadsheet for other audiences.

a. Follow your browser prompts to complete downloading the exported file.

The file is exported as a .CSV file to the default download location for your browser. By default the exported file is created using the name of your site. For example, *yoursitename_fromdate_to_todate_SiteActivityReport.csv* (Genetec Head Office_from_2020-10-22_to_2021-10-22_SiteActivityReport.csv).

NOTE: The columns and entries in the CSV file can vary depending on the filters you have selected when you download the report.

10. (Optional) Click  to reset filter selections.

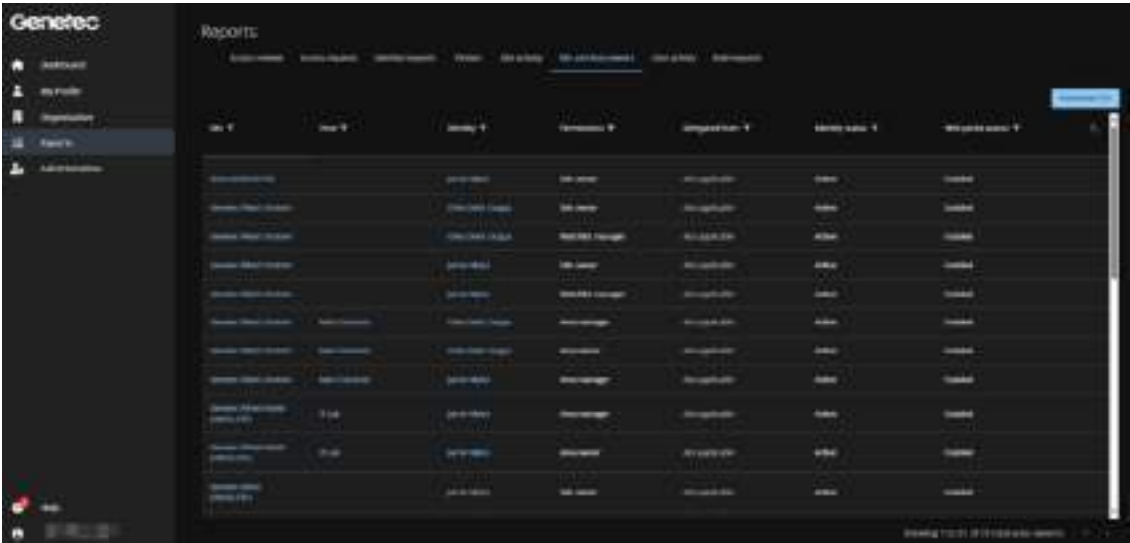
Browse

- About site activity report in ClearID

7.22 | About site and area owners report in ClearID

In Genetec ClearID™, a site and area owners report is a list that provides a global view of the following identities and their permissions: site owner, area manager, area owner, and watchlist manager. The report includes site, area, identity, identity permission, delegated from, identity status, and web portal access information.

Site and area owners report



The site and area owners report is used by account administrators to get a global view of all identities and their permissions. When the report is used by a site owner, only information about their own sites is shown.

Filters can be used to help refine the report search results by site, area, identity, permissions, delegated from, identity status, and web portal access.

Browse

- Viewing a site and area owners report in ClearID

7.23 | Viewing a site and area owners report in ClearID

You can view a site and area owners report to get a global view of all identities and their permissions.

Before you begin

Ensure that you have assigned identities for the following:

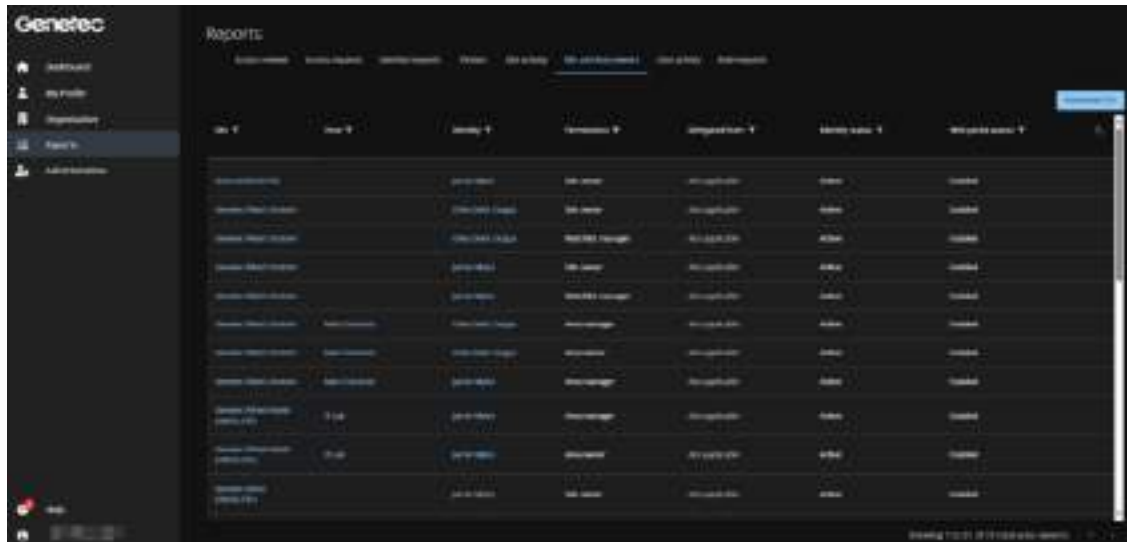
- Site owners
- Area owners and managers
- Watchlist managers

What you should know

Only an account administrator or site owner can view a Site and area owners report to review all identities and their permissions. When the report is used by a site owner, only information about their own sites is shown.

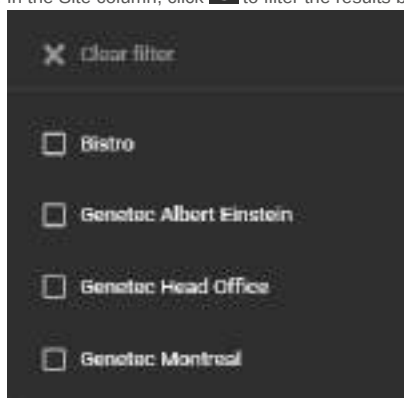
Procedure

1. From the homepage, click Reports > Site and Area owners report.

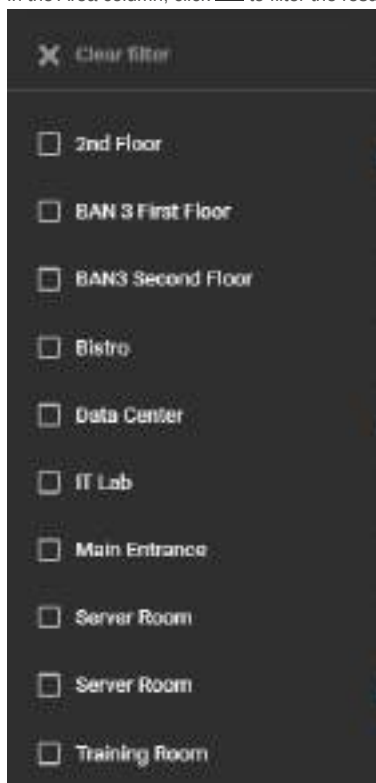


2. In the Site and area owners report page, select the filters that you require.

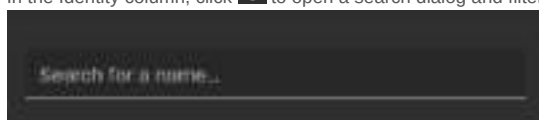
a. In the Site column, click  to filter the results by site.



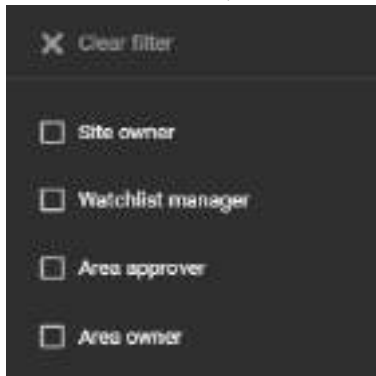
b. In the Area column, click  to filter the results by area.



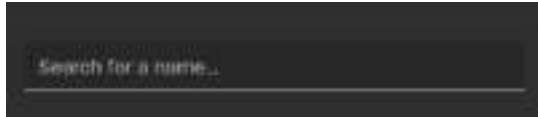
c. In the Identity column, click  to open a search dialog and filter the results by an identity.



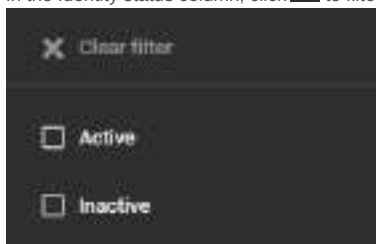
- d. In the Permissions column, click  to filter the results by permission type.



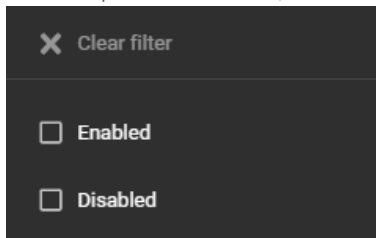
- e. In the Delegated from column, click  to open a search dialog and filter the results by a person delegating tasks.



- f. In the Identity status column, click  to filter the results by identity status.



- g. In the Web portal access column, click  to filter the results by web portal access.



3. Click Download CSV, to download a copy of the site and area owners report in CSV format. This report format can be used for auditing purposes, to keep a physical copy, to attach to an audit request, to review offline, or to manipulate or consolidate data in a spreadsheet for other audiences.

- a. Follow your browser prompts to complete downloading the exported file.

The file is exported as a .CSV file to the default download location for your browser. By default the exported file is created using the report name and download date. For example, SiteAreaOwners_2022-02-14.csv.

NOTE: The columns and entries in the CSV file can vary depending on the filters you have selected when you download the report.

4. (Optional) Click  to reset filter selections.

Browse

- [About site and area owners report in ClearID](#)

8 | Managing areas

8.1 | About areas in ClearID

In Genetec ClearID™, an area is a logical entity that defines the relationship between Synergis™ doors and area owners. Areas are managed by the area owner.

Doors are not managed in Genetec ClearID™, doors are managed in Security Center:

- Managing doors from ClearID is impractical due to the distance from the hardware.
- A door must be properly configured in Security Center and linked to the hardware physically managing the door.
- After areas are created in ClearID and synchronized in Security Center, doors can then be added to those areas in Security Center.
NOTE: Doors moved under areas inherit the access rules of the area.
- Door setup is performed in Security Center separately from the areas. After both *doors* and *areas* are present in Security Center, doors must be added to areas.

Browse

- [Adding doors to areas in ClearID](#)

8.2 | Creating areas in ClearID

In Genetec ClearID™, an area is a logical entity that defines the relationship between Synergis™ doors and area owners. Areas are managed by the area owner.

Before you begin

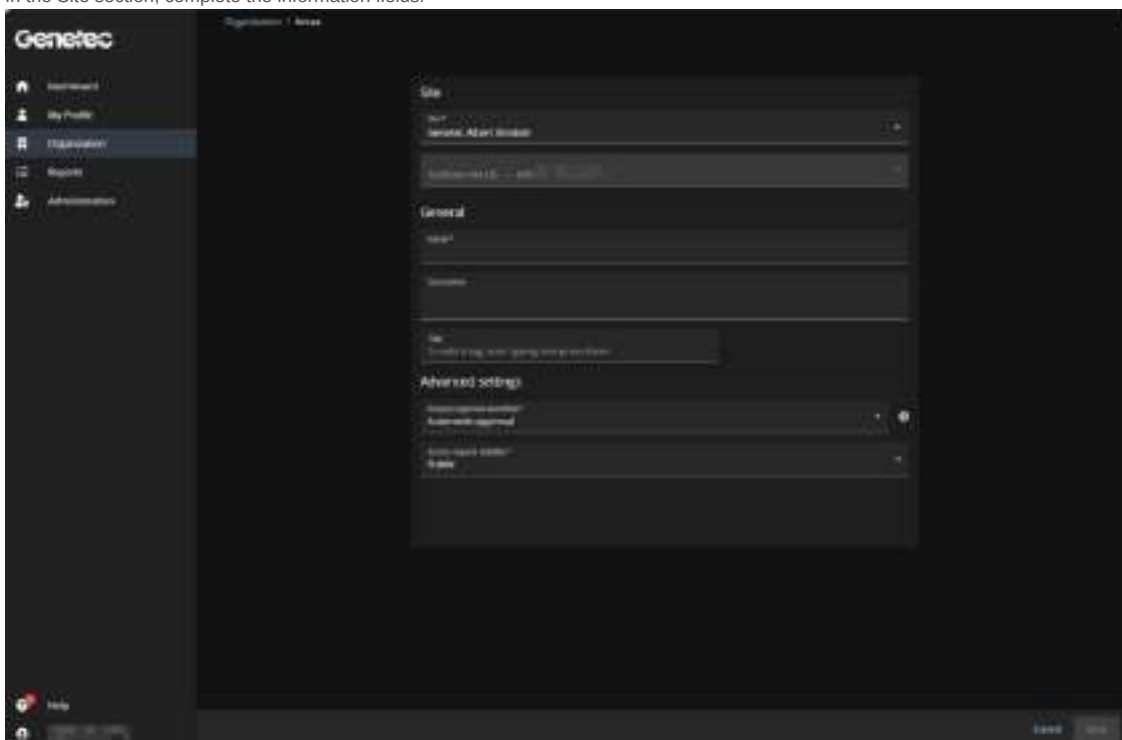
- [Create your sites.](#)

What you should know

- Only account administrators or *site owners* can create areas in Genetec ClearID™.
- In Genetec ClearID™, an area owner is an identity with authority over an area. The owner can define the policy for an area, assign area managers, give or remove access, and approve or deny access requests for an area.
- An *area* is bound to or associated with a Security Center system.

Procedure

1. Click Organization > Areas.
2. Click Create area.
NOTE: Mandatory fields are highlighted in the user interface with an asterisk (*).
3. In the Site section, complete the information fields:



Site

From the Site list, select the site that you want to associate your area with.

Access control system

This field is prefilled based on the previously selected site. This access control system is used to synchronize changes in ClearID back to Security Center.

NOTE: If a warning message is displayed instead of the associated ACS information, click the link to return to the site configuration and enter the associated ACS information.

- a. In the General settings section, complete the information fields:

Name

Enter an area name.

Description

Enter a description that indicates the geographical location of the building or physical area.

Tags

Enter alternative keywords or search term categorizations that might be used to find the area.

- b. In the Advanced settings section, select the options that you require:

Request approval workflow

Choose the approval workflow option that you require:

Automatic approval

Area requests are automatically approved using a role-based policy.

Area managers

Area requests are manually approved by authorized area managers.

Role managers or supervisor and area managers

Area requests for roles are manually approved by role managers, and requests for identities are manually approved by supervisors. Then, requests are manually approved by authorized area managers.

Role managers or supervisors

Area requests for roles are manually approved by role managers, and requests for identities are manually approved by supervisors.

Visibility

Choose the visibility option that you require:

Public

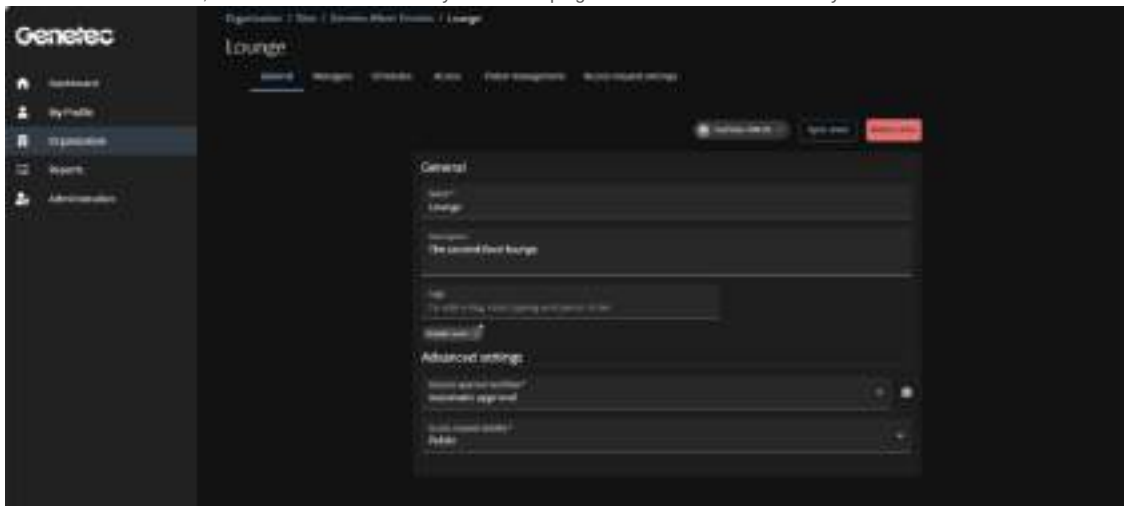
The area is visible to everyone and access requests can be created for the area. This is the default setting.

Private

The area is private and should be hidden, and access requests are not supported for the area.

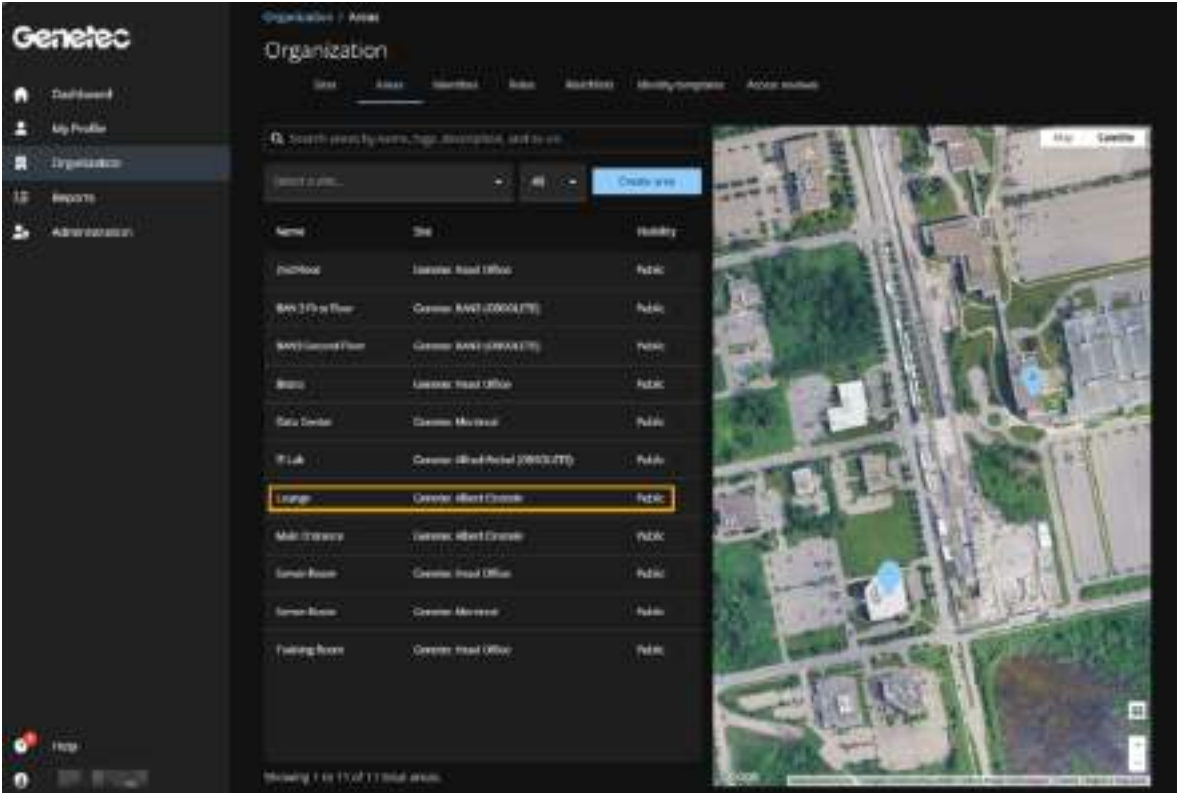
4. Click Save.

When the area is saved, commands are automatically sent to the plugin to create an area in Security Center.



Results

Your area has now been created in ClearID.



Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Add area managers.

8.2.1 | Adding doors to areas in ClearID

Before you can submit access requests or invite visitors, you must add the doors in your areas to the associated areas that were automatically created in Security Center by Genetec ClearID™.

Before you begin

Create your areas.

What you should know

- Only Config Tool users with the *View door properties* privilege can add doors to areas in Security Center that are associated with areas in ClearID.
- When an area is created in ClearID, areas are automatically created in Security Center.
- Doors must then be added to the associated areas that are automatically created in Security Center.

Doors that are members of an area can be configured as *Captive* or *Perimeter* doors:

- Perimeter doors are used to enter and exit an area, and help to control access.
- Captive doors are used within an area.

Set the *door sides* correctly to ensure that *People counting* and *antipassback* are properly tracked. A door's *Entrance* and *Exit* sides are relative to the area being configured.

Procedure

1. From the Config Tool homepage, open the Area view task.
2. Select an area and then click the Properties tab.
3. In the Doors section, click Add an item () and select the doors that you want to link to your area.
4. For all doors in the Doors section, configure the door type:
 - If the door is used to enter or exit the area, set the slider to Perimeter.
 - If the door is located inside the area, set the slider to Captive.

NOTE: If a smaller area is nested inside a larger area, you do not need to add the perimeter doors of the smaller area as captive doors of the larger area. The system automatically organizes nested areas when calculating people counts and applying antipassback rules.

 - To swap the door sides, select the door and click Swap door side.
5. Click Apply.

Results

Your doors are now added to the areas in Security Center that are associated with ClearID areas.

After you finish

In ClearID, you can now [submit access requests](#) or [invite visitors](#).

Parent topic: [Creating areas in ClearID](#)

Browse

- [About areas in ClearID](#)

8.2.2 | Enabling visitor management for areas in ClearID

Before visitors can request an area visit, you must configure the visitor management settings for your area.

Before you begin

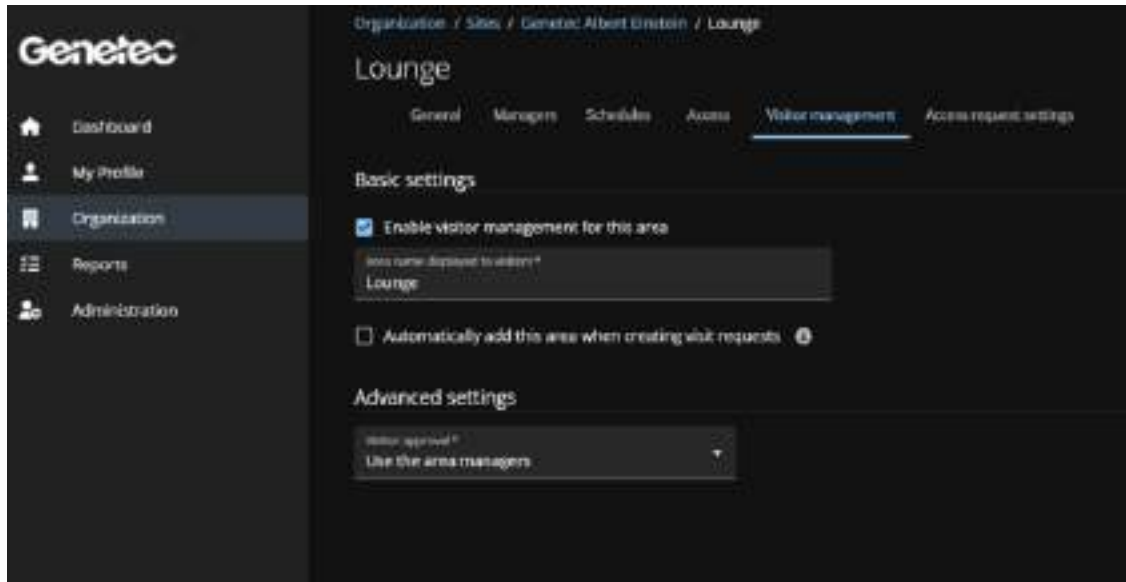
[Create your areas.](#)

What you should know

- Visitor management for areas is off by default.
- Only *area owners* or a *site owners* can enable visitor management for areas in Genetec ClearID™.
- The options displayed when a visit request is created vary depending on the users requesting access and also the settings that you configure here.

Procedure

1. Click Organization > Areas.
2. From the Areas list, select an area.
3. Under the Visitor management tab, configure the following options:



Basic settings

Select the Enable visitor management for this area option to enable visitor management for this area.

Area name displayed to visitors

Enter the area name that you want displayed in email notifications sent to visitors.

Automatically add this area when creating visit requests

If you select this option, all guests in your visit request are automatically granted access to the requested area.

Advanced settings

If you want to define guest access in your visit request, then specify the required approvers:

Visitor approval

Choose the approvers for visitor access from the following options:

Automatically approve visitors

Automatically approve access requests for this area.

Use the area managers

Only area managers can approve or deny access requests for this area.

Define visit approvers

Only people in the Visit approvers list can approve or deny access requests for this area.

4. Click Save.

Results

Visitor management is enabled for the area.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Access requests or visit requests can now be submitted for this area.

Parent topic: Creating areas in ClearID

Browse

- About workflows in ClearID

8.2.3 | About nested areas in Security Center

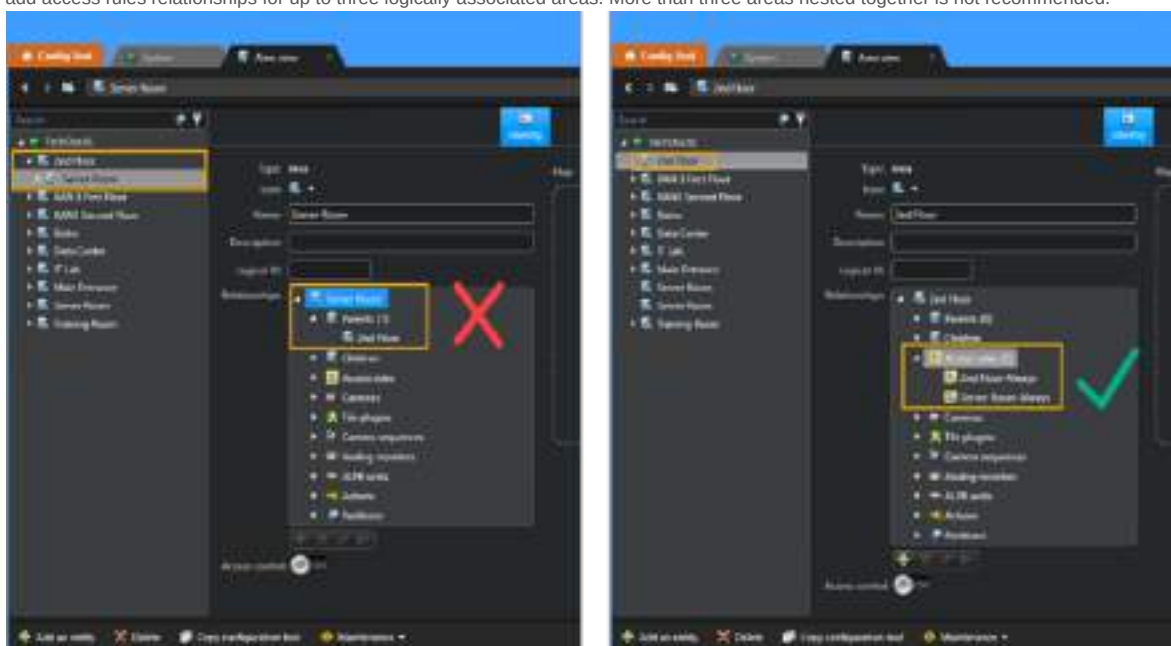
In Security Center, nested areas can be used to logically group areas so that access can be automatically granted to people for associated nested areas when access is requested in Genetec ClearID™ for one of the nested areas.

Nested areas are useful for organizations with lots of restricted areas, lots of logical grouping, or area dependencies. For example, when secure areas require access to other areas to get to the secure area:

- Example 1: Requesting access to a server room might automatically grant access to the floor that the server room is on.
- Example 2: Requesting access to a restricted area might automatically grant access to the floor the restricted area is on, and also grant access to the building that the floor and restricted area are in.

NOTE: In Config Tool, nesting areas using Parents or Children options in the Relationships section of the Area view does not inherit access.

Best Practice: Nest areas using Access rules options in the Relationships section of the Area view to inherit the required access. You can create nested areas to add access rules relationships for up to three logically associated areas. More than three areas nested together is not recommended.



Adding multiple access rules to an area creates the logical group association for nested areas. This relationship association ensures that the areas automatically grant access to the other associated areas when access is requested for one of the nested areas. By default ClearID automatically creates access rules for each schedule that is added to an area.

IMPORTANT: If the schedules for any of the nested areas change, the area relationships (access rules) must be configured again.

Parent topic: [Creating areas in ClearID](#)

Browse

- [Granting access to areas in Security Center automatically](#)

8.2.4 | Granting access to areas in Security Center automatically

To automatically grant access for people to logically grouped areas, you can create nested areas for Genetec ClearID™ in Security Center.

Before you begin

- [Create the areas that you require.](#)
- [Learn about nested areas.](#)
- Plan the logical grouping of your areas before configuring your nested areas to automatically grant or inherit access.

What you should know

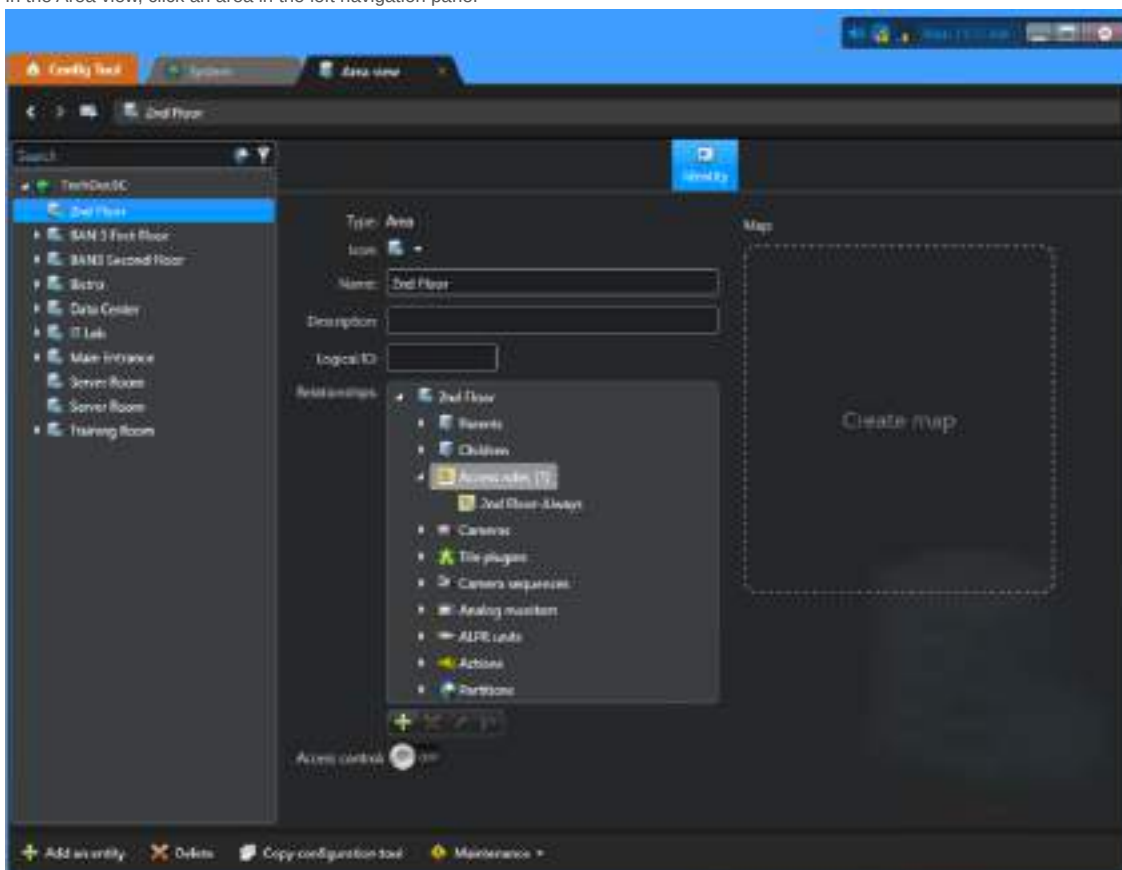
Only a Security Center administrator or system integrator can configure or map the nested areas.

If the schedules for any of the nested areas change, the area relationships (access rules) must be configured again.

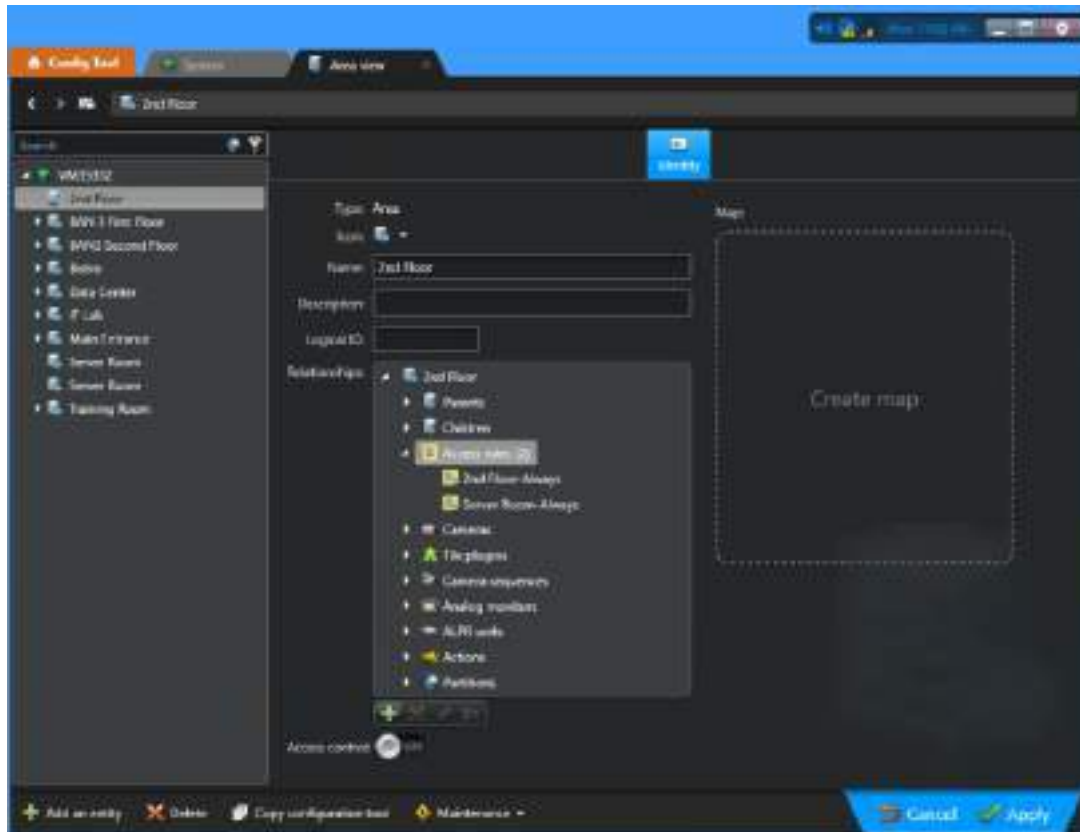
Best Practice: Nest areas using Access rules options in the Relationships section of the Area view to inherit the required access. You can create nested areas to add access rules relationships for up to three logically associated areas. More than three areas nested together is not recommended.

Procedure

1. From the Config Tool homepage, open the Area view task.
2. In the Area view, click an area in the left navigation pane.



3. In the Identity tab Relationships section, double-click Access rules.
 - a. Click Insert an item  then search for and select the *access rules* that contain the required schedules for the *areas* that you want to associate with the area selected earlier in step 2.



Tip: You can also click Entity type and select the Access rule checkbox, then click Search to only display access rules in the entity list.

b. (Optional) Repeat for other areas.

4. Click Apply.

When an access request is received for an area that is part of a group of areas, access is automatically granted based on the relationships defined for the areas. In the previous example, anyone who has access to the Server Room is also automatically granted access to the 2nd floor.

Parent topic: [Creating areas in ClearID](#)

8.3 | Adding area owners and managers in ClearID

Before you can define policies for an area, assign area managers, or approve or deny access requests for an area, you must add your area owners and managers.

Before you begin

Create your areas.

What you should know

- Only *area owners* or *site owners* can add area owners and managers in Genetec ClearID™.
- In Genetec ClearID™, an area owner is an identity with authority over an area. The owner can define the policy for an area, assign area managers, give or remove access, and approve or deny access requests for an area.
- In Genetec ClearID™, an area manager is an identity with approval authority over an area. The manager can give or remove access and approve or deny access requests for an area. They are also responsible for approving area access reviews.

Procedure

1. Click Organization > Areas.
2. From the Areas list, select an area.
3. Click Managers.
4. Use the Search field or click Add managers to add an area owner or manager.
5. Select the required user or users and click Confirm.
6. Select the Role type for the user or users you added:
 - Manager
 - Owner
 - Both



7. Click Save.

Results

The selected people are added to the area as an owner, a manager, or both.

After you finish

[Adding schedules to an area in ClearID.](#)

8.4 | Adding schedules to an area in ClearID

Before you can grant people access to an area, you must add schedules to your areas.

Before you begin

Define schedules in Security Center. For more information, see [Creating schedules](#).

What you should know

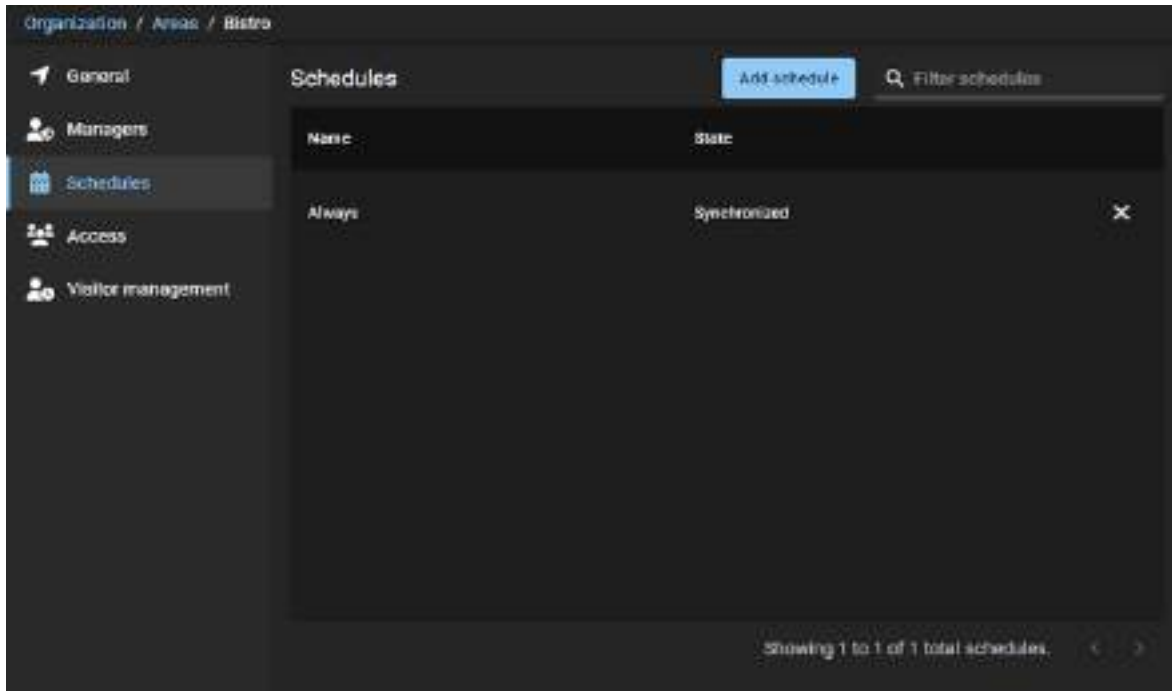
- Only *area owners* can add schedules to an area in Genetec ClearID™.
- A schedule is an entity that defines a set of time constraints that can be applied to a multitude of situations in the system. Each time constraint is defined by a date coverage (daily, weekly, ordinal, or specific) and a time coverage (all day, fixed range, daytime, and nighttime).
- The schedules that are available for selection vary depending on the schedules defined in the Security Center access control system that is selected when you create your area.
- Some schedule examples include: Always, Weekdays, Weekend, 09:00-17:00, and so on.
- When a schedule is added to an area, an *access rule* is automatically created in Security Center. The *area-schedule* access rule defines the schedule that is associated with the area. ClearID automatically adds and removes access for a *cardholder* or *cardholder group* listed in the access rule based on the schedule specified in ClearID.

Procedure

1. Click Organization > Areas.
2. From the Areas list, select an area.
3. Click Schedules.
4. Click Add schedule to configure your area schedule.
 - a. Enter a search term and click Search (🔍).
 - b. Select a schedule from the list and click Confirm.
This list only shows schedules that are not already in your Schedules list.
 - c. (Optional) Repeat previous substeps to add additional schedules.
5. (Optional) Click Remove (✖) to remove any schedules that are no longer required.
6. Click Save.

Results

Your schedules have been added to the area.



After you finish

Grant access to your area.

8.5 | Configuring access request documents for areas in ClearID

For areas with extra security measures or requirements, *Site owners* and *Area owners* can make it mandatory for employees to upload supporting documents like copies of drivers licenses or certifications when requesting access to areas.

Before you begin

Familiarize yourself with [access request workflows](#).

What you should know

- As a *Site owner*, you can manage supporting document requirements for site-level access requests.
- Site or area owners can configure more supporting document requirements at the area level.
- You can configure up to 20 supporting document types per area.

Procedure

1. In the Genetec ClearID™ web portal, click Organization > Site > Area > Access request settings.
2. (*Site owner*) Under Supporting document settings from site, select the radio button to choose whether or not the specific area inherits supporting document requirements configured at the site level:

Include site documents

Access requests use the supporting documents for the area in addition to any existing supporting document settings specified for the site.

Exclude site documents

Access requests only use the supporting documents for the area, excluding the supporting document settings for the site.

NOTE: Include site documents is selected by default for areas. *Site owners* can change these settings.

3. Under Define supporting documents for area, click Add area document.

Access request documents

Supporting document settings from site

Select supporting document settings to inherit from the site for this area.

☒ **Include site documents**
Access requests will only use the supporting documents for this area in addition to any existing supporting document settings specified for the site.

☐ **Exclude site documents**
Access requests will use the supporting documents for this area only, excluding the supporting document settings for the site.

Define supporting documents for area

[Add area document](#)

Configure the following supporting document fields. These mandatory or optional supporting document fields are displayed to users when submitting access requests.

	Certificate of qualification Required • Enabled	
	Driver's license Required • Enabled	
	Work permit Required • Enabled	

- In the Display name field, enter a name for the document type.
 - Select Show this field in access requests to display the document field in access requests.
Tip: When the checkbox is cleared, the document type remains available in draft mode.
 - Choose whether or not uploading the document is mandatory when submitting an access request by clicking the Required or Optional radio button.
- NOTE: You can configure a combination of mandatory and optional document types to appear in a single access request.

Add document field

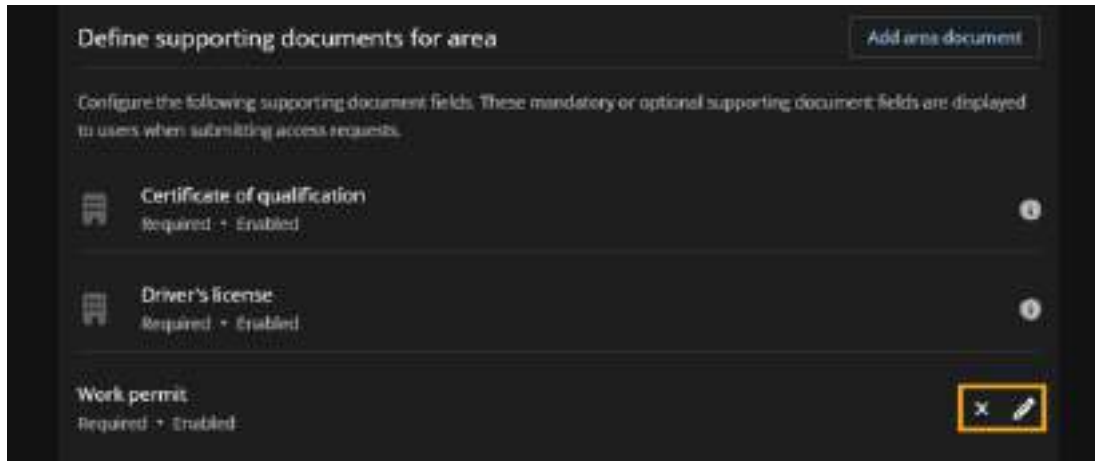
Display name*
Driver's license

☒ **Show this field in access requests**

☒ **Required** ☐ **Optional**

[Cancel](#) [Add](#)

- Click Add.
- (Optional) You can use the icons to modify or remove each document type:



- Click  to modify the configuration of a supporting document.
- Click  to remove a configured supporting document.

8.6 | Granting access to an area in ClearID

To grant people access to an area, you must add identities or roles to an area and schedule access on a person-by-person or role-by-role basis.

Before you begin

[Add schedules to your areas.](#)

What you should know

- Only *area owners*, *area managers*, and supervisors can grant people or roles access to an area.
- The Access page shows all the identities, roles, and visitors that currently have access to the area.

Procedure

- Click Organization > Areas.
- From the Areas list, select an area.
- Click Access.
- Select a filter from the following:



All

- If all the filter icons for access request type are available () , all access request types are displayed.
- If all the filter icons for access request type are unavailable () , all access request types are hidden.

Identity access ()

Show or hide identity access.

Role access ()

Show or hide role access.

Visit request ()

Show or hide visit requests.

- Click Add access.
 - In the Grant area access dialog, select either Identities or Roles.
- If you selected Identities, complete the fields:
 - Enter an identity name and click Search ().
 - Select the identity name from the Identities list.
 - Search for or select the *schedule* that you require from the Schedule list.

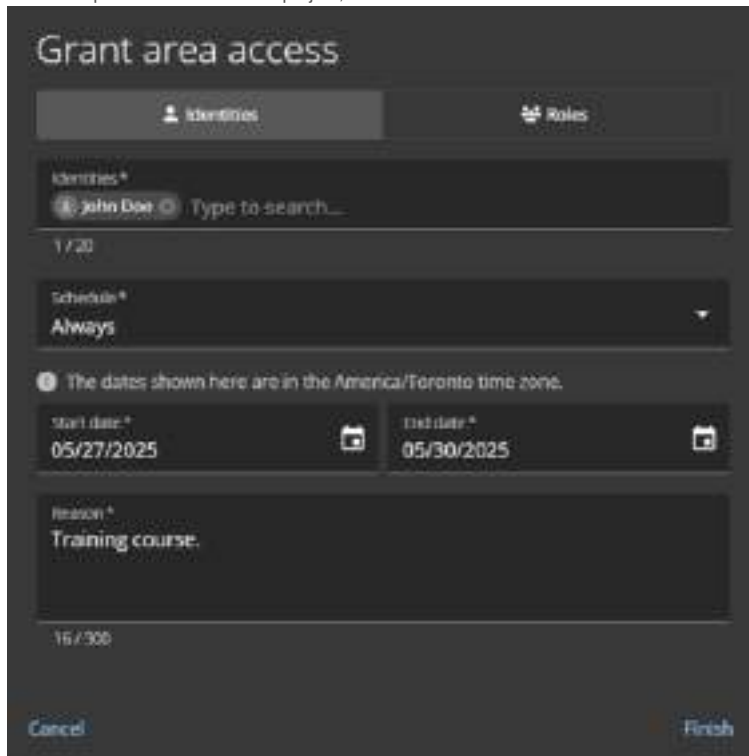
Some schedule examples include: Always, Weekdays, Weekend, 09:00-17:00, and so on.
 - Configure the period that you want the access for.

Start date
Launch a calendar picker to choose the date that the access should start. The default is Now.

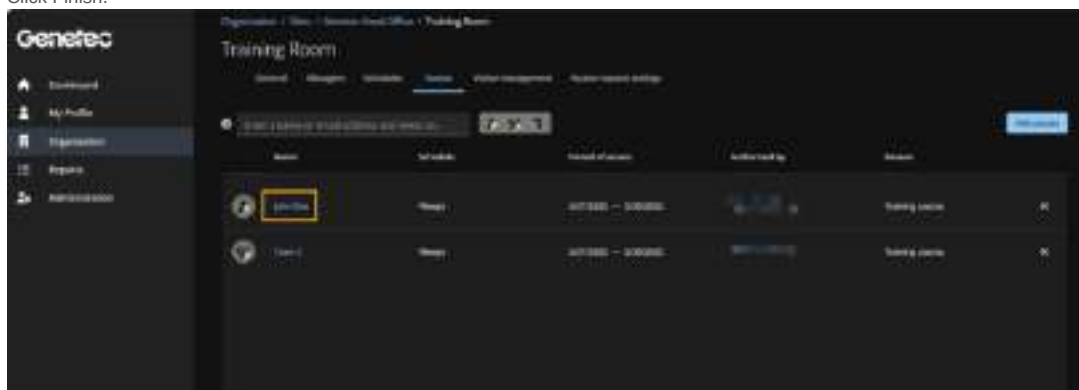
End date
Launch a calendar picker to choose the date that the access should expire. The default is Forever.

Reason

(Optional) Enter a reason for the period of access that you require. For example, access required for a business partner conference, employee access required for a multi-week project, and so on.



e. Click Finish.



7. If you selected Roles, complete the fields:

- Enter a role name and click Search (🔍).
- Select the role name from the Roles list.
- Search for or select the *schedule* that you require from the Schedule list.
- Configure the period that you want the access for.

Start date

Launch a calendar picker to choose the date that the access should start. The default is Now.

End date

Launch a calendar picker to choose the date that the access should expire. The default is Forever.

Reason

(Optional) Enter a reason for the period of access that you require. For example, access required for a business partner conference, employee access required for a multi-week project, and so on.

Grant area access

Identities Roles

Roles *

Team C Type to search...

1 / 20

Schedule *

Always

The dates shown here are in the America/Toronto time zone.

Start date: 05/27/2025

End date: 05/30/2025

Reason *

Training course.

16 / 300

Cancel Finish

e. Click Finish.

Genetec

Organization > Sites > Genetec ClearID Office > Training Room

Training Room

General Manager Schedule Access Visitor management Access request settings

16 / 300

Name	Schedule	Validity	Authorized by	Reason
John Doe	Always	05/27/2025 - 05/30/2025	John Doe	Training course
Team C	Always	05/27/2025 - 05/30/2025	Team C	Training course

8. (Optional) Click Remove (X) to revoke any access that is no longer required.

Results

Your access requests have been granted for this area.

8.7 | Reviewing area access in ClearID

To perform an audit or check who has access to an area, periodic reviews must be performed by an area owner, area manager, or site owner.

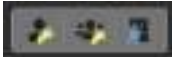
What you should know

Only *area owners*, *area managers*, and *site owners* can review area access.

This procedure describes how to verify who has access to a specified area, one area at a time.

Procedure

- 1. Click Organization > Areas.
- 2. From the Areas list, select an area.
- 3. Click Access.
- 4. Select an access request filter:



All

- If all the filter icons for access request type are available (), all access request types are displayed.
- If all the filter icons for access request type are unavailable (), all access request types are hidden.

Identity access ()

Show or hide identity access.

Role access ()

Show or hide role access.

Visit request ()

Show or hide visit requests.



5. Review the access list to identify any roles, identities, or visitors that can be removed or that require further investigation.

After you finish

Approve access requests or reject access requests.

Browse

- Setting up area access reviews in ClearID
- Completing an area access review (site owner) in ClearID

8.8 | Approving area access requests in ClearID

To approve area access requests, an *Area owner*, *Area manager*, a *Role manager*, or a *Supervisor* must review the pending approvals. They can then decide which requests to approve.

Before you begin

Ensure that some area access requests have already been submitted.

What you should know

Only *Area owners*, *Area managers*, role managers, or supervisors can approve area access requests.

Procedure

1. Click Dashboard > My tasks.

- ## Status

All

Displays all pending or completed tasks.

Pending

Displays tasks waiting for approval.

Completed

Displays completed tasks and their status. For example, approved, completed, denied, or canceled.

3. Click an access request to display additional details about the request.

Access request for John Doe
Request ID: AR-19

Requested by Jack on April 2, 2025

Waiting for approvals

From: 04/03/2025 To: 04/04/2025 Schedule: Always

Genetec Albert Einstein — Main Entrance America/Toronto

Details history

Reason for request
Access required while performing maintenance work.

Mandatory documents
This access request has 3 mandatory document placeholders.

Driver's license * Certificate of qualification * Work permit *

Close Deny Approve

4. Review the request details and make any changes that you require.
Tip: You can modify the request if the request has an error or something that needs to change. For example, you can amend the dates due to an office closure, or amend the schedule to a more appropriate access schedule.
5. (Optional) In the History field, enter a comment about any changes you make to the access request.
6. Click Approve.
7. (Optional) In the Reason for approval field, enter a reason for the access approval.
8. Click Confirm.

Results

The area access requests are now approved. Employees or visitors are able to access the area during the periods specified in their access requests.

8.9 | Rejecting area access requests in ClearID

To reject area access requests, an *Area owner*, *Area manager*, a *Role manager*, or a *Supervisor* must review the pending approvals. They can then decide which requests to deny.

Before you begin

- Ensure that some area access requests have already been submitted.
- Review area access to identify access that is no longer required.

What you should know

Only *area owners*, *area managers*, role managers, or supervisors can reject area access requests.

Procedure

1. Click Dashboard > My tasks.

- Status**
Select a status from the following:
All
Displays all pending or completed tasks.

Displays tasks waiting for approval.

Displays completed tasks and their status. For example, approved, completed, denied, or canceled.

- Displayed in the footer
Page 247 of 473

The screenshot displays the 'Access request for John Doe' interface. At the top, it shows the request ID 'AR-19' and a status 'Waiting for approvals'. Below this, there are fields for 'From' (04/03/2025) and 'To' (04/04/2025), along with a 'Schedule' dropdown set to 'Always'. The location is specified as 'Genetec Albert Einstein — Main Entrance' and the area as 'America/Toronto'. The 'Details' tab is active, showing the 'Reason for request' as 'Access required while performing maintenance work.' and 'Mandatory documents' as 'This access request has 3 mandatory document placeholders.' Below these are three document upload buttons: 'Driver's license *', 'Certificate of qualification *', and 'Work permit *'. At the bottom right, there are 'Deny' and 'Approve' buttons.

4. Review the request details.
5. (Optional) In the History field, enter a comment about any changes you make to the access request.
6. Click Deny.
7. (Optional) In the Reason for denial field, enter the reason why the access request was denied.
NOTE: If the supporting access request documents are incorrect or not valid, you can notify the requester by including this information in the Reason for denial field. The requester will then have to resubmit an access request with valid supporting documents.
8. Click Confirm

Results

The area access requests are now rejected. Employees or visitors are no longer able to access the area.

8.10 | Creating exceptions to the access request approval workflow in ClearID

In Genetec ClearID™, an access request workflow is a series of activities performed by the system or authorized people during the life cycle of an access request. To bypass the access request workflow for certain types of requests or roles, you can modify an area's access request approval workflow settings.

Before you begin

Create an area and define its access request approval workflow.

What you should know

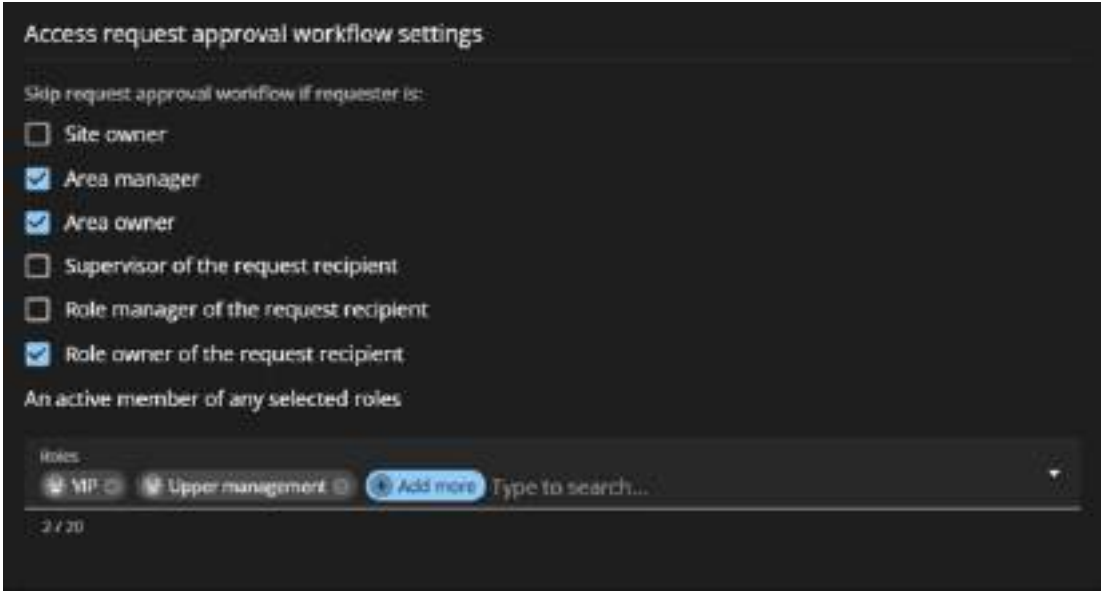
All access requests for an area must follow the steps for approval set by the chosen access request workflow. You can create exceptions to this approval process when certain users or roles make access requests.

For example, you can automatically approve access requests made for users who belong to a VIP or Upper Management role. You can also automatically approve requests if the requester is the Supervisor of the person for whom the request is made.

You must be a *Site owner* or *Area owner* to set exceptions to the access request approval workflow for an area.

Procedure

1. In the Genetec ClearID™ web portal, click Organization > Site > Area > General.
2. Under Access request approval workflow settings, define exceptions to the access request workflow set for the area as needed:
NOTE: If the request approval workflow is set to Automatic approval, the Access request approval workflow settings section is hidden.



Site owner

Automatically approve access requests when the requester is the *Site owner*.

Area manager

Automatically approve access requests when the requester is the *Area manager*.

Area owner

Automatically approve access requests when the requester is the *Area owner*.

Supervisor of the request recipient

Automatically approve access requests when the requester is the *Supervisor* of the identity that is the request recipient.

Role manager of the request recipient

Automatically approve access requests when the requester is the *Role manager* of the role for which the access request was made.

Role owner of the request recipient

Automatically approve access requests when the requester is the *Role owner* of the role for which the access request was made.

An active member of any selected role

Automatically approve access requests when the requester is a member of a listed role.

3. Click Save.

Browse

- [About workflows in ClearID](#)
- [About access request workflow in ClearID](#)

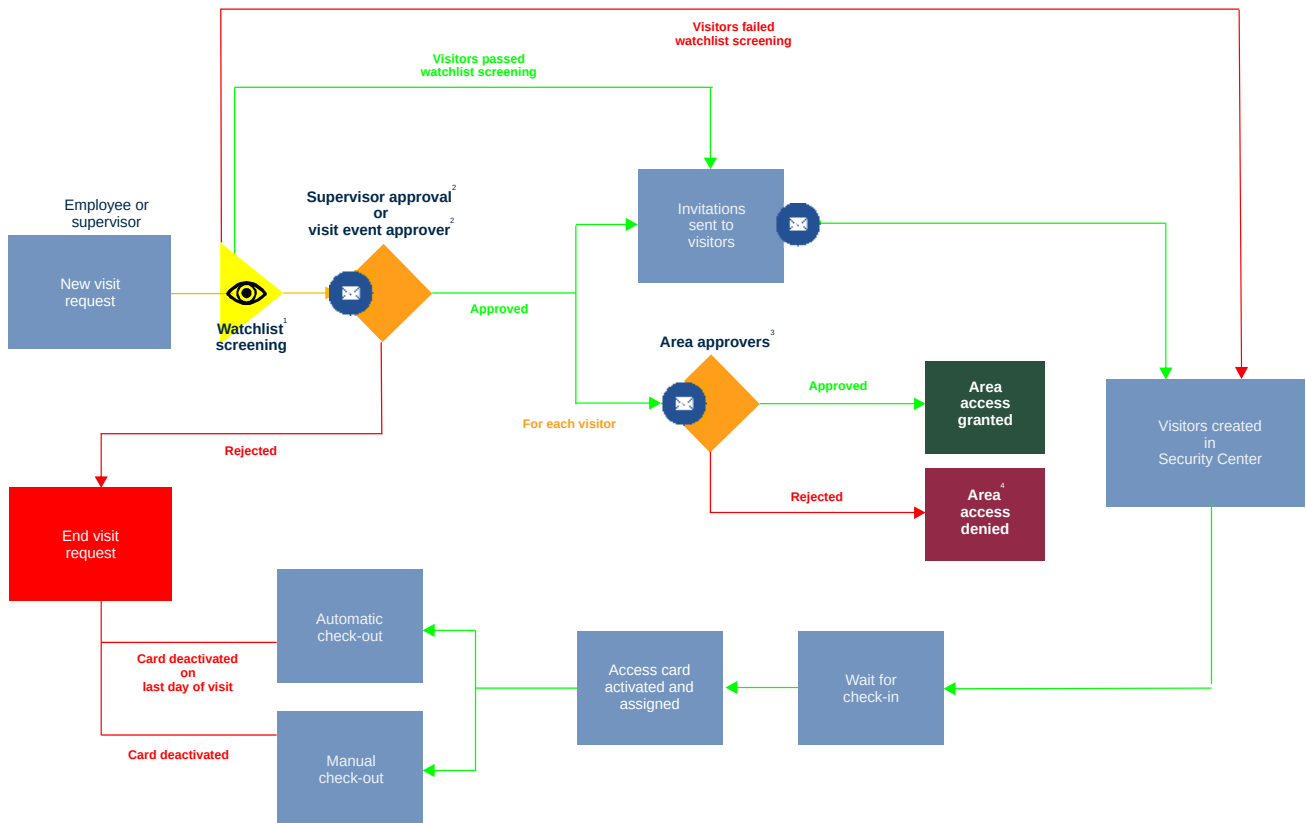
9 | Managing visitors

9.1 | About visit request workflow in ClearID

A visit request workflow is a series of activities performed by the system or authorized people during the life cycle of a visit request. The activities can change the state and properties of visit requests, affect other entities in the system, or wait for conditions to be met.

The workflow helps automate visit request tasks, such as approving or rejecting access requests, so that people involved in the review and approval process can focus on other tasks.

The following diagram illustrates the *visit request workflow* that occurs in Genetec ClearID™ and Synergis™.



¹ (Optional) For more information, see Visit request watchlist workflow.

² (Optional) Approval can be enabled or disabled for each site.

³ (Optional) Approval can be enabled or disabled for each area.

⁴ Visit event has been created and visitor has been created in Security Center but area access has been denied. Visitor might be able to access denied areas if escorted by a host, this access exception is at the discretion of the organization.

Browse

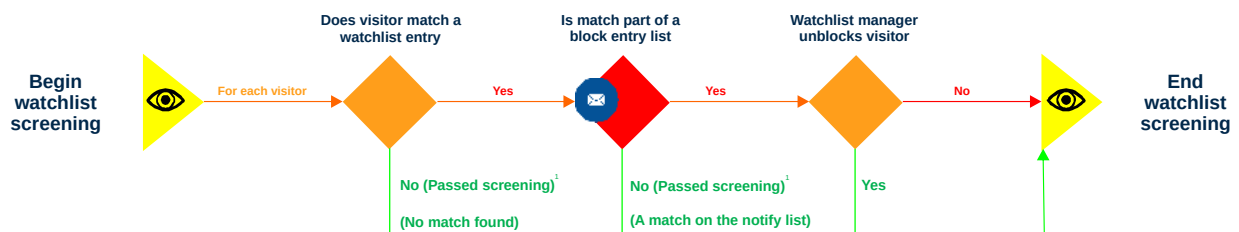
- [About workflows in ClearID](#)

9.2 | About visit request watchlist workflow in ClearID

A watchlist workflow is a series of activities performed by the system or authorized people during the life cycle of a visit request if watchlists are enabled. The activities can change the state and properties of watchlists, affect other entities in the system, or wait for conditions to be met.

The workflow helps automate screening visitors for persons or companies of interest during a self-service check-in or a self-registration, so that people involved in the review and approval process can focus on other tasks.

The following diagram illustrates the *watchlist workflow* that occurs (if the watchlist function is enabled for your account) in Genetec ClearID™ and Synergis™ in parallel with the visit request workflow.



¹ Visitor registration is only confirmed after screened visitors are not found in any block entry watchlists. Any visitors that are blocked do not receive a visit notification email.

Browse

- [About workflows in ClearID](#)

9.3 | Inviting visitors in ClearID

To invite one or more guests for a site visit or event, use the self-service portal. Using a self-service portal with area managers specified simplifies the approval process, and avoids interrupting a chain of people who might or might not be the correct approvers.

Before you begin

1. Familiarize yourself with workflows.
2. Enable visitor management for your site.
3. Ensure that you have the required permissions to invite visitors to the site.

What you should know

You can add visitors individually or import a large list of visitors using a CSV file.

- If you have fewer than five visitors to invite, add your visitors individually.
- If you have more than five visitors to invite, prepare a CSV file to import your visitor list.
- If your identity home site is configured, you are automatically granted access to invite visitors to that site only if the site visitor management options have been configured to allow people to invite visitors.
- The options displayed when creating a visitor invite can vary depending on the site settings and settings configured for visitor management.

NOTE: Mandatory fields are highlighted in the user interface with an asterisk (*).

Procedure

1. Log on to the self-service portal.
2. Do one of the following:
 - Click Dashboard > My requests > New request > Invite visitors.
 - Click Dashboard > Visits > New visit event.
3. In the New visit event wizard, follow the prompts to complete the wizard for one of the following situations:
 - Invite visitors manually
 - Invite visitors using a CSV import
4. Click Finish.

Results

Your visit request has been submitted and is waiting for the required approvals.

Example



After you finish

Confirm whether the request was approved or rejected:

- Check your email for a *Visit approved* email.
- Check My requests in Genetec ClearID™.

Browse

- [Enabling visitor management for sites in ClearID](#)

Browse

- Visitor Management Feature Note (2 pages)

9.3.1 | Inviting visitors manually in ClearID

If you have fewer than five visitors to invite to your event, you can add your visitors manually.

Before you begin

1. Familiarize yourself with workflows.
2. Enable visitor management for your site.
3. Ensure that you have the required permissions to invite visitors to the site.

What you should know

- If your identity home site is configured, you are automatically granted access to invite visitors to that site. Access is only automatically granted if the options for site visitor management have been configured to allow people to invite visitors.
- The options displayed when inviting visitors can vary depending on the site settings and settings configured for visitor management.

NOTE: Mandatory fields are highlighted in the user interface with an asterisk (*).

Procedure

1. Log on to the self-service portal.
2. Do one of the following:
 - Click Dashboard > My requests > New request > Invite visitors.
 - Click Dashboard > Visits > New visit event.
3. In the New visit event wizard, enter or select details about *where* the event will take place.

Channel Partner event at Genetec Alfred-Nobel

1 Where 2 When 3 Who 4 Details

What is the name of the event?

Name *

Channel Partner event

21 / 100

Where will this event take place?

Site *

Genetec Alfred-Nobel

Host meeting location

Main Entrance

Parking location

Alfred-Nobel

Visitors are automatically assigned default access ⓘ

Area *

IT Lab

Cancel Next

4. Enter or select details about *when* the event takes place and the purpose of the event.

Channel Partner event at Genetec Alfred-Nobel

✓ Where ② When ③ Who ④ Details

When does the visitor require access?

Remember to include any time before and after the meeting when the visitor might also require access.

ⓘ The dates and times shown here are in the UTC time zone.

Start date *	01/01/2024	Start time *	10:00 AM
End date *	01/01/2024	End time *	04:00 PM

⌚ Duration: 6 hr

What is the purpose of this event?

Visit reason *

Meeting

Cancel Back Next

Tip: Remember to include time before and after the visitor event or meeting when the visitor might also require access.

5. Enter or select details about *who* to invite to the event.

Channel Partner event at Genetec Alfred-Nobel

✓ Where ✓ When ③ Who ④ Details

Who are the visitors?

2 visitors added.

Import visitors Add visitor

John Doe	✉ john.doe@test.com	📁 Genetec ✎
Jane Doe	✉ jdoe@test.com	📁 N/A ✎

Cancel Back Next

- a. Click Add visitor and complete the fields.
 - b. Click Save.
 - c. Repeat for each additional visitor.
6. Complete *details* about the event.

Channel Partner event at Genetec Alfred-Nobel

✓ Where ✓ When ✓ Who 4 Details

Who will escort the visitors?

Name	Email	SMS alerts ⓘ
John Doe	john.doe@test.com	☒ +1 5141234567 ✕
Type to search...		

Notes for security ⓘ

Cancel Back Finish

Name

The name of the visitor event host.

Email

The email address for the visitor event host.

SMS

Enter a mobile phone number to send SMS alert notifications to visitor hosts when the visitor checks in.

- NOTE: Use the search field to add more visitor hosts. You can add up to 10 visitor hosts.

(Optional) Notes for security

Add notes about the visitor, the visit invite, or the visit event.

7. Click Finish.

Results

Your visit request has been submitted and is waiting for the required approvals.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Confirm whether the request was approved or rejected:

- Check your email for a *Visit approved* email.
- Check My requests in ClearID.

Parent topic: [Inviting visitors in ClearID](#)

Browse

- [SMS alerts in ClearID](#)
- [About email notifications in ClearID](#)

Browse

- [Visitor Management Feature Note \(2 pages\)](#)

9.3.2 | Inviting visitors using a CSV import in ClearID

If you have more than five visitors to invite to your event, you can use a CSV file import to populate your visitor list.

Before you begin

1. Familiarize yourself with workflows.
2. Enable visitor management for your site.
3. Ensure that you have the required permissions to invite visitors to the site.

What you should know

- If your identity home site is configured, you are automatically granted access to invite visitors to that site. Access is only automatically granted if the options for site visitor management have been configured to allow people to invite visitors.
- The options displayed when inviting visitors can vary depending on the site settings and settings configured for visitor management.

Tip: When you Import visitors, a sample CSV file provided by the system can be used. The columns in the sample CSV file match the settings in the site configuration. You can then complete the visitor details values in the CSV file and import all visitors in one click. For example, importing 500 people to a site visit or customer event.

NOTE: Mandatory fields are highlighted in the user interface with an asterisk (*).

Procedure

1. Log on to the self-service portal.
2. Do one of the following:
 - Click Dashboard > My requests > New request > Invite visitors.
 - Click Dashboard > Visits > New visit event.
3. In the New visit event wizard, enter or select details about *where* the event will take place.

Channel Partner event at Genetec Alfred-Nobel

1 Where 2 When 3 Who 4 Details

What is the name of the event?

Name *
Channel Partner event
21 / 100

Where will this event take place?

Site *
Genetec Alfred-Nobel

Host meeting location
Main Entrance

Parking location
Alfred-Nobel

Visitors are automatically assigned default access 1

Access *
IT Lab

Cancel Next

4. Enter or select details about *when* the event will take place and the purpose of the event.

Channel Partner event at Genetec Alfred-Nobel

1 Where 2 When 3 Who 4 Details

When does the visitor require access?
Remember to include any time before and after the meeting when the visitor might also require access.

1 The dates and times shown here are in the UTC time zone.

Start date * 01/01/2024

Start time * 10:00 AM

End date * 01/01/2024

End time * 04:00 PM

Duration 6 hr

What is the purpose of this event?

Visit reason *
Meeting

Cancel Back Next

Tip: Remember to include time before and after the visitor event or meeting when the visitor might also require access.

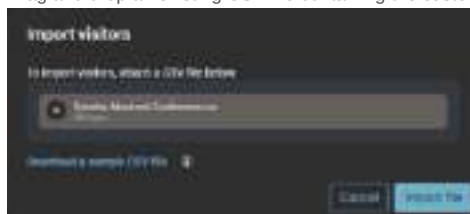
5. Prepare to import who you want to invite to the event.



- a. In the Who will attend this event? section, click Import visitors and then choose one of the following:
 - o Use an existing CSV file.
 - o Download a sample CSV file.

6. If you chose to use an existing CSV file, do the following:

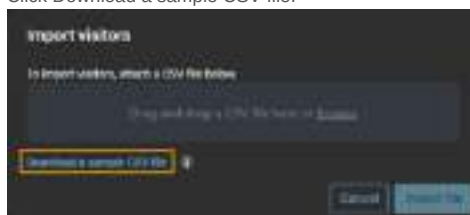
- a. Drag and drop an existing CSV file containing the customers you want to invite or click Browse to select the file you require.



- b. Click Import file to import the visitor list.
- c. Click Confirm to complete the import.
- d. (Optional) Click Edit (✎) to modify any visitor details and click Save to confirm the update.

7. If you chose Download a sample CSV file, do the following:

- a. Click Download a sample CSV file.



- b. Select and open the downloaded CSV file.
- c. For each visitor, complete a row of visitor information in the CSV template file.

ClearID CSV Template - Test										
File Home Insert Draw Page Layout Formulas Data References View Add-ins Help About Tools Tell me what you want to do										
Clipboard Font Alignment Number										
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40										
1	FirstName	LastName	Email	CompanyName	IsDisabledByAdmin	RequiresRegistration	RequiresControl	RequiresAccessAgreement		
2	Phoebe	Hegarty	rhagarty@next.com	Hegarty Inc.	TRUE		DoNotApply	NSACompleted		
3	Rand	Blanning	rlblanning@next.com	Blanning Inc.	FALSE		StreamingCompleted	DoNotApply		
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										
25										
26										
27										
28										
29										
30										
31										
32										
33										
34										
35										
36										
37										
38										
39										
40										

NOTE: The columns in the CSV template can vary depending on the settings in your site configuration.

- d. Save the visitor list as a CSV file.
- e. Return to the Import visitors dialog, to drag and drop or click Browse to select the file you created.
- f. Click Import file to import the visitor list.



g. Click Confirm to complete the import.

8. Complete *details* about the event.

Name

The name of the visitor event host.

Email

The email address for the visitor event host.

SMS

Enter a mobile phone number to send SMS alert notifications to visitor hosts when the visitor checks in.

- NOTE: Use the search field to add more visitor hosts. You can add up to 10 visitor hosts.

(Optional) Notes for security

Add notes about the visitor, the visit invite, or the visit event.

9. Click Finish.

Results

Your visit request has been submitted and is waiting for the required approvals.

Example

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Confirm whether the request was approved or rejected:

- Check your email for a *Visit approved* email.
- Check My requests in ClearID.

Parent topic: [Inviting visitors in ClearID](#)

Browse

- [SMS alerts in ClearID](#)
- [About email notifications in ClearID](#)

Browse

- [Visitor Management Feature Note \(2 pages\)](#)

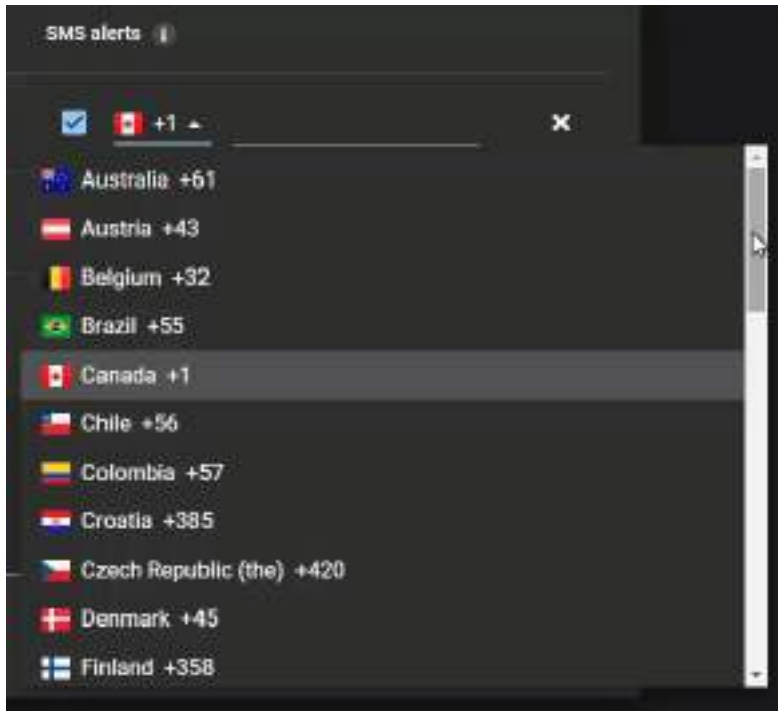
9.3.3 | SMS alerts in ClearID

In Genetec ClearID™, SMS alerts are used in the visit event wizard to automatically send notifications to visitor hosts to inform them when visitors check-in.

SMS alerts for visitor check-in are supported for the following countries:

Country	Country code
 Austria	+43
 Australia	+61
 Belgium	+32
 Brazil	+55
 Canada	+1
 Chile	+56
 Columbia	+57
 Croatia	+385
 Czech republic (the)	+420
 Denmark	+45
 Finland	+358
 France	+33
 Germany	+49

Country	Country code
 Greece	+30
 Iceland	+354
 India	+91
 Ireland	+353
 Italy	+39
 Japan	+81
 Luxembourg	+352
 Malaysia	+60
 Mexico	+52
 Monaco	+377
 Netherlands	+31
 Norway	+47
 Peru	+51
 Philippines (the)	+63
 Portugal	+351
 Romania	+40
 Singapore	+65
 Spain	+34
 Sweden	+46
 Switzerland	+41
 Taiwan (Province of China)	+886
 Thailand	+66
 United Kingdom of Great Britain and Northern Ireland (the)	+44
 United States of America (the)	+1
 Vietnam	+84



Parent topic: Inviting visitors in ClearID

Browse

- Inviting visitors manually in ClearID
- Inviting visitors using a CSV import in ClearID

9.4 | Reviewing visit events in ClearID

Area owners, security, and reception can review current or upcoming visits or events for their areas. Visits can be requested for hosting other site employees, maintenance contractors, appointments, meetings, interviews, customer visits, business partner conferences, and so on.

What you should know

Only *area owners*, security, or reception can review visits.

Procedure

1. Click Dashboard > Visits.
2. Select the options that you require.

Current and upcoming visits

Displays current and upcoming visits. By default, 10 visits are displayed and you can click Load more to display the next 10 visits.

Past visits

Displays past visits. By default, 10 past visits are displayed and you can click Load more to display the next 10 past visits. You can find past visits that occurred in the last year.

All visits

Displays all visits. By default, 10 visits are displayed and you can click Load more to display the next 10 visits.

3. (Optional) Use the column filters to refine the list of visits.

Name

In the Name field, enter your search criteria. Only search results for visits that contain the entered word in the visit name are displayed. For example, if you enter *training*, only visits with names that include the word *training* are displayed in the search results.

Status

Select a filter from the Status list to filter results for the visit request state:

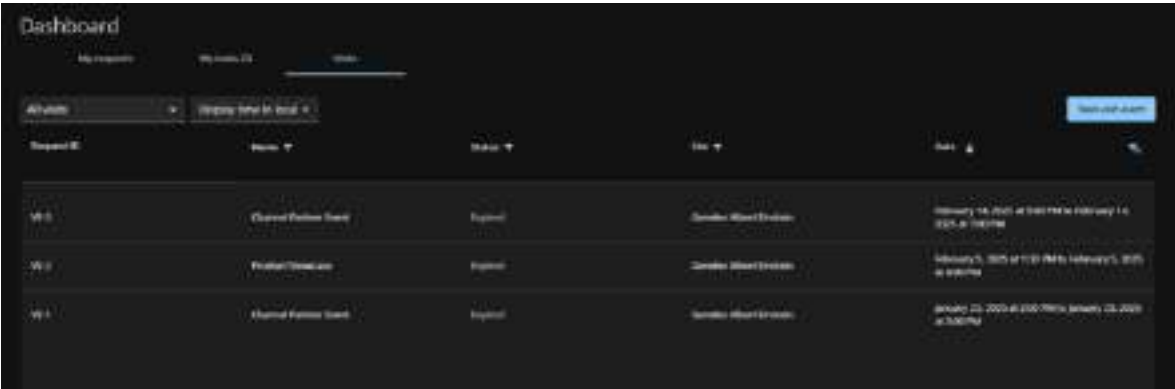
- Submitted
- Waiting for approvals
- Approved
- Canceled
- Denied
- Expired

Site
Select a site from the Site list.

Date
Sort the visits by date in ascending or descending order.

Results

The visits matching your selections are displayed.



The screenshot shows the 'Dashboard' interface with a table of visit events. The table has columns for 'Request ID', 'Event', 'Status', 'Site', and 'Date'. There are three rows of data. The first row shows a 'Request ID' of 'W-1', an 'Event' of 'Checked-Passport Scan', a 'Status' of 'Expired', a 'Site' of 'London Board Entrance', and a 'Date' range from 'January 14, 2025 at 09:00 PM to February 14, 2025 at 11:59 PM'. The second row shows a 'Request ID' of 'W-2', an 'Event' of 'Proctor/Observer', a 'Status' of 'Expired', a 'Site' of 'London Board Entrance', and a 'Date' range from 'January 5, 2025 at 11:59 PM to January 5, 2025 at 11:59 PM'. The third row shows a 'Request ID' of 'W-3', an 'Event' of 'Checked-Passport Scan', a 'Status' of 'Expired', a 'Site' of 'London Board Entrance', and a 'Date' range from 'January 23, 2025 at 00:00 PM to January 23, 2025 at 11:59 PM'.

Request ID	Event	Status	Site	Date
W-1	Checked-Passport Scan	Expired	London Board Entrance	January 14, 2025 at 09:00 PM to February 14, 2025 at 11:59 PM
W-2	Proctor/Observer	Expired	London Board Entrance	January 5, 2025 at 11:59 PM to January 5, 2025 at 11:59 PM
W-3	Checked-Passport Scan	Expired	London Board Entrance	January 23, 2025 at 00:00 PM to January 23, 2025 at 11:59 PM

After you finish

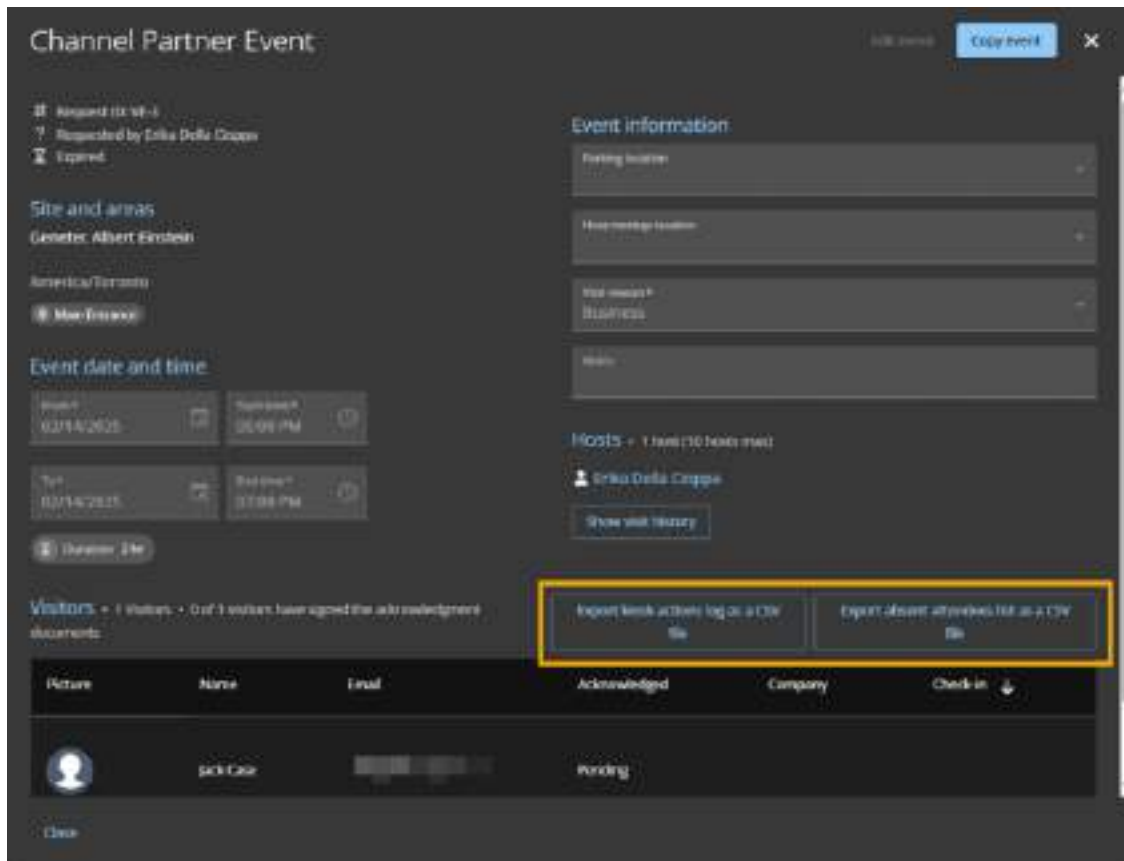
- Copy a visit event.
Browse
- About visit event logs in CearID

9.5 | About visit event logs in CearID

In Genetec ClearID™, *Account administrators*, *Site owners*, requesters, and hosts can use visit event logs to audit events and identify absentees. These logs show detailed records of operator and visitor actions on check-in devices, as well as invited guests who didn't check in.

ClearID organizes visit data into two logs:

- Kiosk actions log
- Absent attendees list



Kiosk actions log

The kiosk actions log contains information about actions performed at activated Self-Service Kiosk iPads and Mobile Operator Check-In iPhones during a visit event. Each time a device scans a visitor's QR code or a visitor checks into the visit event, an entry is entered in the log.

The exported .CSV file contains columns with identifying data for each kiosk action:

Timestamp

The time and date when the kiosk action was performed.

Action type

The type of kiosk action performed at a Self-Service Kiosk or with a Mobile Operator Check-In device. This column contains Scan when a device scans a QR code, and CheckIn when the visitor check-in process is complete.

Visit event ID

The identification number assigned to the visit event in the ClearID portal.

Visitor ID

The identification number assigned to the visitor associated with the visit event in the ClearID portal.

Visitor email

The email of the visitor associated with the visit event.

Registration code

The visitor QR code value associated with the visit event.

Device object ID

The identification number assigned to the device that performed the scan or check-in during the visit event.

Absent attendees list

The absent attendees list contains information about visitors who were invited to the event but didn't check in. The list can be used to identify absent attendees, allowing hosts to follow up as needed.

The exported .CSV file contains columns with identifying data for each absent attendee:

Visitor email

The email of the visitor flagged as an absent attendee.

Visit event name

The name assigned to the visit event.

Visitor ID

The identification number assigned to the visitor in the ClearID portal.

Visit event ID

The identification number assigned to the visit event in the ClearID portal.

Browse

- Viewing visit event logs in ClearID.
- Reviewing visit events in ClearID

9.6 | Viewing visit event logs in ClearID.

To audit operator and visitor actions on check-in devices during visit events, and review lists of absent attendees, you can export the logs of each event from the Genetec ClearID™ portal.

Before you begin

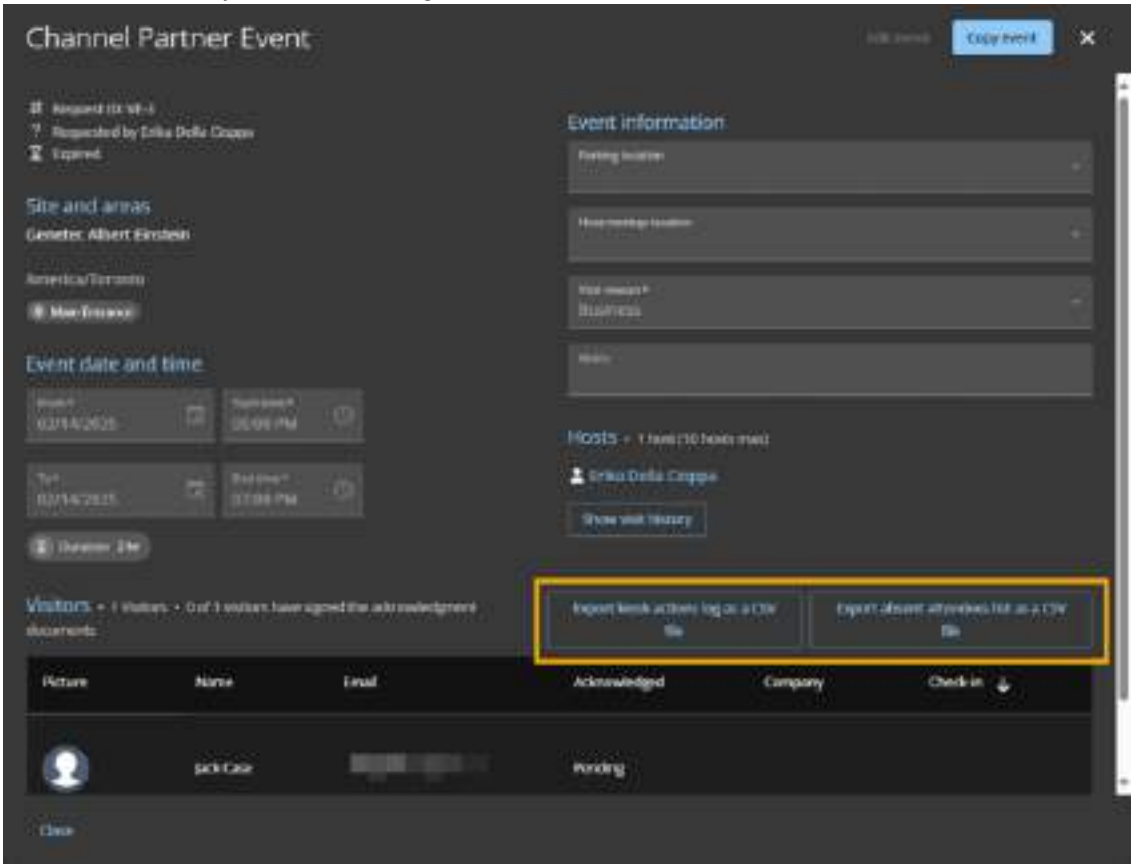
Invite visitors and review your visit events.

What you should know

You must be an *Account administrator*, *Area owner*, requester, or host to view visit event logs.

Procedure

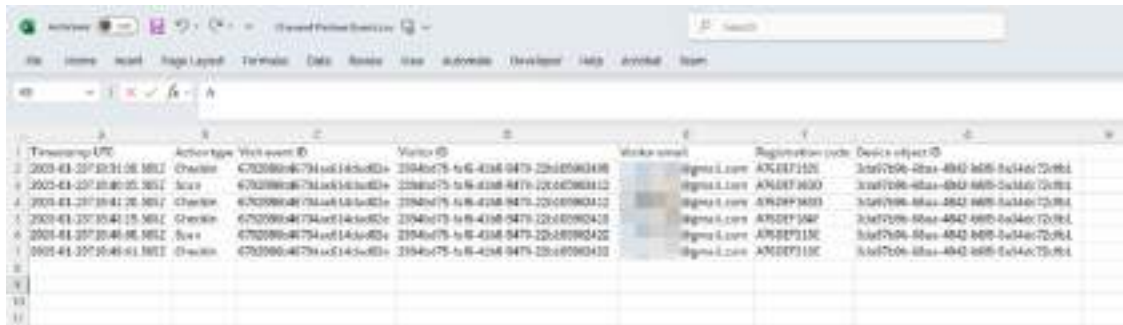
1. From the dashboard, go to Visits.
2. From the visit type filter, select All visits.
NOTE: By default, 10 visits are displayed. You can click Load more to display the next 10 visits.
3. Select the event for which you want to audit visit logs.



- a. Click Export kiosk actions log as CSV file to download a log of actions performed on visitor management devices during the event.
- b. Click Export absent attendees list as CSV file to download a list of visitors who didn't check in to the visit event.

Example

The visit event log is downloaded as a .CSV file. By default, the exported file is created using the visit event name. For example, Channel Partner Event.csv or Channel Partner Event-absentees.csv.



Timestamp	Action type	Visit event ID	Visitor ID	Visitor email	Registration code	Device object ID
2023-01-20 10:00:00	Checkin	670208046734a6143a083e	2304a675-5a5e-42a8-9479-22a00903110	sigma.l.com	A90E7110	3a0700e-88aa-4942-8605-5a34ac7208d
2023-01-20 10:00:00	Scan	670208046734a6143a083e	2304a675-5a5e-42a8-9479-22a00903110	sigma.l.com	A90E7110	3a0700e-88aa-4942-8605-5a34ac7208d
2023-01-20 10:00:00	Checkin	670208046734a6143a083e	2304a675-5a5e-42a8-9479-22a00903110	sigma.l.com	A90E7110	3a0700e-88aa-4942-8605-5a34ac7208d
2023-01-20 10:00:00	Checkin	670208046734a6143a083e	2304a675-5a5e-42a8-9479-22a00903110	sigma.l.com	A90E7110	3a0700e-88aa-4942-8605-5a34ac7208d
2023-01-20 10:00:00	Scan	670208046734a6143a083e	2304a675-5a5e-42a8-9479-22a00903110	sigma.l.com	A90E7110	3a0700e-88aa-4942-8605-5a34ac7208d
2023-01-20 10:00:00	Checkin	670208046734a6143a083e	2304a675-5a5e-42a8-9479-22a00903110	sigma.l.com	A90E7110	3a0700e-88aa-4942-8605-5a34ac7208d

Browse

- About visit event logs in ClearID

9.7 | Copying a visit event in ClearID

You can copy a visit event to take advantage of reusable information in a recurring visit or visit events that include a large number of participants.

Before you begin

Review visit events.

What you should know

- Any user can copy their visits to create a similar visit.
- Use the Copy event function when you have recurring visits or a visit that includes a large number of participants. For example, one of the following situations:
 - Repeat visitors
 - A meeting that has the same or similar attendees as a previous meeting
 - Monthly customer visits
 - A yearly business partner conference

Procedure

1. Click Dashboard > Visits.
2. Click the visit event that you want to copy.
3. Click Copy event.
A copy of the visit event is created.
4. Modify the visit event as required and click Save.
For example: changing the event details, changing dates, adding or removing visitors, adding or removing hosts, or amending notifications.

Results

The new visit event is created and a *Visit created* email notification is sent to all visitors and hosts.

9.8 | Modifying visit events in ClearID

From time to time, you might want to modify a visit event to change the event details, or to add or remove visitors or hosts. Updating the visit event details ensures that your visitors are always kept up to date following any changes to an upcoming event.

Before you begin

Create your visit events in Genetec ClearID™ by doing one or more of the following:

- Inviting visitors manually in ClearID
- Inviting visitors using a CSV import in ClearID

What you should know

- Visit events can only be modified before the start of the visit event.
- Any modifications to a visit event are highlighted in the updated email notifications sent to relevant recipients.
- If visit event approval is enabled, any modifications to a visit event that are not Reason field modifications generate approval notifications for the relevant approvers to re-approve any changes or additions.
- Changing an existing visitor or host email to a different email triggers a cancellation notification for the original email and a visit event notification for the newly updated email.
- If visit event approval is enabled, changing a visitor name or host name details does not trigger email notifications for visitors, but does trigger the approval workflow again.

Procedure

1. Click Dashboard > Visits.
2. (Optional) If the list is long, use the drop-down menus and column filters to refine the results.

Name

Enter a search criteria to search for the visit event by name.

Status

Select one or more status filters to search for the visit event using the event status.

Site

Start typing to find a site or select a site from the Site list.

Date

In the Date column, use the ascending (▲) or descending (▼) controls to adjust the order of the results.

3. Click a visit event and review the event details to verify it is the event that you want to modify.
4. Click Edit event.

5. Modify one or more of the following as required:
 - a. In the Name field, modify the name.¹
 - b. In the Event date and time section, modify the start or end date and time.¹
 - c. In the Event information section, modify the parking location, host meetup location, or notes.¹
Visit event Visit reason modifications do not trigger any approval notifications because the reason has no impact on visitors attending the event.
 - d. In the Visitors section, add, modify, or remove visitors.
Any changes to visitors are assessed again to verify any watchlist screening criteria.
 - e. In the Hosts section, add, modify, or remove hosts.
- NOTE: ¹Modifying the Name, Event date and time, or Event information does not trigger re-approval (if approvals are applicable).
6. Click Save to confirm your changes.

After you finish

Review your visit event details to verify that the changes are correct.

9.9 | Approving visit event requests in ClearID

To modify or approve visit requests, *Visit event approvers* must review the pending approvals and then decide which requests to approve.

Before you begin

Enable visitor management for sites.

What you should know

When a visit request is submitted, the specified *Visit event approvers* receive an email notification.

Procedure

1. To view the details of a request for approval or denial, click Approve in the visit request email.
You're redirected to the Genetec ClearID™ portal where you're prompted to sign in.
2. Review the request details and make any required changes.
Tip: You can modify the request if the request has an error or something that needs to change. For example, you can amend the dates due to an office closure, or amend the parking location to a more appropriate location.

The screenshot displays the Genetec ClearID portal interface for a visit request titled "Global meeting with vendors". The request is in a "Waiting for approval" state, requested by "Sharon". The interface is divided into several sections: "Site and areas" (SJ Corp, New York), "Event date and time" (From: 10/13/2024, To: 10/17/2024), and "Event information" (Parking location, Host meeting location, Visit reason: Business). A "History" section on the right shows system actions like "Genetec ClearID™ system edited the request" and "Genetec ClearID™ system has verified all people against watchlists". At the bottom right, there are "Deny" and "Approve" buttons, with the "Approve" button highlighted by a yellow box.

- a. (Optional) Click Show more... to view the history of changes made to the visit request.
 - b. (Optional) Click Add comment to add notes to the history of the visit request. For example, you can add notes explaining why you changed the date and time of the visit.
3. Click Approve.
 - a. (Optional) In the Reason for approval field, enter a reason for the visit approval.
 - b. Click Confirm.

Tip: To view a list of all pending approvals, go to Dashboard > My tasks and select Pending from the list.

Results

A confirmation email is sent to both the visitor and the host outlining the details of the visit.

After you finish

Add the visit event to your calendar.

9.10 | Adding ClearID visit events to your calendar

Hosts and visitors can keep track of events and simplify the check-in process by adding visits to their calendars. To add a Genetec ClearID™ visit event to your calendar, open the visit confirmation email and download the attached ICS file.

Before you begin

Create a visit event.

What you should know

When a visit event is created, both the host and the visitors receive a confirmation email with the details of the event. The confirmation email also includes an ICS file that you can use to add the event to your digital calendar.

Procedure

1. Open the visit confirmation email.
2. Download the attached CSV file.

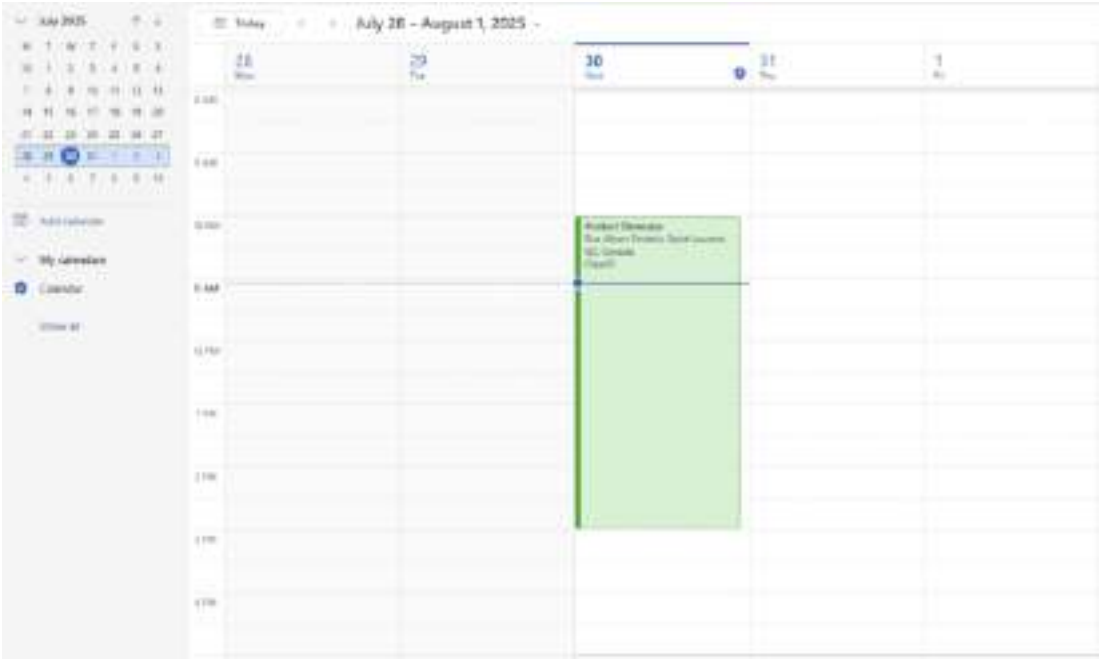


NOTE: Both ICS files contain the details of the visit. The visitor's copy also includes a QR code, allowing them to check in to the event directly from their calendar.

3. Follow the instructions in your chosen digital calendar to add the visit event.

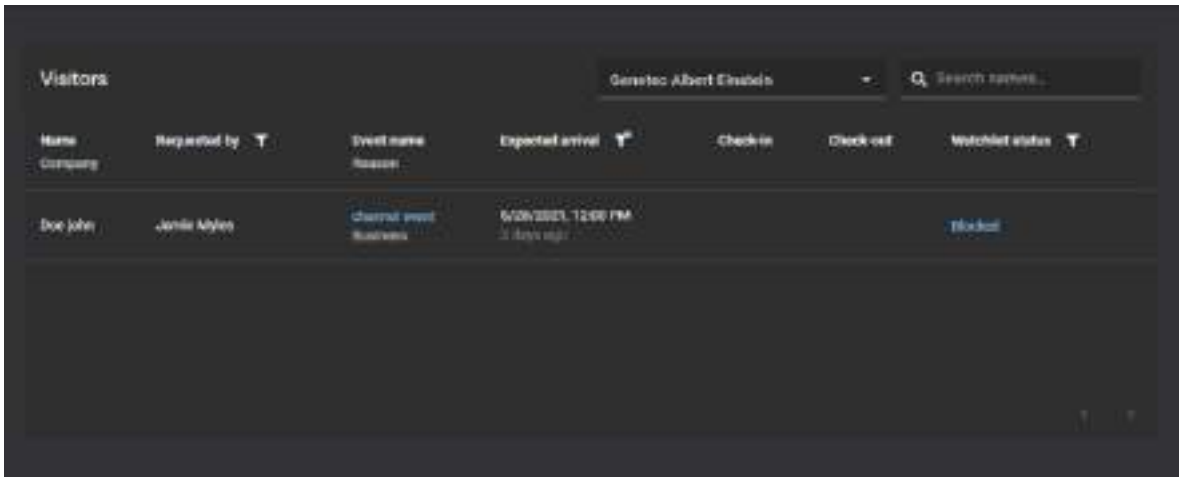
Results

You can now view the visit event and its details in your calendar.



9.11 | About visitors report in ClearID

In Genetec ClearID™, a visitors report is a list of current or upcoming visits, or visits that occurred in the past for a specific site. The report includes information about visitor name, event requester, event name, expected arrival, check-in, check-out, and watchlist status.



Visitors report

The visitors report is used by *site owners* and *watchlist managers* to check current or upcoming visits, or visits that occurred in the past and also to provide information to auditors.

Filters can be used to help refine the report search results by event requester, expected arrival, and watchlist status.

Browse

- [Viewing a visitors report in ClearID](#)

9.12 | Viewing a visitors report in ClearID

You can view a visitors report for any current or upcoming visits, or visits that occurred in the past. The report results are specific to a site, and can be filtered using event requester, expected arrival, and watchlist status.

Before you begin

[Invite your visitors.](#)

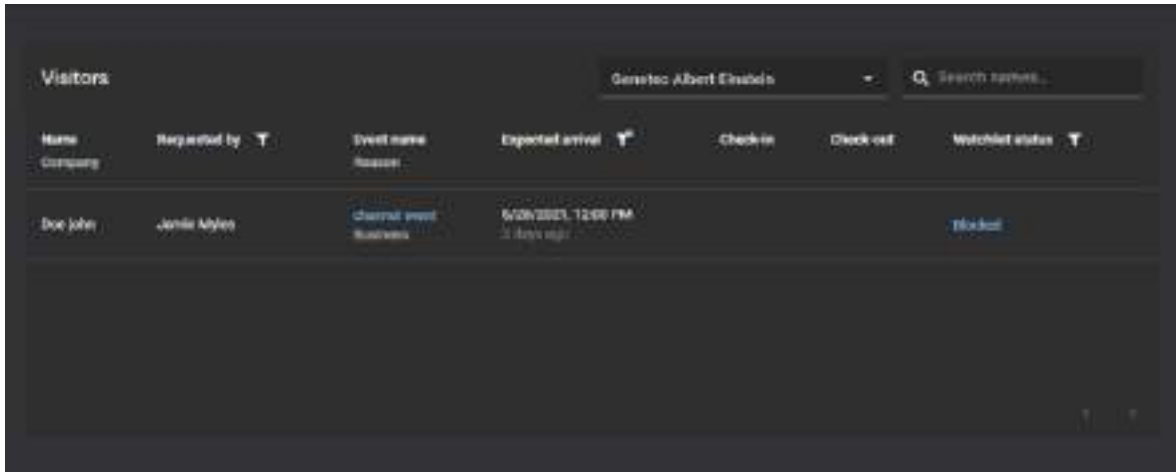
What you should know

- *Site owners* and *watchlist managers* can view the visitors report.
- Only watchlist managers can unblock or allow blocked visitors.

NOTE: For customers who have not purchased a watchlist license, the Watchlist status column is present in the report but displays N/A because no watchlist data is available.

Procedure

1. From the homepage, click Reports > Visitors.
2. Select a site from the Site list.



3. (Optional) Enter a name in the search box.
4. (Optional) Click the Requested by filter icon  and enter a visit requesters name.
5. (Optional) Click the Expected arrival filter icon  and select an expected arrival option:
 - Current and upcoming visits
 - A day ago
 - 7 days ago
 - 30 days ago
 - 90 days ago
 - All past events

Tip: If no visitors are displayed, select a longer Expected arrival filter to increase the filtered results that are displayed.

6. (Optional) Click the Watchlist status filter icon  and select one or more checkbox options:

Allowed

The visitor did not match any block list entries during the watchlist screening process and was allowed access to visit the site.

Blocked

The visitor matched one or more block list entries during the watchlist screening process and was blocked from visiting the site.

Unblocked

The visitor matched one or more block list entries during the watchlist screening process but was allowed access to visit the site by the watchlist manager.

In progress

Visitor watchlist screening is in progress.

Notified

The visitor matched one or more notify list entries during the watchlist screening process. The watchlist manager was notified and the visitor was allowed access to the site.

- a. (Optional) Click the Blocked hyperlink to open the Visitor watchlist alert dialog. From this dialog, a watchlist manager can allow entry if required.
- b. (Optional) Click the information icon next to an unblocked watchlist status for more information about who unblocked the visitor.

7. (Optional) Click  to reset filter selections and return to the visitors list.

Browse

- [Unblocking visitors blocked by a watchlist in ClearID](#)
- [About visitors report in ClearID](#)

9.13 | QR codes as a credential for visitors in ClearID

Genetec ClearID™ can use QR codes as a credential for visitors to simplify access to parking entrance barriers, turnstiles, or gated facilities.



The following third-party vendor QR code solutions are currently supported:

- Qscan barcode readers
- STid QR code readers

Visitors can use a QR code as a credential to open parking entrance barriers, turnstiles, or gated facilities:

- The QR code contained in a visitor confirmation email can be presented using a smartphone.
- The visitor confirmation email can also be printed and used for check-in.
- SMS messages notify hosts when their visitors arrive (if the check-in notification function is enabled).

Browse

- [Supported devices for ClearID](#)

9.13.1 | Importing a custom card format (QR code credential) in Synergis

Before you can use QR codes as a credential in Genetec ClearID™, you must configure Synergis™ to support the ClearID QR code custom card format. A QR code can then be used as a credential to access parking entrances, turnstiles, or gated facilities.

Before you begin

- [Install the ClearID plugin](#)
- Make sure that the Visitor Management module is activated in your Security Center Synergis License.

What you should know

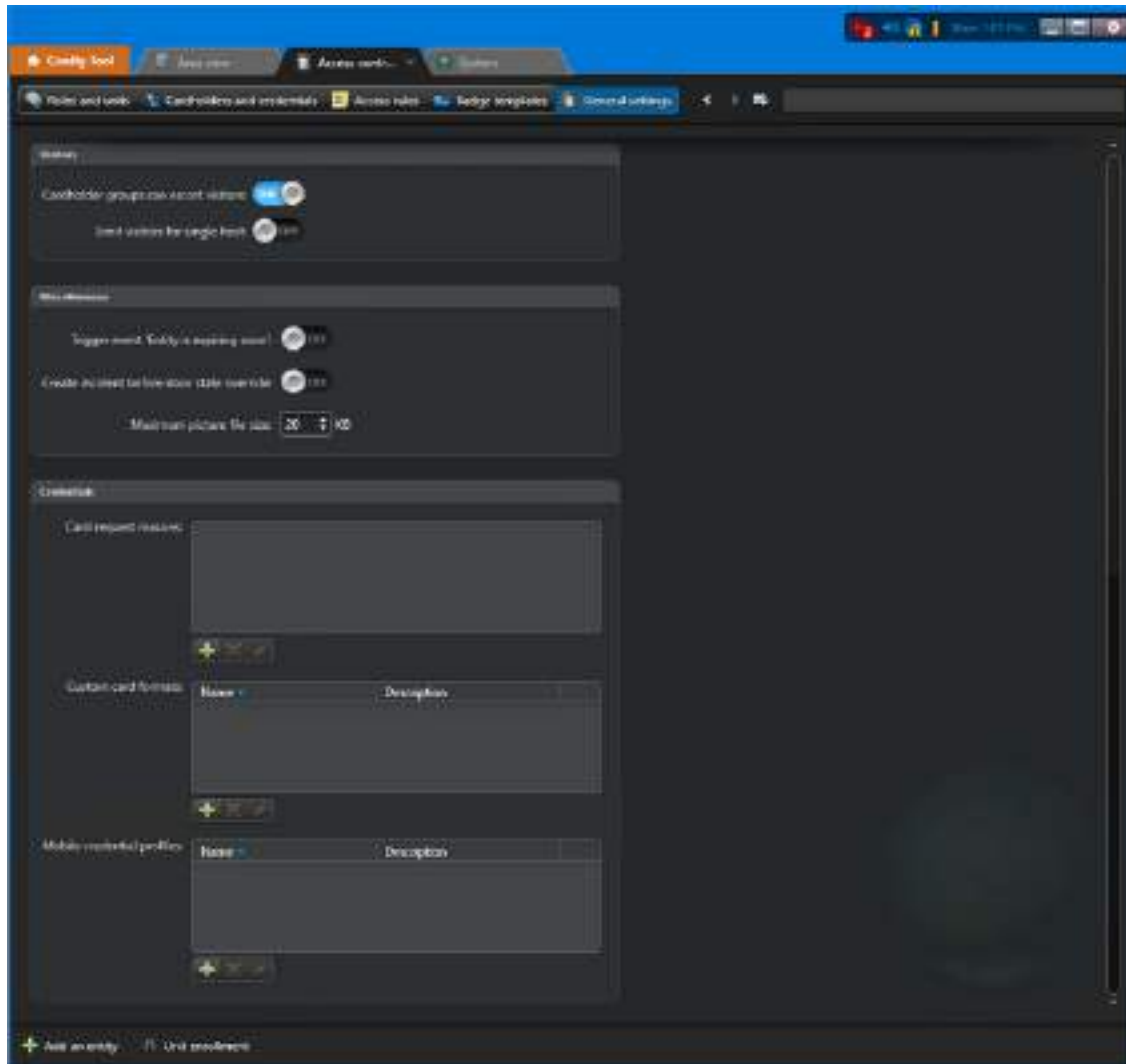
Only Security Center administrators or users with the *modify credential properties* privilege can import the custom card format.

The SDK and ClearID Plugin do not automatically create the custom card format for QR codes.

IMPORTANT: The custom card format is found on the Security Center machine where the ClearID plugin is installed.

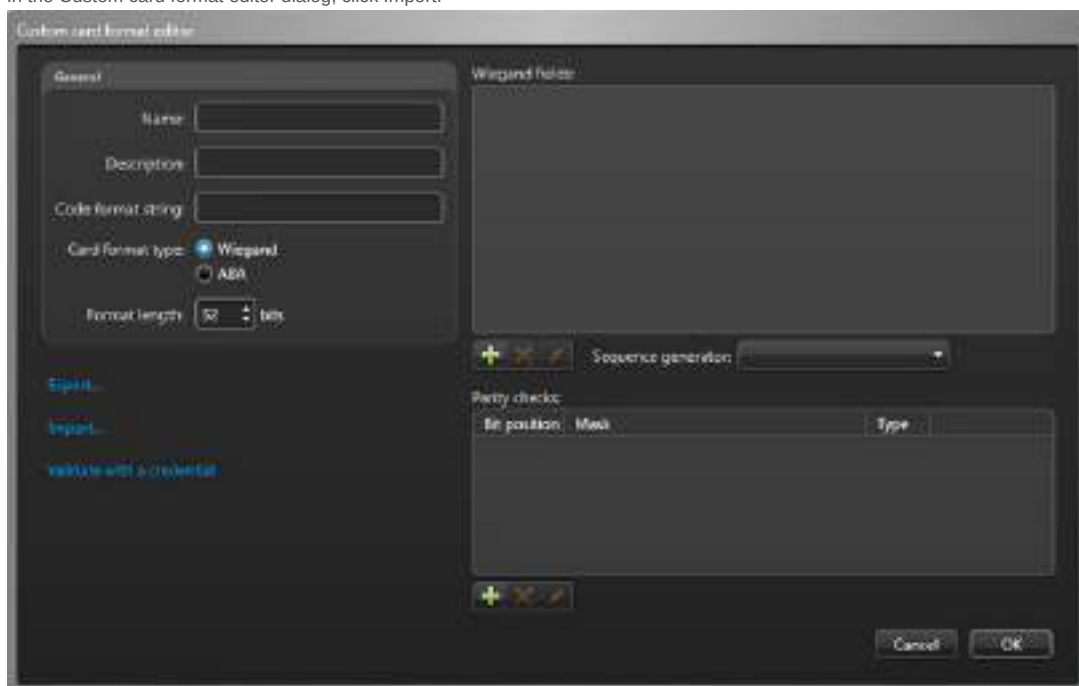
Procedure

1. In Config Tool, open the Access control task and select the General settings view.



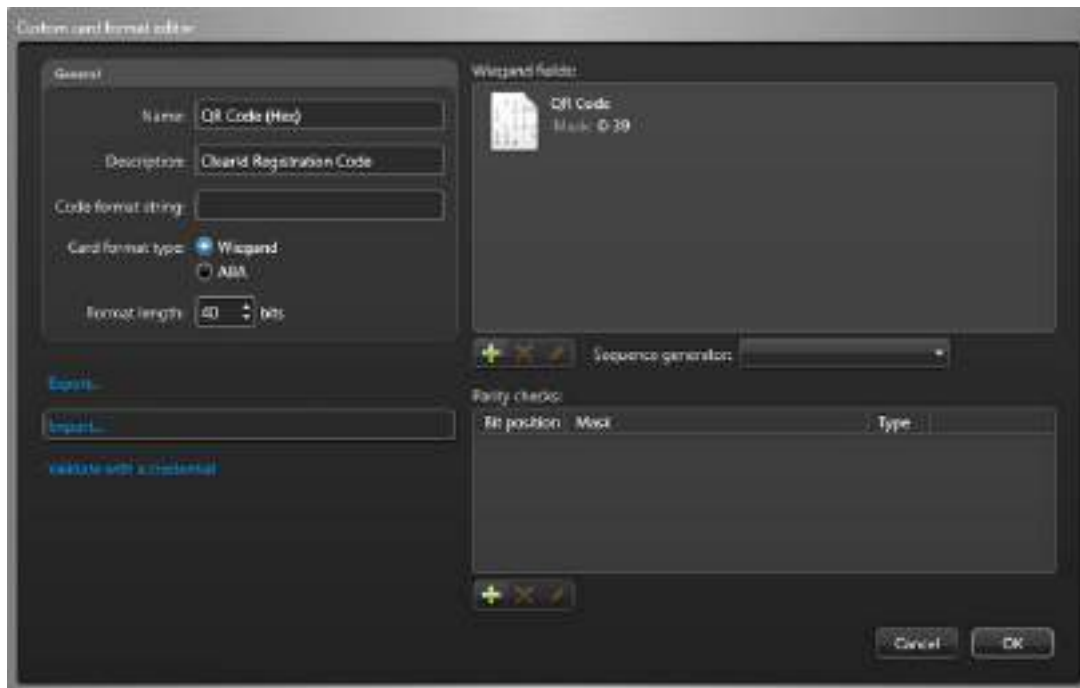
2. In the Custom card formats section of Credentials, click Add an item (+).

 - a. Download this [QRcode.xml](#) file.
 - b. In the Custom card format editor dialog, click Import.

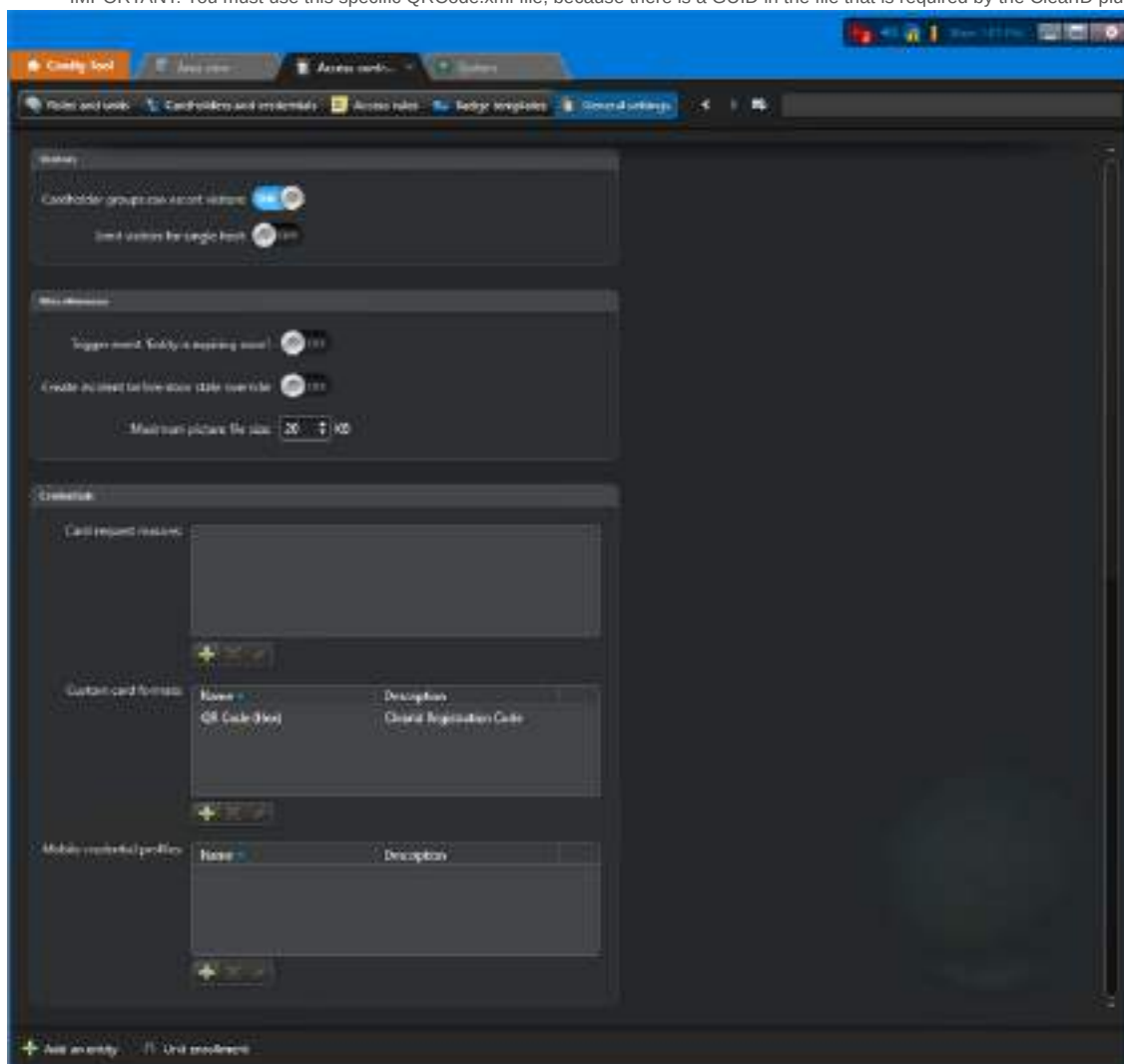


IMPORTANT: You must import the custom card format on the machine where the ClearID plugin is installed. The card format type that is used during import is Wiegand format.

- c. Navigate to and select the QRcode.xml file you downloaded.
- d. Click Open and click OK.



IMPORTANT: You must use this specific QRCode.xml file, because there is a GUID in the file that is required by the ClearID plugin.



Results

In the Access control task General settings view, the QR code (Hex) custom card format is now selected and available.

After you finish

Enable QR code credentials for visitors.

Parent topic: QR codes as a credential for visitors in ClearID

Browse

- License options for ClearID system integration

9.13.2 | Enabling QR code credentials for visitors in ClearID

To automatically create a QR code credential for visitors when a visit request is created, you must enable QR code credentials for visitors.

Before you begin

- Enable visitor management for sites in Genetec ClearID™
- Import a custom card format (QR code credential) in Synergis™

IMPORTANT: Make sure that the custom card format (QR code) is imported and available in the Security Center that your site is connected to.

What you should know

Only site owners or account administrators can enable the QR code credentials for visitors.

- When a QR code is automatically created for a visitor, the visitor is created in an inactive state, and the visitor credential contains an automatically generated QR code. The QR code in the credential matches exactly the QR code in the visitor confirmation email.
- The visitor credential is active at this point, but the QR code is not usable, because the visitor is not checked in yet. When the visitor check-in occurs, the QR code is valid until the visitor checks-out, or the end of the day for the scheduled visit.

For example, QR code credentials for visitors could be used to automatically grant access to a turnstile after check-in.

Procedure

1. Click Organization > Sites.
2. Search for and select a site.
3. Click Visitor management to configure the visitor management options for a site.
4. In the Advanced section, select Automatically create QR code credentials for visitors.



5. Click Save.

Results

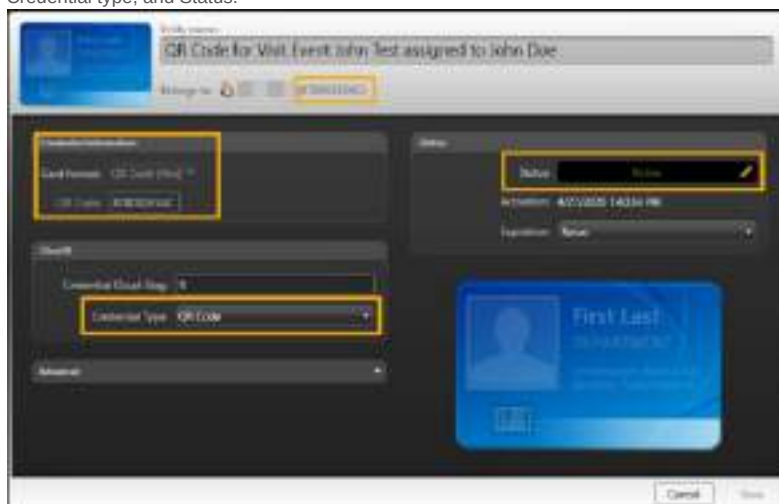
The next time a visitor is invited to the site, ClearID automatically creates a QR code credential for the visitor. The QR code is included in the visitor confirmation email.



After you finish

Perform a visitor invite and check-in test, to validate that QR code credentials are automatically created for visitors.

Tip: You can perform a visitor search in the Visitor management task in Security Desk, then edit the credential to check the visitors' Credential information, Credential type, and Status.



Parent topic: QR codes as a credential for visitors in ClearID
Browse

- Enabling visitor management for sites in ClearID

9.13.3 | Configuring Qscan devices for ClearID

Before you can use QR codes as a credential in Genetec ClearID™, you must configure your Qscan devices to support the custom card format (QR code credential) used in ClearID. A QR code can then be used as a credential to access parking entrances, turnstiles, or gated facilities.

Before you begin

Familiarize yourself with the Qscan documentation:

- [Qscan User Guide \(PDF\)](#)
- [Qscan \(for parking lots\) brochure \(PDF\)](#)
- [QscanT \(for turnstiles\) brochure \(PDF\)](#)
- [QscanI \(indoor version\) brochure \(PDF\)](#)

WARNING: Qscan barcode readers contain a Class 2 laser. Do not look directly into the laser.

What you should know

This procedure is for system integrators or account administrators who install and configure barcode scanners.

The following Qscan devices can be used with ClearID to scan QR codes as a credential for visitors:

- Qscan (for parking lots)
- QscanT (for turnstiles)
- QscanI (indoor version)

Procedure

1. Connect a Qscan barcode reader to a Mercury Controller.
2. Configure Qscan barcode reader to support 40-bit hexadecimal QR codes.

Parent topic: [QR codes as a credential for visitors in ClearID](#)

Browse

- [Supported devices for ClearID](#)

9.13.3.1 | [Connecting a Qscan barcode reader to a Mercury Controller for ClearID](#)

[QR codes as a credential for visitors in ClearID](#) >

In situations where you need to use a Qscan barcode reader to access parking entrances, turnstiles, or gated facilities, you must connect a Qscan barcode reader to a Mercury controller. This ensures that the barcode reader can communicate with Security Center Synergis™ to manage access.

Before you begin

WARNING: Qscan barcode readers contain a Class 2 laser. Do not look directly into the laser.

What you should know

This procedure is for system integrators or account administrators who install and configure barcode scanners.

In this scenario, we describe how to connect a Qscan barcode reader to a Mercury EP 1502 controller.

Procedure

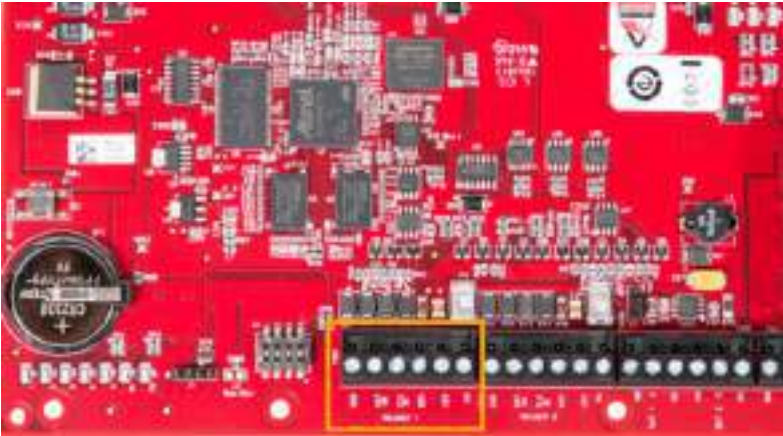
Connect your Qscan barcode reader device to the Reader 1 connection block in the Mercury EP 1502 controller.



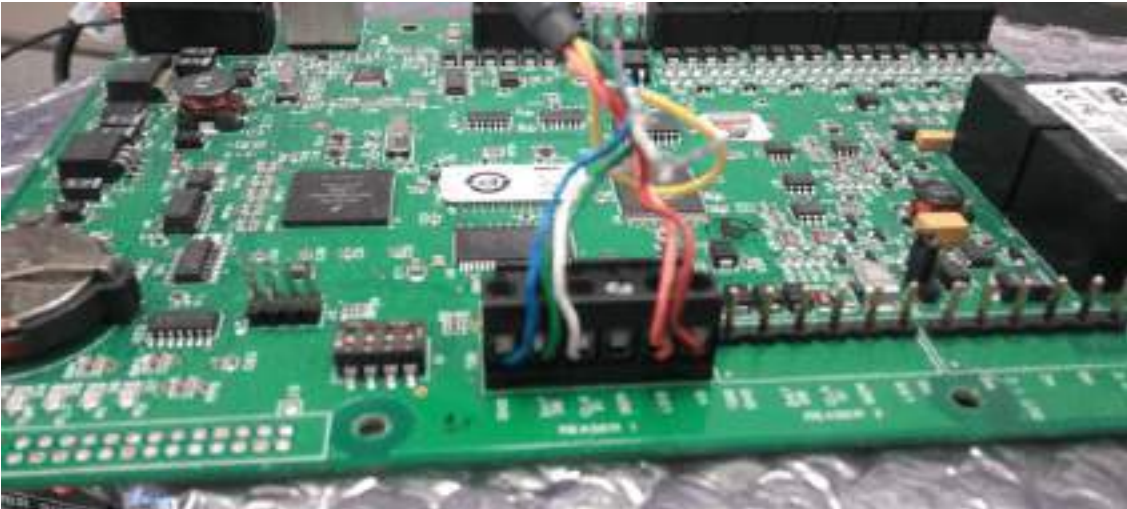
Figure 1: Qscan barcode reader



Figure 2: Mercury EP1502 controller boards



NOTE: The Mercury controller boards can vary in color depending on when they were manufactured and purchased.
Figure 3: Mercury EP1502 controller board wiring loom connections



Use the following table to understand how to connect the Qscan barcode reader wires to the terminals on the Mercury controller *Reader 1* connector block.

Mercury controller and Qscan reader wiring connections	
Mercury EP1502: Reader 1 connections	Qscan barcode reader: wire colors
GND (Ground)	BLUE
DAT D0 (Data/Data 0/TR-)	GREEN
CLK D1 (Clock/Data 1/TR+)	WHITE
BZR (Reader Buzzer)	Not applicable
LED (Reader LED)	ORANGE
V0 (Reader Power)	RED

After you finish

Configure Qscan barcode reader to support 40-bit hexadecimal QR codes
Parent topic: [Configuring Qscan devices for ClearID](#)

9.13.3.2 | Configuring Qscan barcode reader to support 40-bit hexadecimal QR codes for ClearID

QR codes as a credential for visitors in ClearID >

Before the QR codes automatically generated by Genetec ClearID™ for visitor confirmation email notifications can be understood and processed by Synergis™ Cloud Link during check-in, you must configure your Qscan barcode reader to support 40-bit hexadecimal QR codes.

Before you begin

Connect Qscan barcode reader to Mercury controller

WARNING: Qscan barcode readers contain a Class 2 laser. Do not look directly into the laser.

What you should know

This procedure is for system integrators or account administrators who install and configure barcode scanners.

In this scenario, we describe how to program Qscan devices to support 40-bit hexadecimal QR codes used in ClearID and output to Synergis Cloud Link.

For example, a QR code when scanned by Qscan is typically read as alphanumerics ABC1234567.

Synergis Cloud Link requires the QR code in HEX format 0xAB 0xC1 0x23 0x45 0x67 to manage access requests.

CAUTION:

The steps described in the following process remove alphanumeric QR code support from the Qscan barcode reader. The Qscan barcode reader cannot be used in alphanumeric mode while the 40-bit hexadecimal mode is active.

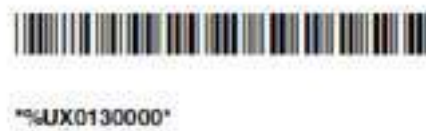
Procedure

1. To reset to factory default settings, scan the qscan resetbarcode1.pdf barcode.



NOTE: The Qscan reader beeps twice if the factory reset is successful.

2. To ignore alphanumeric characters, scan the qscan no alpha delete.pdf barcode.



3. To turn HEX conversion on, scan the qscan hex conversion.pdf barcode.



4. To output 40-bits, scan the qscan 40-bit.pdf barcodes.

NOTE: This file has three barcodes so scan one at a time.



Parent topic: Configuring Qscan devices for ClearID

9.13.4 | Configuring STid devices for ClearID

Before you can use QR codes as a credential in Genetec ClearID™, you must configure your STid devices to support the QR code custom card format used in ClearID. A QR code can then be used as a credential to access parking entrances, turnstiles, or gated facilities.

Before you begin

Familiarize yourself with the STid documentation:

- Architect® Blue QR code readers.
 - ARCS-AQ/BT - 13.56 MHz + Bluetooth® + QR Code multi-technology reader
- SECard - High security programming kits
- SECard User Manual

What you should know

This procedure is for system integrators or account administrators who install and configure QR code readers.

In this scenario, we describe how to program STid devices to support 40-bit hexadecimal QR codes used in ClearID and output to Synergis™ Cloud Link.

Procedure

1. Learn about STid QR code readers.
2. Import custom card format.
3. Set up and connect your QR code reader to your access control panel.

NOTE: The steps you must perform will vary depending on your access control panel.

 - To connect your OSDP reader to Synergis Cloud Link, see OSDP readers connected to the Synergis Cloud Link RS-485 ports.
 - To connect your OSDP reader to Mercury, see Adding OSDP (Secure Channel) readers to a Mercury controller.
4. Creating an STid QR code reader configuration for ClearID.
5. Transferring your reader configuration to your STid QR code reader for ClearID.

After you finish

Add doors to areas.

Parent topic: [QR codes as a credential for visitors in ClearID](#)

9.13.4.1 | [About STid QR code readers in ClearID](#)

[QR codes as a credential for visitors in ClearID](#) >

In Genetec ClearID™, STid QR code readers can be used to read QR code credentials.



NOTE: The image shown here illustrates STid readers that you might have in your organization. For a list of the Open Supervised Device Protocol (OSDP) readers that ClearID supports, see [Supported devices](#).

Why choose the OSDP protocol over Wiegand protocol?

WIEGAND Protocol

In Wiegand the reader always sends a fixed-length wiegand format, regardless of the credential length. The *custom card format* called by Security Desk is always the same. The manufacturer has confirmed this Wiegand readers (SY-ARCS-R31-AQBT1-XX1) limitation.

Consequence: The credential does not match the length required by the protocol and an Unknown credential message is displayed in Security Desk even if this QR code credential is already enrolled in the Security Center Synergis™ database.

Workaround: To make sure that all types of credentials work simultaneously with Wiegand protocol readers and Synergis, all other credentials (RFID or QR code from another source such as Axis) should match the ClearID QR code credential length (40 bits). This approach ensures that Synergis always receives the same *custom card format* (the card format from ClearID) and correctly interprets all types of payloads that the reader sends.

OSDP Protocol

In Open Supervised Device Protocol (OSDP) the reader dynamically adapts the format length regarding the credential length.

Best Practice: Use OSDP with STid QR code readers to ensure that the QR code credential is accepted and understood.

The following table shows example reads from the same reader.

Credential code	Card format	
4AE6CD6464E	QR code (HEX)	ClearID QR code
E01EC72022429729	64 bits	DESFire 64 bits private ID credentials

The examples show that the *custom card format* called by Security Desk is different for each read.

Consequence: The OSDP reader is more flexible and correctly interprets the credential.

Planning your QR code reader deployment

Depending on your needs, you can use the latest STid Architect® Blue QR code readers. Alternatively, you can add interchangeable QR code modules if you want to reuse existing STid readers.



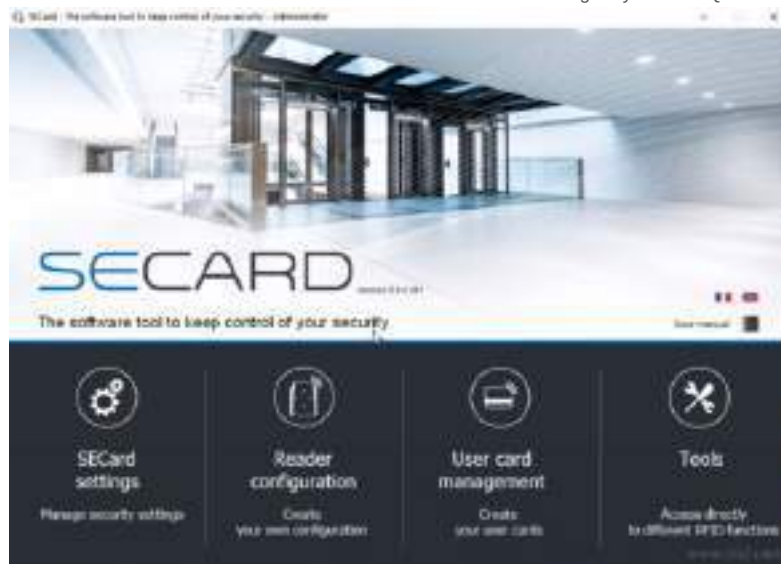
Consider the following when planning your STid QR code reader implementation:

- Best Practice: If you are planning a new STid QR code reader implementation, consider using the latest QR code readers with the latest firmware. For example, model: ARCS-AQ/BT. Only use STid readers that support the OSDP protocol and have upgraded to firmware version 10.
- If you already have numerous STid readers deployed in your organization, consider adding the interchangeable QR code reader module and updating your firmware.
Tip: Using the interchangeable module upgrades can result in significant savings on a large project.
- If you are re-using existing readers, refer to *STid documentation* about how to upgrade your reader to firmware version 10 or later.

Programming your STid QR code readers

The STid QR code readers can be programmed using the *STid SECard - High security programming kit*.

Best Practice: Use STid SECard software version 3.5 or later to configure your STid QR code readers.



The KIT-SECARD-BT-V3.X includes the following:

- STid Architect® ARC-G desktop reader, enroller, encoder



- USB key containing the STid SECard software



IMPORTANT: Genetec Inc. does not provide support for the STid SECard solution. Customers must use the stand-alone STid SECard software to configure the OSDP readers to work with the ClearID ACS panel solution.

Parent topic: [Configuring STid devices for ClearID](#)

[Browse](#)

- [Supported devices for ClearID](#)

9.13.4.2 | Creating an STid QR code reader configuration for ClearID

[QR codes as a credential for visitors in ClearID >](#)

Before you can use QR codes as a credential in Genetec ClearID™, you must create your STid QR code reader configuration. A QR code can only be used as a credential for an STid QR code reader after the QR code reader configuration has been uploaded to an STid OCB smart card and then transferred to the STid QR code reader.

Before you begin

Familiarize yourself with the STid documentation:

- [SECard - High security programming kits](#)
- [SECard User Manual](#)
- [Install the STid SECard - High security programming kit software.](#)

What you should know

This procedure is for system integrators or account administrators who install and configure QR code readers.

NOTE: The STid SECard software requires a license, the number is typically found on the USB reader that is used to encode a smart card.

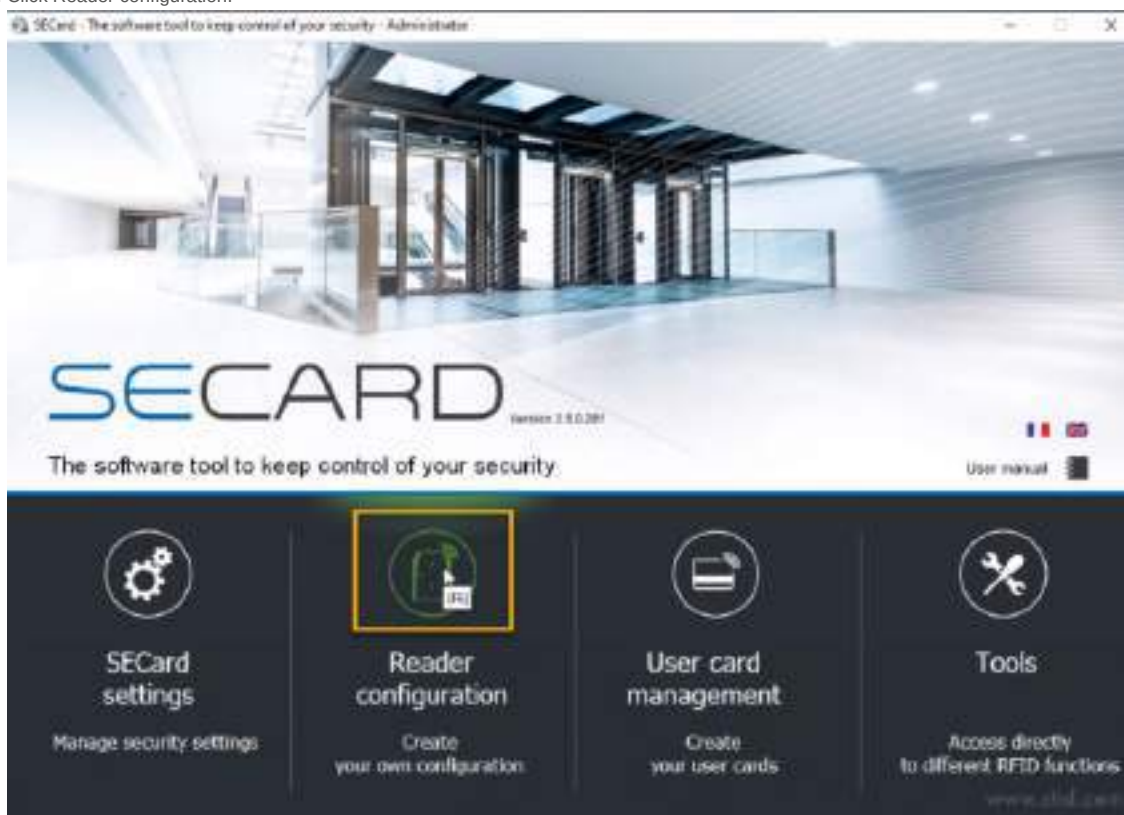


Procedure

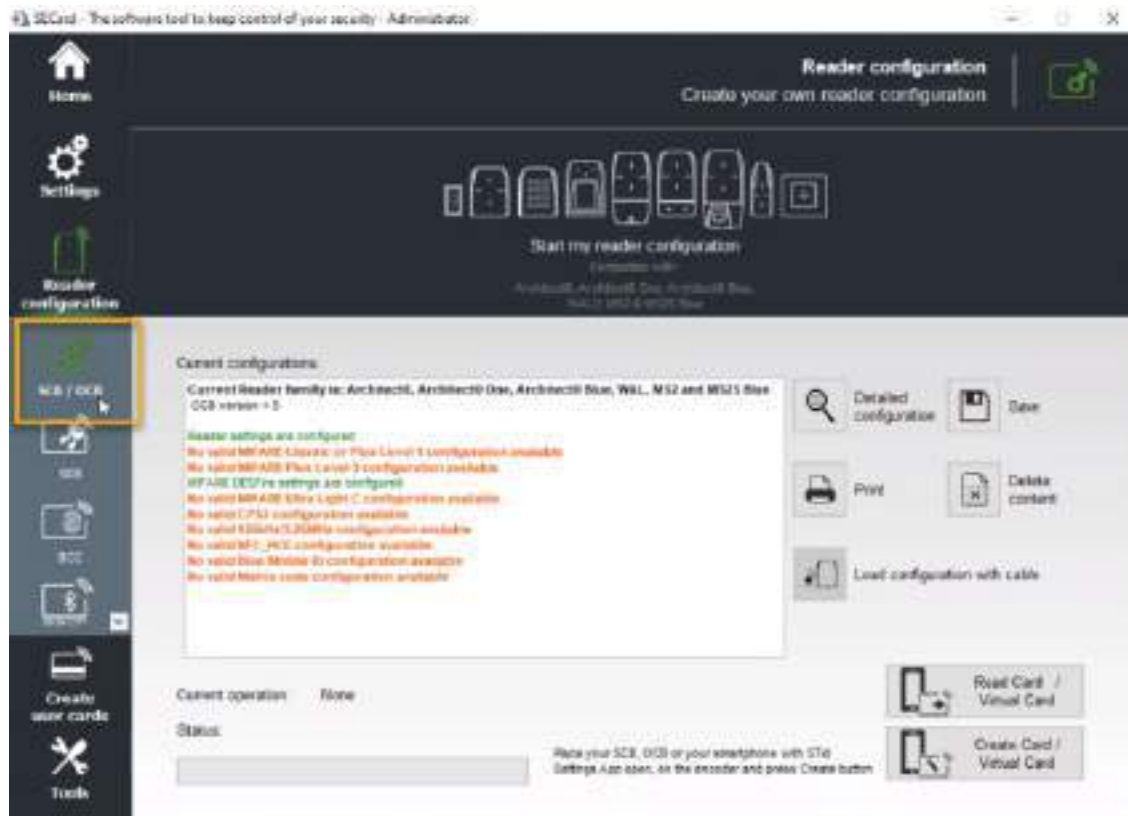
1. Launch the STid SECard - High security programming kit software to configure your STid QR code reader.



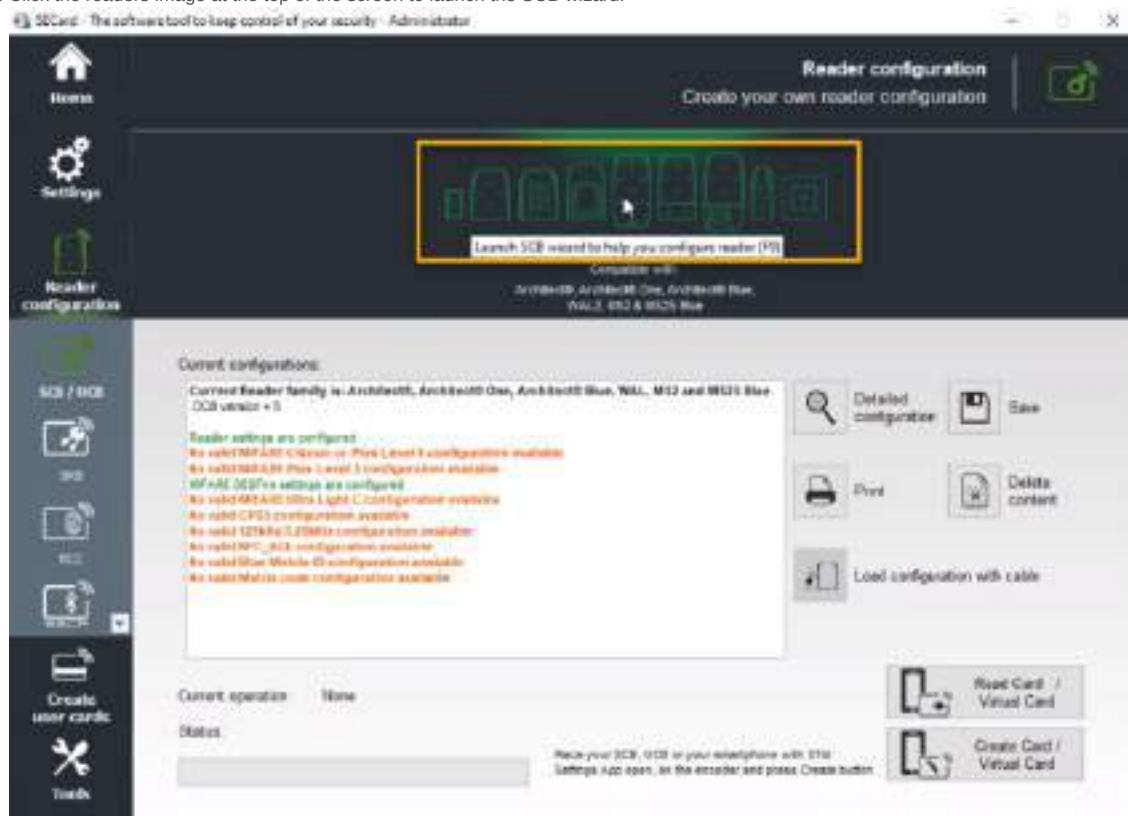
2. Click Reader configuration.



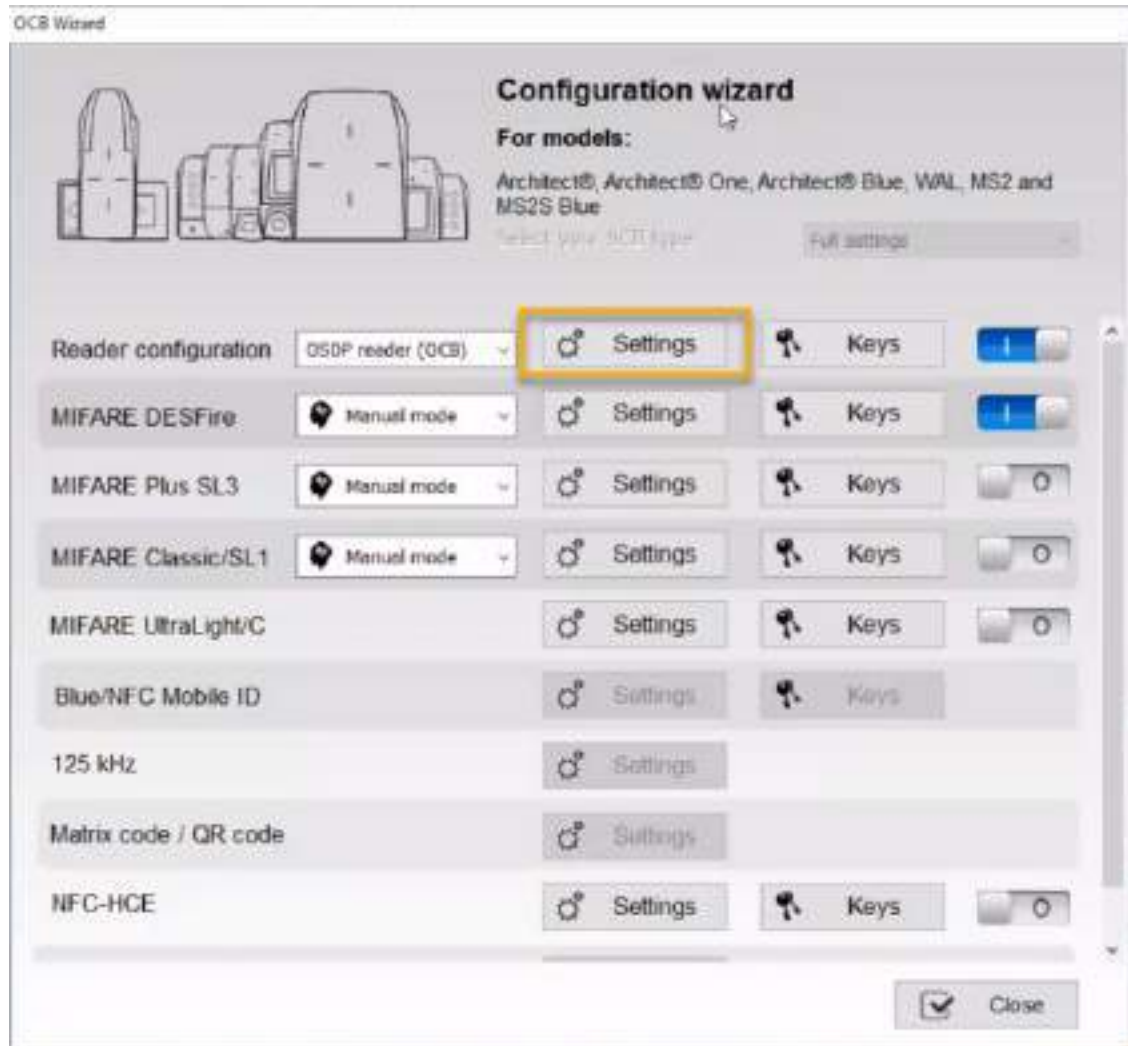
a. In the navigation sidebar, click SCB / OCB.



b. Click the readers image at the top of the screen to launch the SCB wizard.



c. In the Reader configuration row, next to OSDP reader (OCB), click Settings to open the Configuration wizard.



3. In the Configuration wizard dialog, select SECard V3.5 x OCBv5 and click Next.



a. In the Reader reference selection dialog, select the Matrix / QR Code check box and click Next.

OCB Wizard

Reader reference selection

Choose reader type and options to configure

1 2 3 4 5 6 7 8

Features activation

☐ Keypad

☐ Touchscreen

☐ Blue/NFC Mobile ID

☐ Biometric

☐ Prox 125 kHz

☒ Matrix code / QR code

Reader protection options

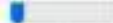
☒ Save user keys in non volatile memory

☒ Tamper switch signal

☒ Erase keys on tamper switch activation

Accelerometer sensitivity

☐ On tamper activation keeps LED red as default

 Low

Back Next Cancel

b. In the Reader parameters dialog Protocols section select the Type RAW and click Next.

OCB Wizard

Reader parameters
Protocol and options

1 2 3 4 5 6 7 8

Private ID security

☐ Data authenticated encryption

Protocols

Type ☒ RAW ☐ Wiegand

☐ Use protocol size: 4 Byte(s)

☒ Backward compatibility

☒ Justify data to left ☐ Justify data to right

Protocol options

☐ Forced site code on UID

☐ 2 bytes Value AB

☐ Enable Plain mode after secure channel authentication

☐ Use ACK instead of Busy command

Offset 0 bit(s)

☐ Change RS485 address 0

Baudrate No change

☐ No wrap text

ISO14443-3B PUPi / iClass

☐ Enable

Card ID range filter (LSB)

UID/ID range 00000000 to 80000000

Back Next Cancel

NOTE: The Byte(s) setting is not used when the Use protocol size check box is not selected. This ensures that the reader will adapt the length according to the length of the credential.

4. The following steps (4.a - 4.d) are not essential for QR code use, but might still be relevant to your installation.
- a. Click Next to skip the LED and Buzzer dialog.

OCB Wizard

LED and Buzzer
Options and parameters

1 2 3 4 5 6 7 8

LED default state

Mode ☒ Off ☐ Fixed ☐ Blinking

Color

Blink duration ON 4 at 80ms

Blink duration OFF 4 at 80ms

Buzzer sound level

Low

Card detection action

LED cycle number 3

LED duration ON 4 at 80ms

LED duration OFF 4 at 80ms

Buzzer cycle number 3

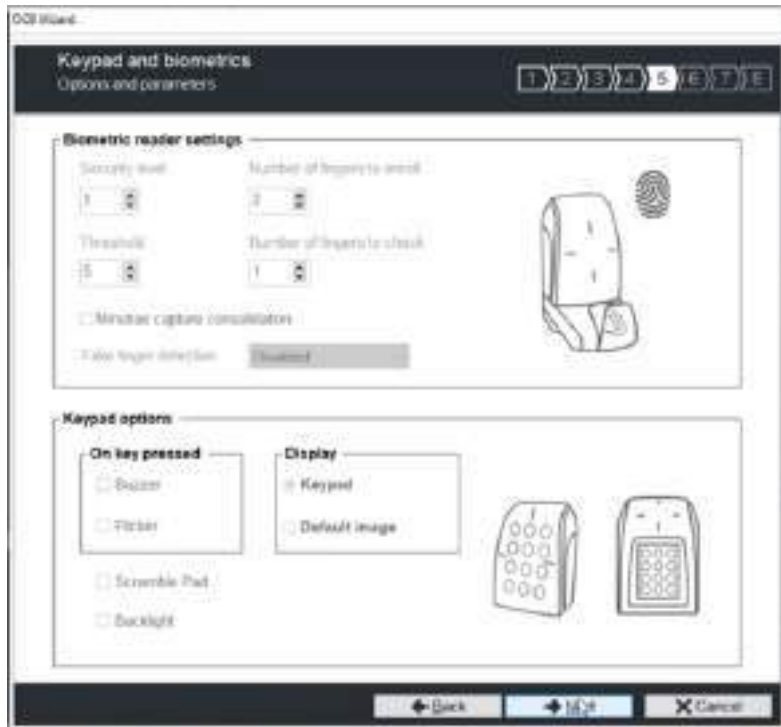
Buzzer duration ON 4 at 80ms

Buzzer duration OFF 4 at 80ms

☐ Lights at Bluetooth (BT) connector

Back Next Cancel

- b. Click Next to skip the Keypad and biometrics dialog.



c. Click Next to skip the Touchscreen options dialog.

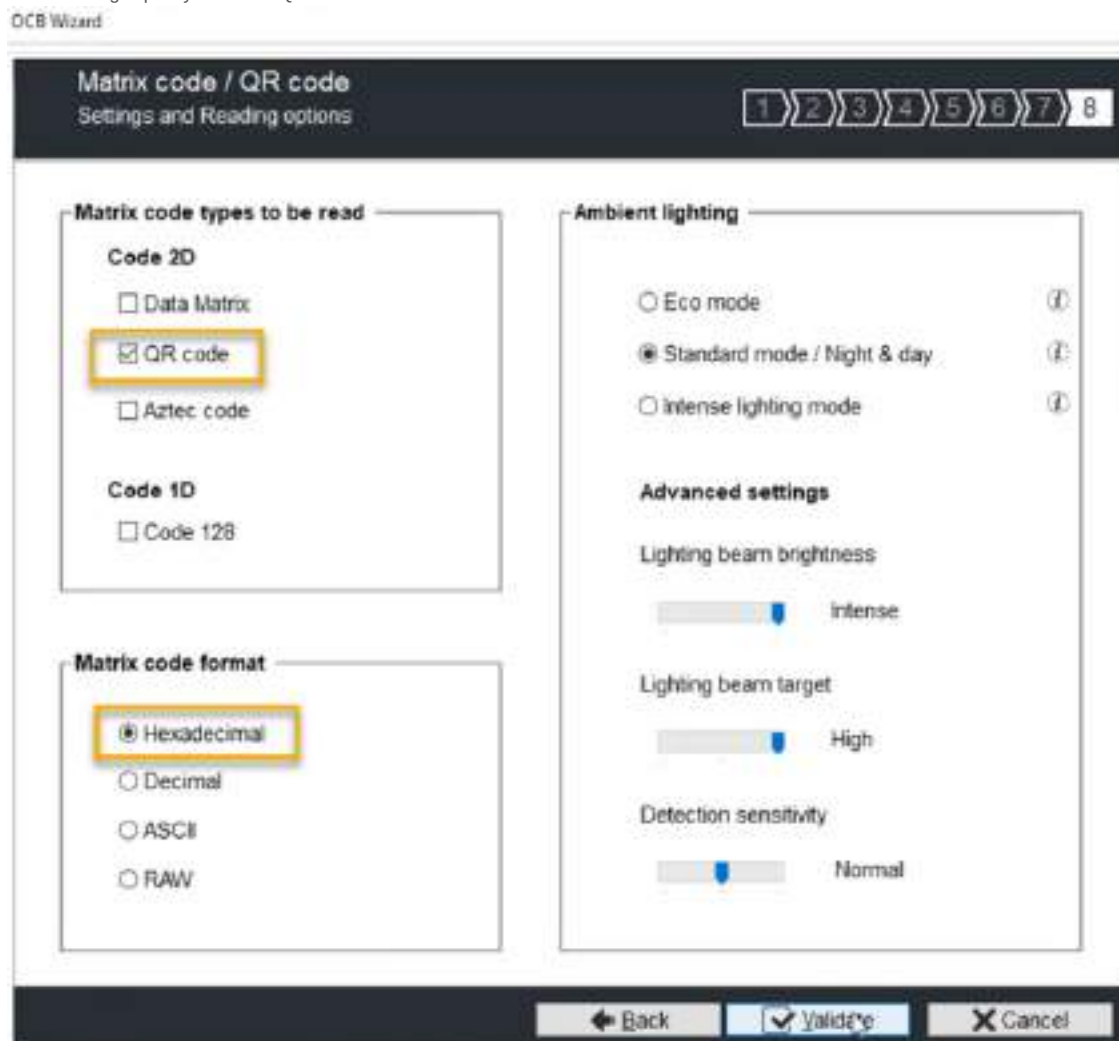


d. Click Next to skip the Blue/NFC Mobile ID options dialog.



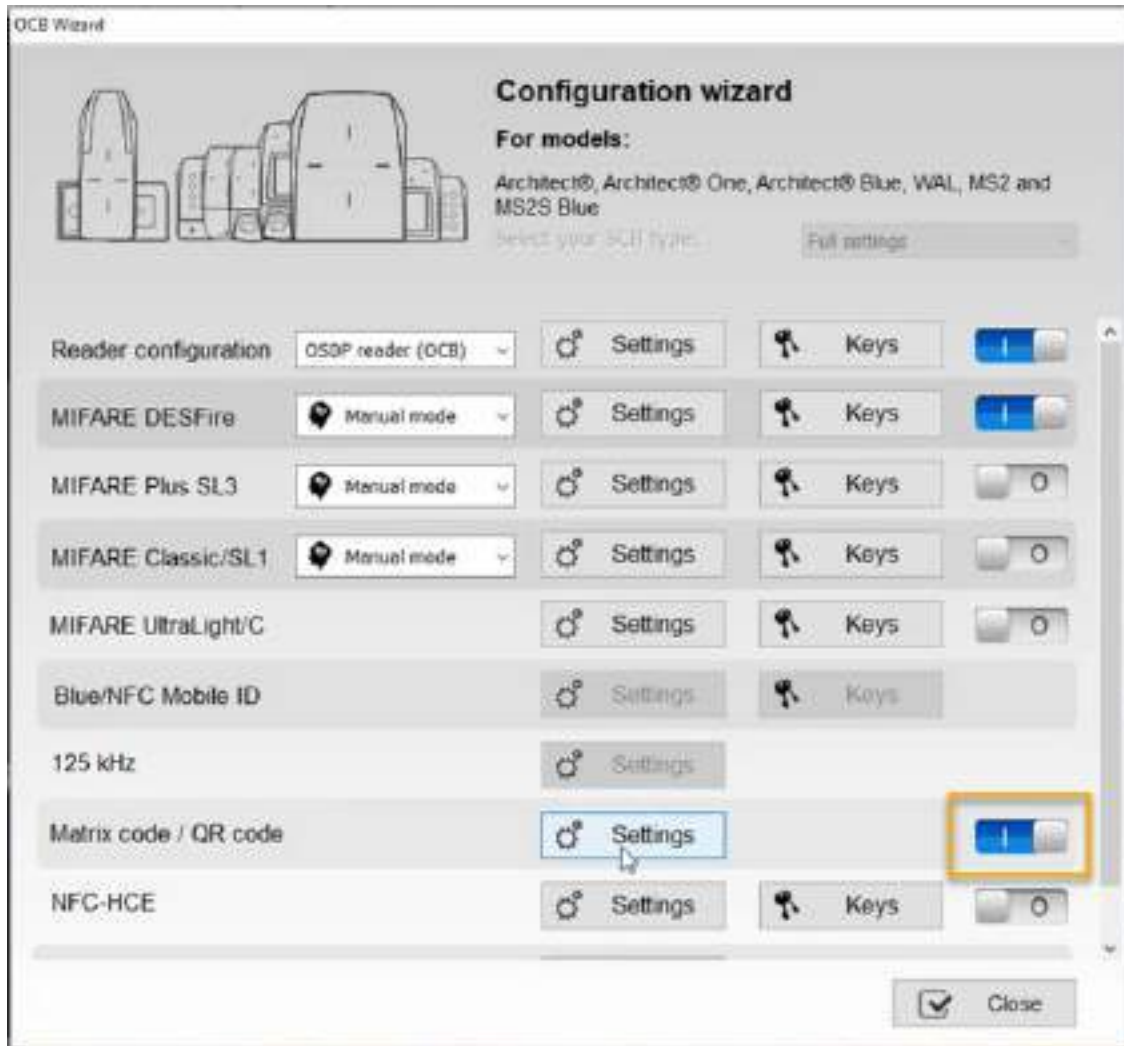
5. In the Matrix code types to be read section of the Matrix code / QR code dialog, select the QR code check box only. Then in the Matrix code format section, select the Hexadecimal check box.

These settings specify that a 2D QR code can be read and sent in hexadecimal format.



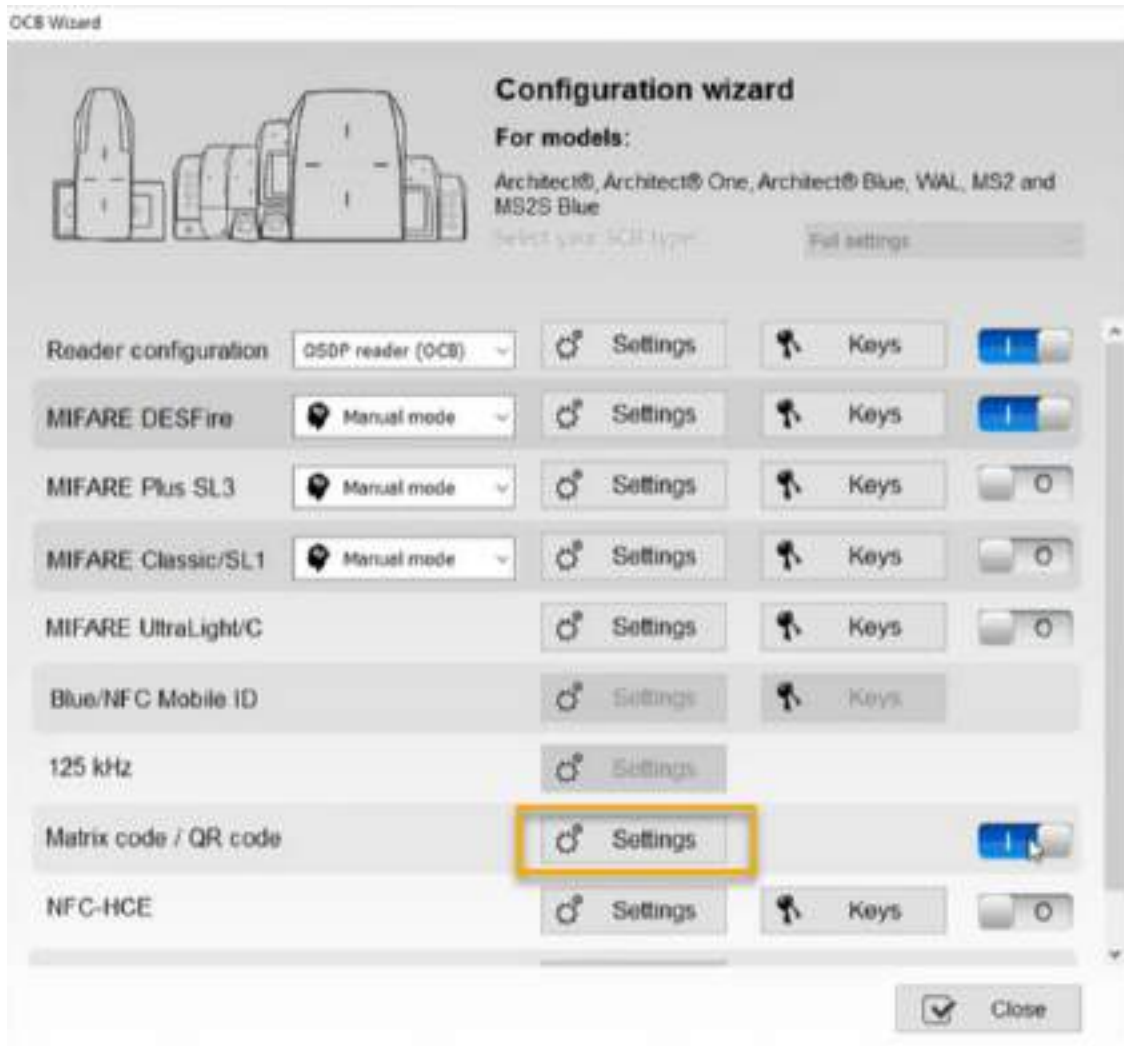
- a. (Optional) In the Ambient lighting section, modify the settings if required.
- b. Click Validate.

6. In the Matrix code / QR code row, drag the slider to the enabled position.



Tip: If the Matrix code / QR code section is not available for selection in the Configuration wizard, make sure that you have validated your Reader configuration as detailed earlier.

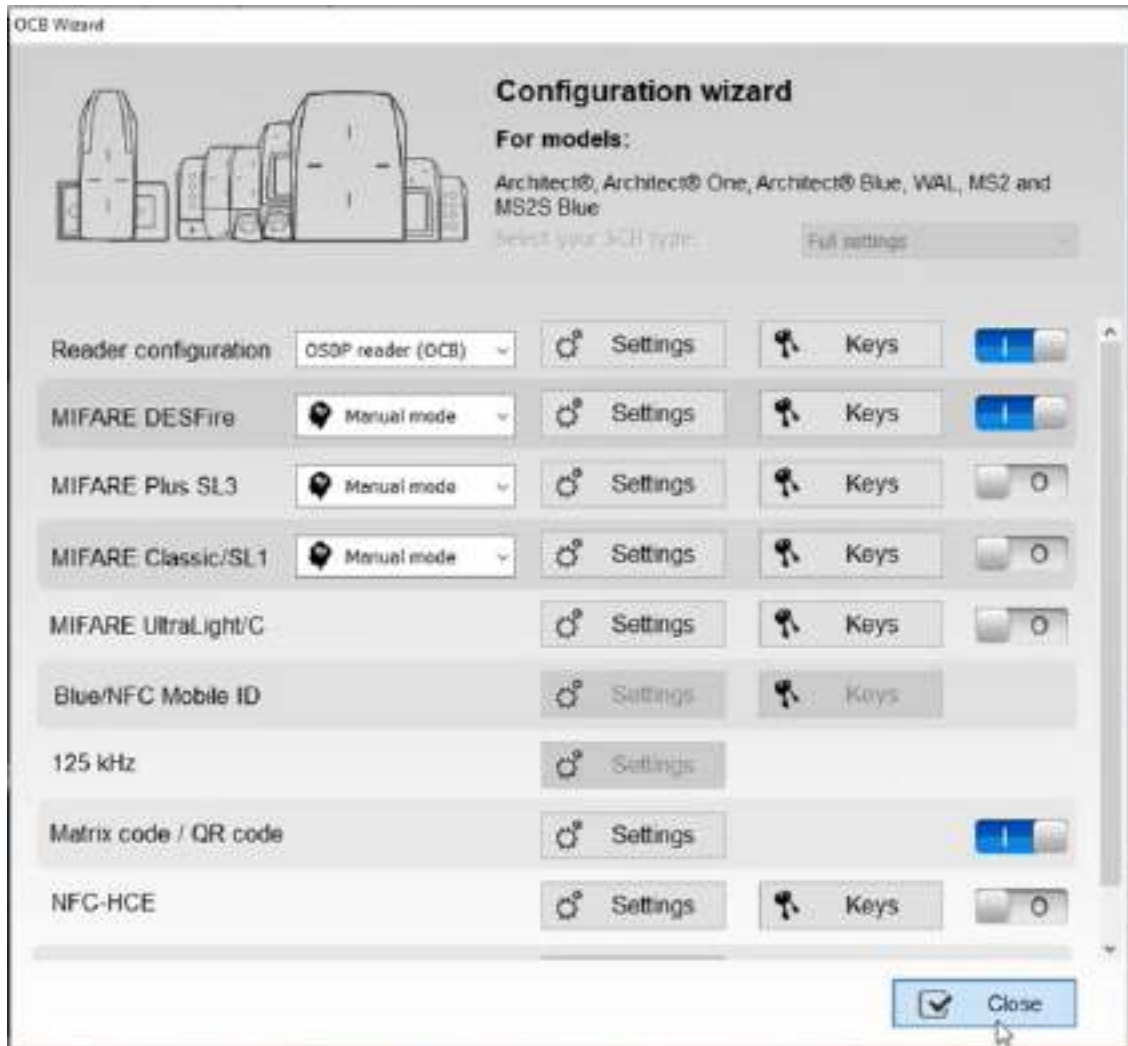
7. In the Matrix code / QR code row, click Settings.



a. In the Matrix code / QR code settings dialog, use the default settings and click Validate.



b. Click Close.



Results

Your STid QR code reader configuration has now been created.

After you finish

Transfer your reader configuration to your STid QR code reader.

Parent topic: Configuring STid devices for ClearID

9.13.4.3 | Transferring your reader configuration to your STid QR code reader for ClearID

QR codes as a credential for visitors in ClearID >

Before you can use QR codes as a credential in Genetec ClearID™, you must complete your STid QR code reader configuration by configuring an STid OCB smart card so that you can transfer the reader configuration to the STid QR code reader.

Before you begin

Familiarize yourself with the STid SECard documentation:

- SECard - High security programming kits
- SECard User Manual
- Install the STid SECard - High security programming kit software
- Create your STid QR code reader configuration

What you should know

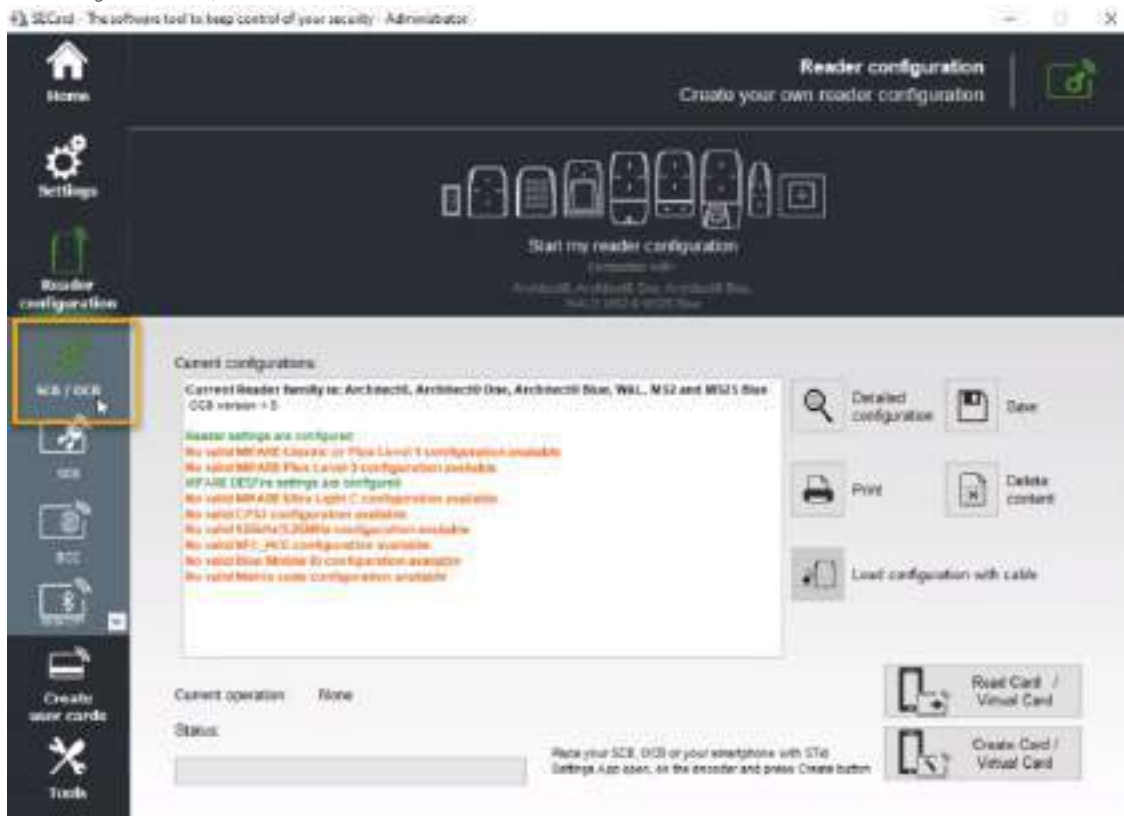
This procedure is for system integrators or account administrators who install and configure QR code readers.

NOTE: Ensure that you have a USB encoder installed and ready to configure your OCB card. For example, the STid Architect® ARC-G desktop reader, enroller, encoder.



Procedure

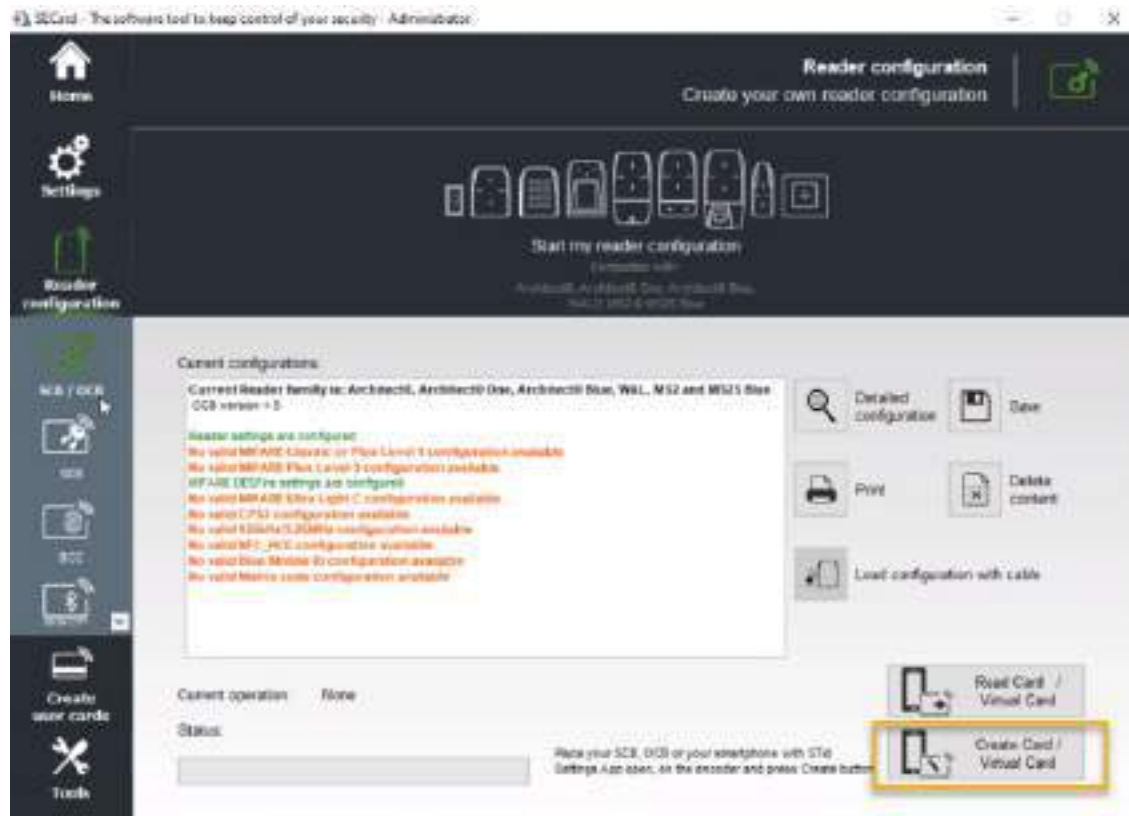
1. Launch the STid SECard software to configure your card.
2. In the navigation sidebar, click SCB / OCB.



3. Create your STid OCB card.
 - a. Place the OCB card on your USB encoder (reader).



- b. Click Create Card / Virtual Card to create your configuration card.

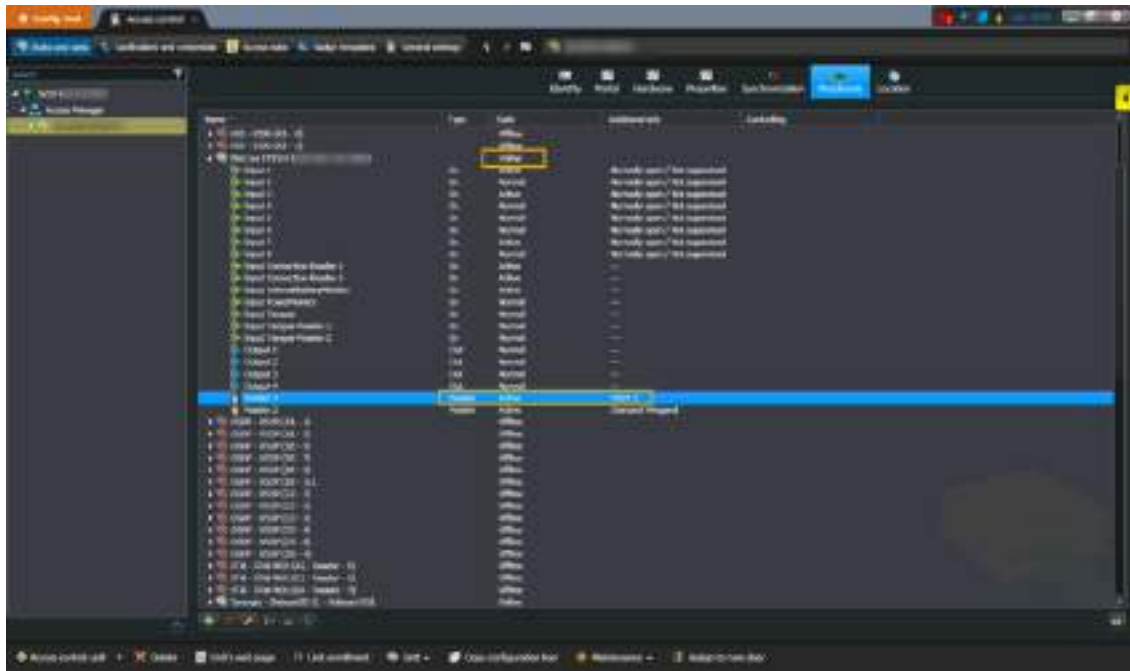


4. Take the OCB smart card containing your reader configuration to the location of your new QR code reader and pass the card in front of the reader.



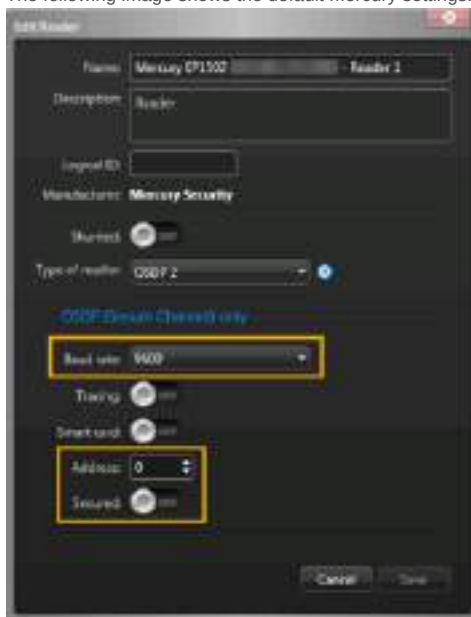
NOTE: Your new QR code reader must be online and available for the QR code reader to transfer the QR code reader configuration settings from the smart card to your QR code reader.

5. Verify your QR code reader is still active after the OCB has been swiped on the wall reader.
 - a. In Config Tool, open the Access control task.
 - b. In the Roles and units view, navigate to and select your access control unit.
 - c. In the Peripherals tab Name field, Select your OSDP reader.



- d. In the Peripheral tab Name field, verify that the ODSP reader State is Online.
- e. In the Peripheral tab Name field, verify that the Reader State is Active.
- f. Double-click your reader (Reader 1) in the Edit Reader dialog, make sure your settings match the reader settings.

The following image shows the default Mercury settings:



After you finish

Add doors to areas.

Parent topic: [Configuring STId devices for ClearID](#)

9.13.5 | Automating visitor access and check-in using a macro in Security Center

You can configure a Security Center macro to automatically check in and grant access to visitors at specified parking entrances or gated facilities. The macro can be used for visitors who need access to a parking entrance or gated facility before they can check in or at locations without self-service kiosks.

Before you begin

- Import a custom card format (QR code credential) in Synergis™
- Enable QR code credentials for visitors

What you should know

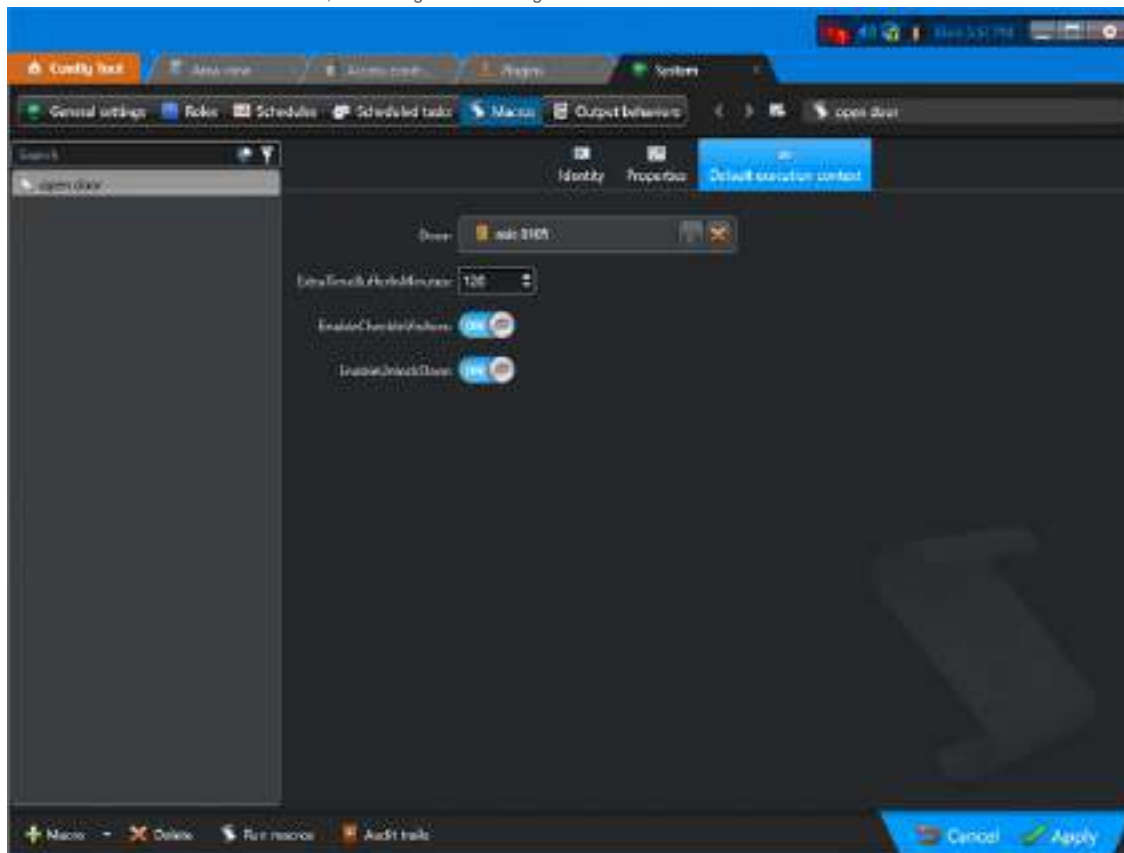
This macro is only for use when sites want to use a QR code as a credential to automate visitor check-in. The macro can grant access for a specified parking entrance or gated facility automatically before visitor check-in.



IMPORTANT: This procedure is only compatible with Security Center 5.11 and later.

Procedure

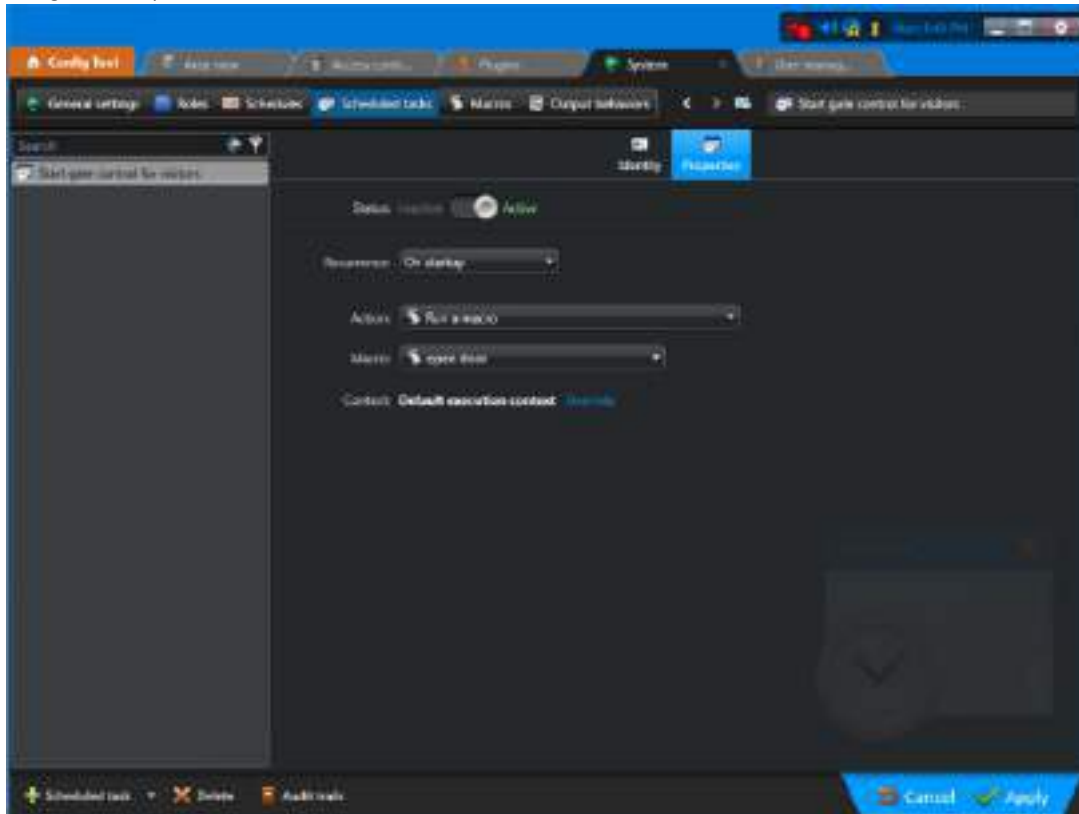
1. From the Config Tool homepage, open the System task and click the Macros view.
2. Click Macro (+), and enter the macro name.
3. Click the Properties tab, and do one of the following:
 - Cut and paste the Macro file code into the Macro definition (C#) section in the Properties tab.
 - Macro 1 (C# example) : Compatible with Security Center 5.7 SR4 - 5.11.2.
 - Macro 2 (C# example) : Compatible with Security Center 5.11.3 or later.
 - Import the source code from a file by clicking Import from file, select the file containing the C# code, and then click Open.
4. Click the Default execution context tab, and configure the settings as follows:



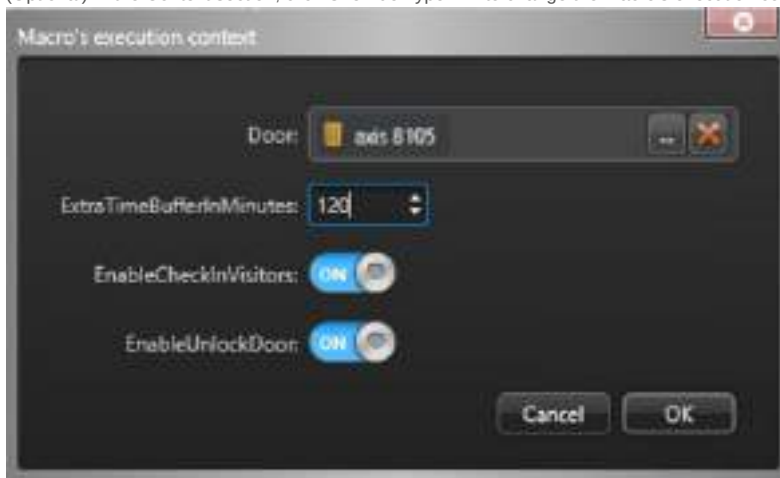
NOTE: The door selected in the Default execution context relates to a specific parking entrance or gated facility entrance. When a visitor presents their QR code, the macro is triggered to automatically provide access for this door only.

5. Click Apply.
6. Click Run macros.
7. From the Config Tool homepage, open the System task and click the Scheduled tasks view.

- a. Click Scheduled task (📅), and enter the scheduled task's name.
- b. Configure the Properties tab as follows:



- c. (Optional) In the Context section, click Override hyperlink to change the macro's execution context:



Results

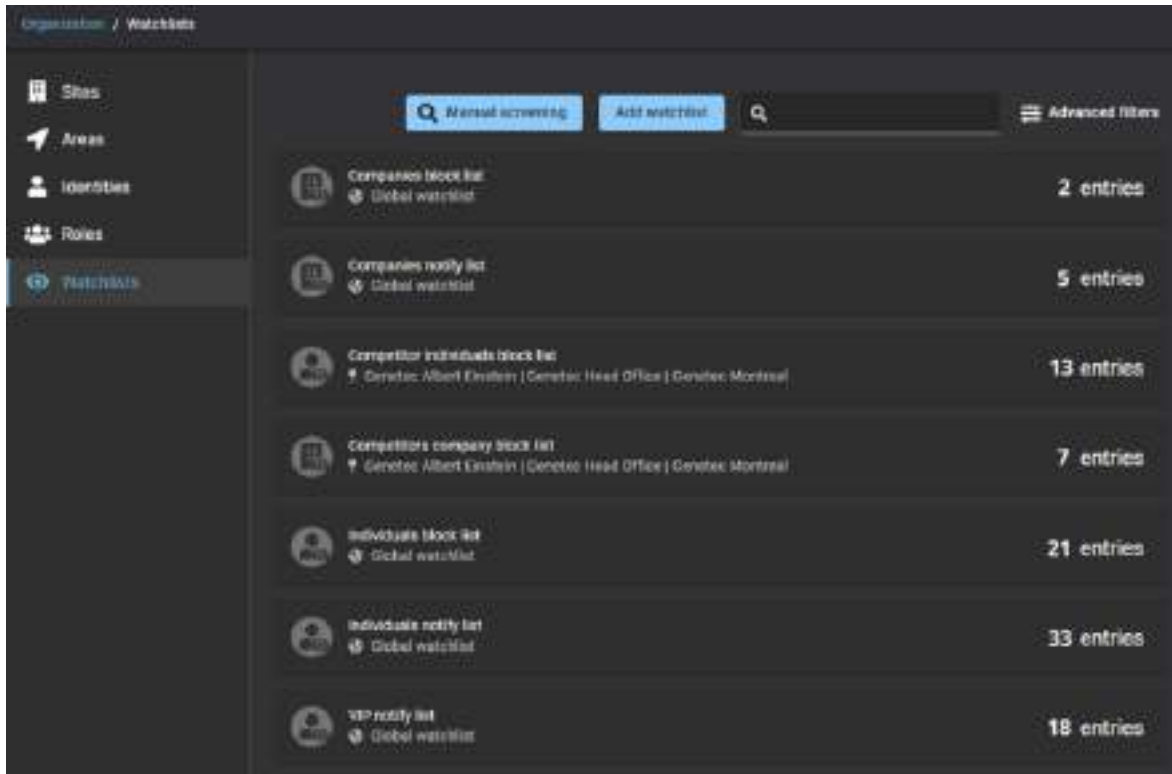
The Security Center macro is now configured. It can trigger automatic check-in and grant access to specific parking entrances or gated facilities when the relevant QR code is scanned at the entrance.

Parent topic: QR codes as a credential for visitors in ClearID

10 | Managing visitor watchlists

10.1 | About watchlists in ClearID

In Genetec ClearID™, watchlists are used to screen visitors at an individual or company level. You can configure the watchlist to perform allow, block, or notify actions at a site or global level.



Screening matches only occur when the following applies:

- Individuals: There is a First name and Last name match, First name and Last name alias match, or Email address match.
- Companies: There is a Company name, company domain, or email address domain match.

There are two types of watchlist:

- Individuals watchlist
- Companies watchlist



An Individuals watchlist is used to monitor visitor check-ins for *persons of interest* listed in a watchlist and then take action as specified in the watchlist configuration. For example, you might create an individuals watchlist to automatically block visitors listed in a watchlist and notify watchlist managers. For other situations, you might only notify watchlist managers. You might also create an individuals watchlist to notify all watchlist managers when VIPs check-in at your site.



A Companies watchlist is used to monitor visitor check-ins for *companies of interest* listed in a watchlist and then take action as specified in the watchlist configuration. For example, you might create a companies watchlist to automatically block access for people with a Company name, company domain, or email address domain that matches specific companies of interest listed in this watchlist.

NOTE: The *Individuals* or *Companies* listed in the entries inside a watchlist can be entered individually or imported as a whole using a .CSV file.

Watchlist behavior

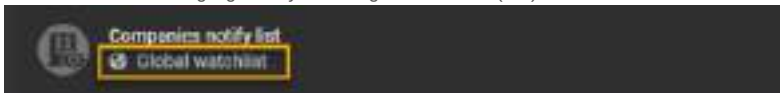
The behavior of the watchlists can be configured differently as follows:

- Notify watchlist managers.
- Automatically block visitors listed in a watchlist and notify watchlist managers.

Global watchlists

In Genetec ClearID™, a global watchlist is a watchlist that is enforced across all sites in your system.

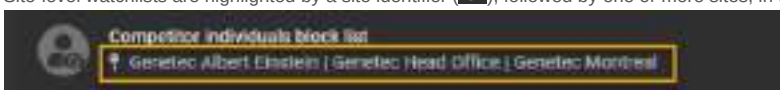
Global watchlists are highlighted by a world globe identifier (🌐) in the watchlist view as follows:



Site watchlists

If a watchlist is not configured as a *global watchlist*, it is considered a site-level watchlist and can be applied to one or more sites.

Site-level watchlists are highlighted by a site identifier (📍), followed by one or more sites, in the watchlist view as follows:



Reasons to block or notify

Reasons to block entry to visitors listed in a watchlist, or notify a watchlist manager might include one or more of the following:

- Serious criminal records by Government agency
- Violent activity or threats
- False Credentials
- Contraband items
- Theft
- Safety violation
- Other reasons

NOTE: Only a *watchlist manager* can view the reasons why visitors are in notify or block watchlists.

10.2 | Adding watchlist managers in ClearID

In Genetec ClearID™, a watchlist manager is an identity that is responsible for watchlists. A watchlist manager can create or modify watchlists and add individuals or companies to a watchlist. They are also responsible for configuring watchlists as a site-specific watchlist or a global watchlist. Before you can add or modify watchlists or configure watchlist settings, you must add your watchlist managers.

Before you begin

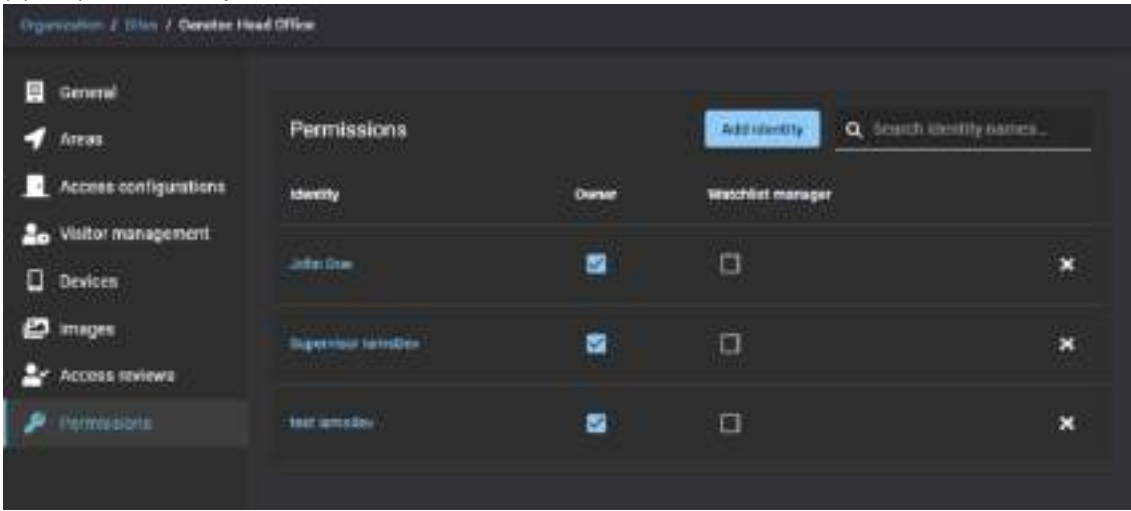
Create your sites.

What you should know

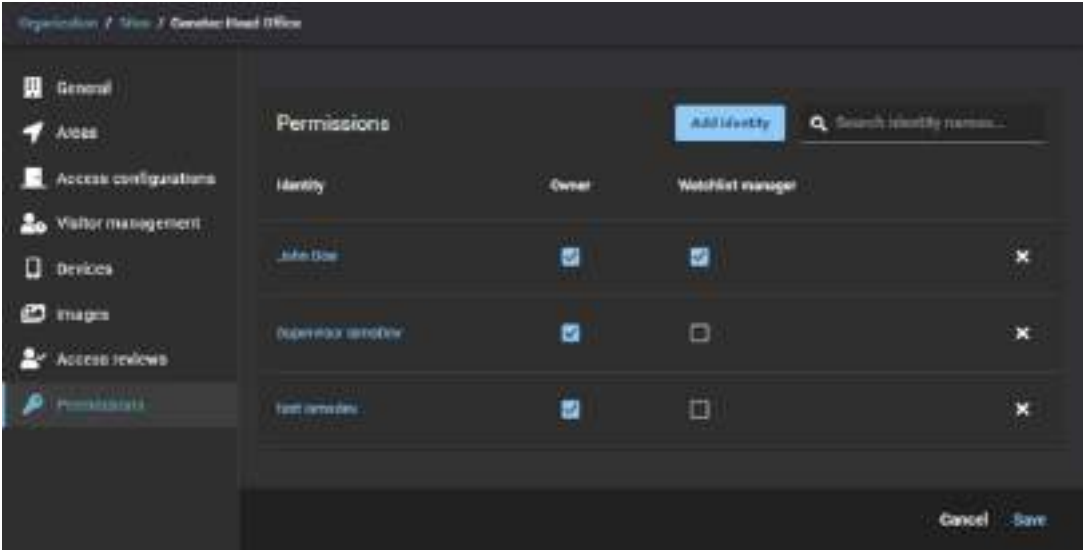
To add watchlist managers in Genetec ClearID™, you must be an account administrator.

Procedure

1. Click Organization > Sites.
2. Select your site and click Permissions.
3. (Optional) Click Add identity to add identities to the site Permissions list.



- a. Search for or select the identities that you require and click Add.
Tip: You can click the identity hyperlink in the Identity column to review identity details (company, department, home site, supervisor, and email) and to verify that you have the correct identities in the list.
4. Select the Watchlist manager check box to assign watchlist manager permissions to an identity.
 - a. (Optional) Clear a check box to remove individual permissions that are no longer required from an identity.
 - b. (Optional) Click  to remove all permissions that are no longer required from an identity.



5. Click Save.

After you finish

[Add your watchlists.](#)

10.3 | Adding watchlists in ClearID

Add individuals watchlists or companies watchlists so that you can screen visitors at an individual level or company level and automatically perform block or notify actions at a site or global level as specified in the watchlist configuration.

Before you begin

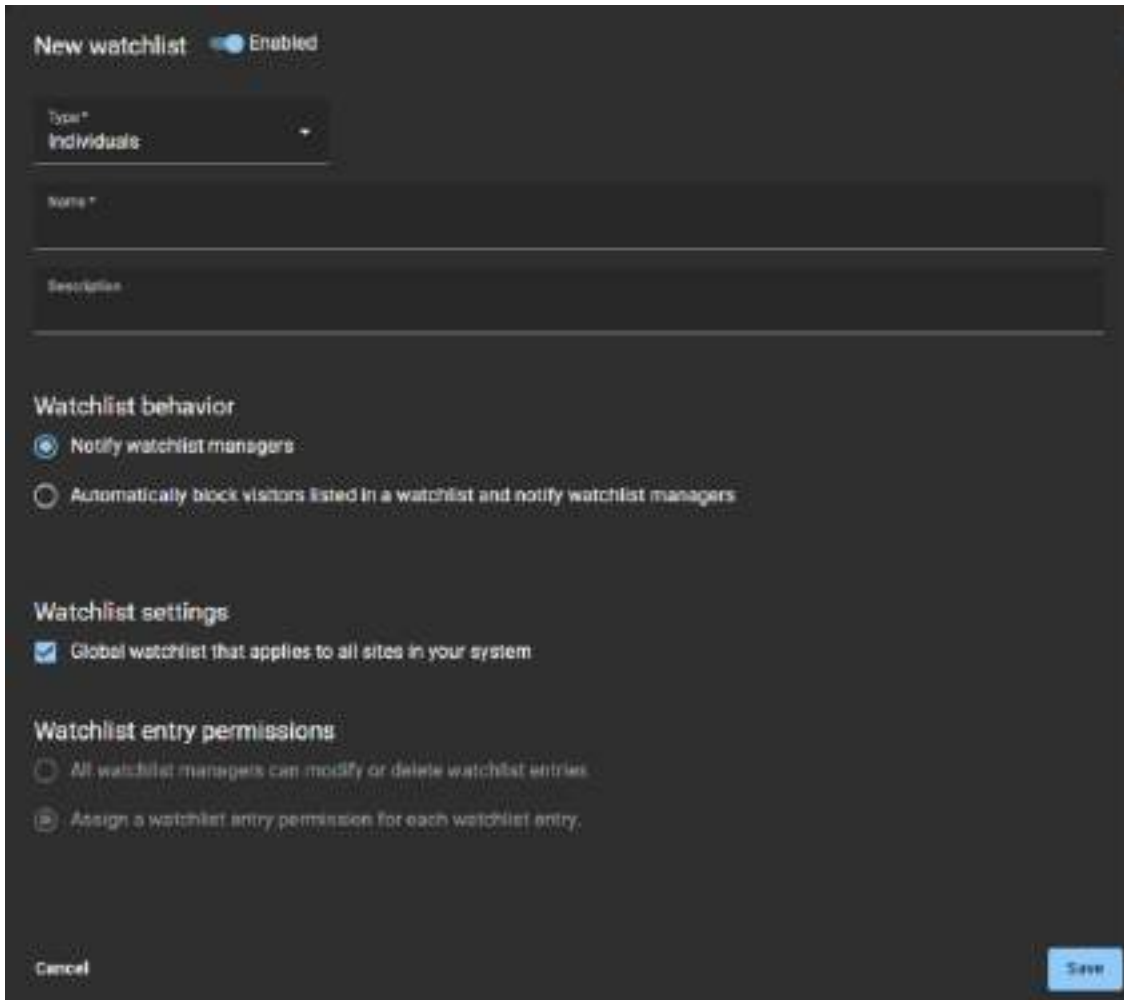
[Learn about watchlists.](#)

What you should know

- Any *watchlist manager* or account administrator can modify or delete any watchlist that is configured as a *global watchlist*.

Procedure

- Click Organization > Watchlists.
- Click Add watchlist.



3. At the top of the new watchlist, click the Enabled slider to enable or disable the watchlist.
4. In the Type field, select a watchlist type. From the list select either Individuals or Companies:

Individuals



An Individuals watchlist is used to monitor visitor check-ins for *persons of interest* listed in a watchlist and then take action as specified in the watchlist configuration. For example, you might create an individuals watchlist to automatically block visitors listed in a watchlist and notify watchlist managers. For other situations, you might only notify watchlist managers. You might also create an individuals watchlist to notify all watchlist managers when VIPs check-in at your site.

Companies



A Companies watchlist is used to monitor visitor check-ins for *companies of interest* listed in a watchlist and then take action as specified in the watchlist configuration. For example, you might create a companies watchlist to automatically block access for people with a Company name, company domain, or email address domain that matches specific companies of interest listed in this watchlist.

5. Enter a Name for the watchlist.
The name of a watchlist can be changed at any time to suit your needs.
Tip: Consider using a *discreet name* where applicable to avoid divulging sensitive information about why someone might be blocked or on a list when the notification is sent to people.
6. Enter a Description for the watchlist.
7. In the Watchlist behavior section, select one of the following:
 - o Notify watchlist managers
 - o Automatically block visitors listed in a watchlist and notify watchlist managers
8. In the Watchlist settings section, choose whether you want a global watchlist or a site-specific watchlist.
 - o To apply the watchlist to all sites in your system, select Global watchlist that applies to all sites in your system.
 - o To apply the watchlist to one or more specific sites, clear the Global watchlist that applies to all sites in your system check box.
 - a. If you chose to apply your watchlist at a site-level, add your sites and press enter.
 - b. Repeat at necessary.

NOTE: The Watchlist entry permissions section is disabled if the Global watchlist that applies to all sites in your system check box is selected.
9. If you have Watchlist entry permissions activated for your account, in the Watchlist entry permissions section, select one of the following:
 - o All watchlist managers can modify or delete watchlist entries.
 - o Assign a watchlist entry permission for each watchlist entry

All watchlist managers can modify or delete watchlist entries

Specifies that watchlist entries can only be modified or deleted by all watchlist managers for the specified sites.

Assign a watchlist entry permission for each watchlist entry

Specifies that watchlist entry permissions are assigned at a more granular site level in each watchlist entry. This means that only watchlist managers for the site can modify or delete entries.

Example 1: Individuals block watchlist - configured as a global watchlist to automatically block visitors and notify watchlist managers.

The screenshot shows the 'New watchlist' configuration interface. At the top, the title 'New watchlist' is followed by a toggle switch labeled 'Enabled'. Below this, there are three input fields: 'Type' with a dropdown menu showing 'Individuals', 'Name' with the text 'Individuals BLOCK list', and 'Description' with the text 'Automatic block GLOBAL watchlist all sites'. The 'Watchlist behavior' section contains two radio button options: 'Notify watchlist managers' and 'Automatically block visitors listed in a watchlist and notify watchlist managers', with the latter being selected. The 'Watchlist settings' section has a checked checkbox for 'Global watchlist that applies to all sites in your system'. The 'Watchlist entry permissions' section contains two radio button options: 'All watchlist managers can modify or delete watchlist entries' and 'Assign a watchlist entry permission for each watchlist entry', with the latter being selected. At the bottom left is a 'Cancel' button, and at the bottom right is a 'Save' button.

New watchlist ☒ Enabled

Type *
Individuals

Name *
Individuals BLOCK list

Description
Automatic block GLOBAL watchlist all sites

Watchlist behavior

☐ Notify watchlist managers

☒ Automatically block visitors listed in a watchlist and notify watchlist managers

Watchlist settings

☒ Global watchlist that applies to all sites in your system

Watchlist entry permissions

☐ All watchlist managers can modify or delete watchlist entries

☒ Assign a watchlist entry permission for each watchlist entry

Cancel Save

Example 2: Companies notify watchlist - configured as a site-specific watchlist to notify watchlist managers when visitors are from a competitors company.

New watchlist ☒ Enabled

Type*
Companies

Name*
Companies NOTIFY list

Description
Notify when visitors from Competitor company visit specific sites

Watchlist behavior

☒ Notify watchlist managers

☐ Automatically block visitors listed in a watchlist and notify watchlist managers

Watchlist settings

☐ Global watchlist that applies to all sites in your system

Watchlist sites

Genetec Albert Einstein Genetec Head Office Genetec Marinsol **Add more** To add a site, start typing and press Enter

Watchlist entry permissions

☒ All watchlist managers can modify or delete watchlist entries

☐ Assign a watchlist entry permission for each watchlist entry.

Cancel Save

10. Click Save.

Example

Ocorreu um erro.

[Tente assistir o vídeo em www.youtube.com](http://www.youtube.com) ou ative o JavaScript caso ele esteja desativado em seu navegador.

After you finish

Do one or more of the following:

- [Add your individuals watchlist entries](#)
- [Add your companies watchlist entries](#)

10.3.1 | Adding an individuals watchlist entry in ClearID

Add one or more individuals watchlist entries so that you can screen visitors at an individual level and automatically perform block or notify actions at a site or global level as specified in the watchlist configuration.

Before you begin

[Add your watchlists.](#)

What you should know

Only a *watchlist manager* can:

- Add individuals watchlist entries.
- View reasons why visitors are in notify or block watchlists.

Procedure

1. Click Organization > Watchlists.
2. Select a watchlist from the list.
3. Click Add entry.

Individual ☒ Enabled

Watchlist entry criteria

First name * Middle name Last name *

First name aliases
To add an alias, start typing and press Enter

Last name aliases
To add an alias, start typing and press Enter

Emails
To add an email, start typing and press Enter

Emails to always allow

Emails
To add an email, start typing and press Enter

Additional information

Physical description

Location

Add Image

Date of birth
MM/DD/YYYY

External reference ID

Company name

Permissions

This entry can only be modified or deleted by the watchlist manager for the following sites

Sites with watchlist entries that can be modified or deleted
To add a site, start typing and press Enter

Cancel Save

4. At the top of the watchlist entry click the Enabled slider to enable or disable the watchlist entry.

5. In the Watchlist entry criteria section, complete the fields:

First name

Enter a first name.

Middle name

Enter a middle name.

Last name

Enter a last name.

First name aliases

Add any known first name aliases and press enter. Repeat as required.

NOTE: Aliases are shown in brackets in the watchlist entries list.

Last name aliases

Add any known last name aliases and press enter. Repeat as required.

Emails

Add any known emails and press enter. Repeat as required.

Genetec ClearID™ User Guide

Displayed in the header

6. In the Emails to always allow section, add any emails that you want to exclude from the watchlist screening process.

This section is used to add any similar emails or false positive email matches that you might want to always allow. For example, a possible match that happens to have the same name details, but is a different person with a different email address that should be allowed.

7. In the Additional information section, complete any additional fields that you require:

Physical description

Enter a physical description.

Reason

Enter a reason for the block or notify.

NOTE: The Reason field can contain sensitive private information, and can only be viewed by the watchlist manager for the site.

Date of birth

Use the calendar picker to enter a date of birth.

The date of birth information is useful additional information when a visitor check-in matches multiple people with the same name. It can be used to validate an identity and also eliminate duplicates or false positive matches.

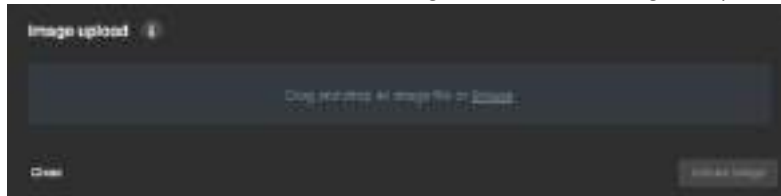
External reference ID

Enter an external reference ID.

Company name

Enter a company name.

8. In the Additional information section, Click Add image to add one or more images if required.



a. Drag and drop an image or click Browse to select the image file that you require and click Upload image.

b. Repeat for each additional image you want to upload.

c. (Optional) Click Delete image for any images you no longer require.

Tip: Click Open in new tab to view the image full size.

9. If you have Watchlist entry permissions activated for your account, in the Permissions section, add the sites that you require.

10. Click Save.

Example



After you finish

Test your watchlist entries.

Parent topic: [Adding watchlists in ClearID](#)

10.3.2 | Adding a companies watchlist entry in ClearID

Add one or more companies watchlist entries so that you can screen visitors at a company level and automatically perform block or notify actions at a site or global level as specified in the watchlist configuration.

Before you begin

Add your watchlists.

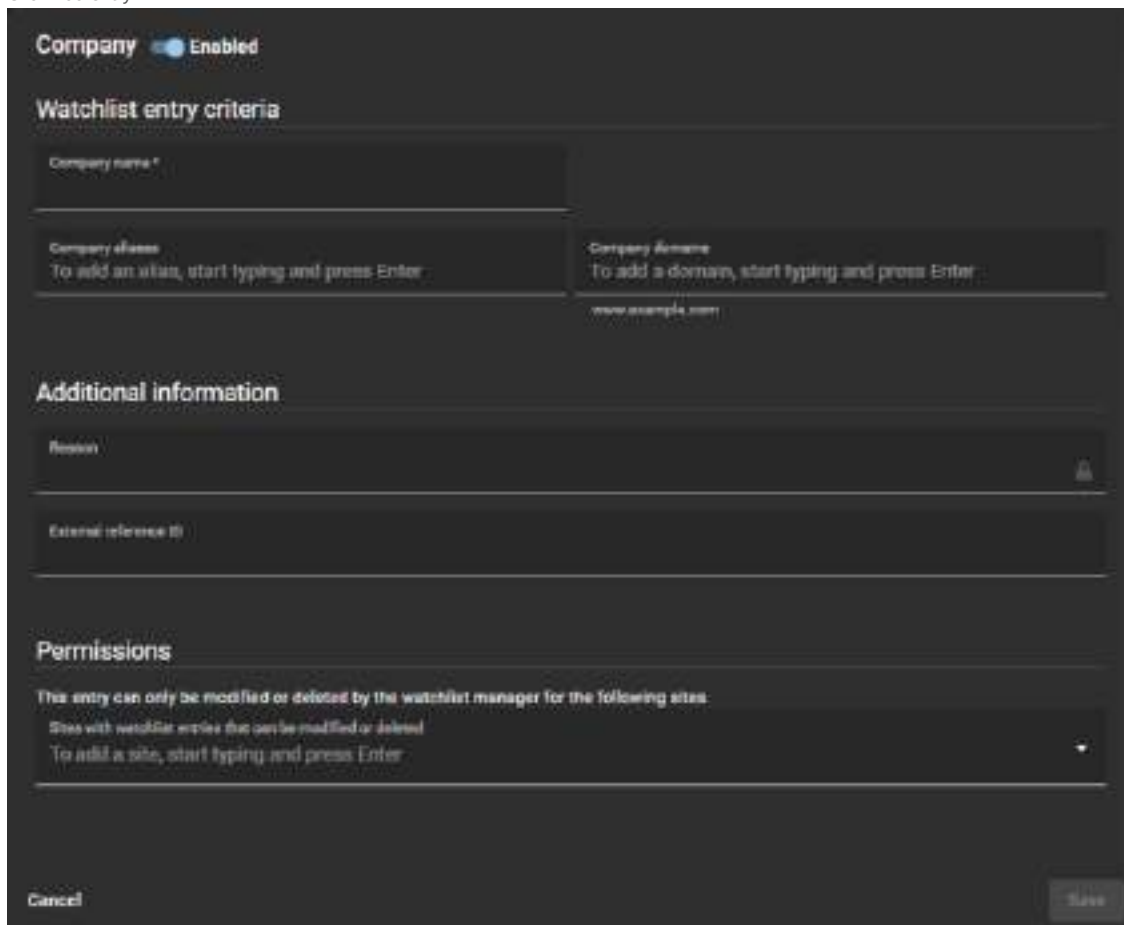
What you should know

Only a *watchlist manager* can:

- Add companies watchlist entries.
- View reasons why visitors are in notify or block watchlists.

Procedure

1. Click Organization > Watchlists.
2. Select a watchlist from the list.
3. Click Add entry.

The screenshot shows a web interface for adding a watchlist entry. At the top, there's a 'Company' section with an 'Enabled' toggle switch. Below this is the 'Watchlist entry criteria' section, which includes a 'Company name' field, a 'Company aliases' field with a hint 'To add an alias, start typing and press Enter', and a 'Company domains' field with a hint 'To add a domain, start typing and press Enter' and the example 'www.example.com'. The 'Additional information' section has a 'Reason' field with a help icon and an 'External reference ID' field. The 'Permissions' section states 'This entry can only be modified or deleted by the watchlist manager for the following sites' and includes a list of sites with a hint 'To add a site, start typing and press Enter'. At the bottom, there are 'Cancel' and 'Save' buttons.

4. At the top of the watchlist entry click the Enabled slider to enable or disable the watchlist entry.
5. In the Watchlist entry criteria section, complete the fields:

Company name

Enter a company name.

Company aliases

Add any known company aliases and press enter. Repeat as required.

NOTE: Aliases are shown in brackets in the watchlist entries list.

Company domains

Add any known company domains and press enter. Repeat as required.

6. In the Additional information section, complete any additional fields that you require:

Reason

Enter a reason for the block or notify.

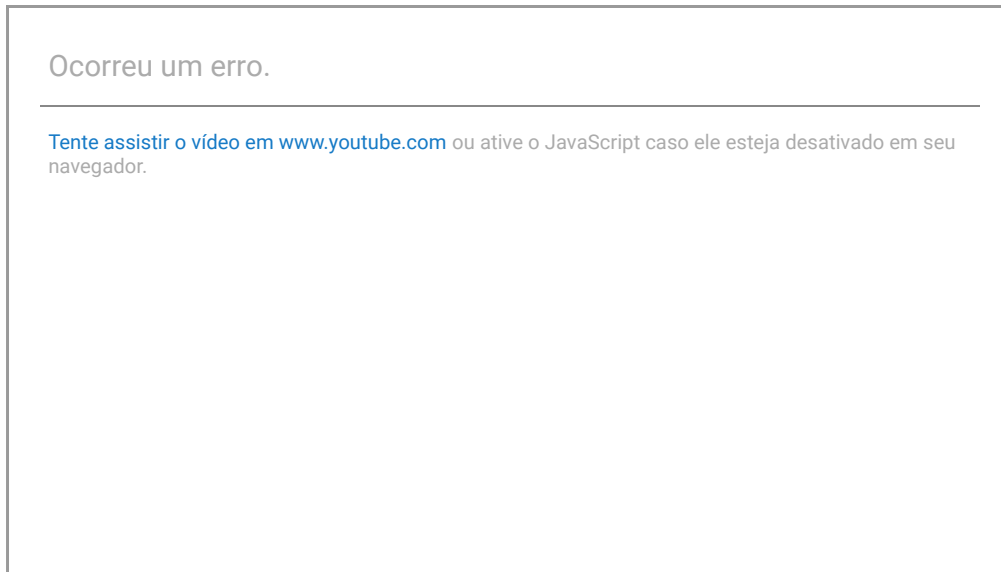
NOTE: The Reason field can contain sensitive private information, and can only be viewed by the watchlist manager for the site.

External reference ID

Enter an external reference ID.

7. If you have Watchlist entry permissions activated for your account, in the Permissions section, add the sites that you require.
8. Click Save.

Example



After you finish

Test your watchlist entries.

Parent topic: [Adding watchlists in ClearID](#)

10.3.3 | Importing watchlist entries from a file in ClearID

To accelerate your watchlist configuration and setup, you can import your watchlist entries from a .CSV file. You can also download a sample .CSV file to help you prepare your watchlist entries file in the correct format.

Before you begin

Prepare your watchlist entries in a .CSV file, ready for import.

What you should know

Only a *watchlist manager* can import watchlist entries.

You can import pre-existing watchlist entry data using a .CSV file from one or more of the following sources:

- Sharepoint
- Excel
- Be on (the) look-out (BOLO) list - a watchlist term typically used in the field of policing.
- No entry list
- Deny entry list (DEL)

Procedure

1. Click Organization > Watchlists.
2. Select a watchlist.
3. Click  and click Import from file.

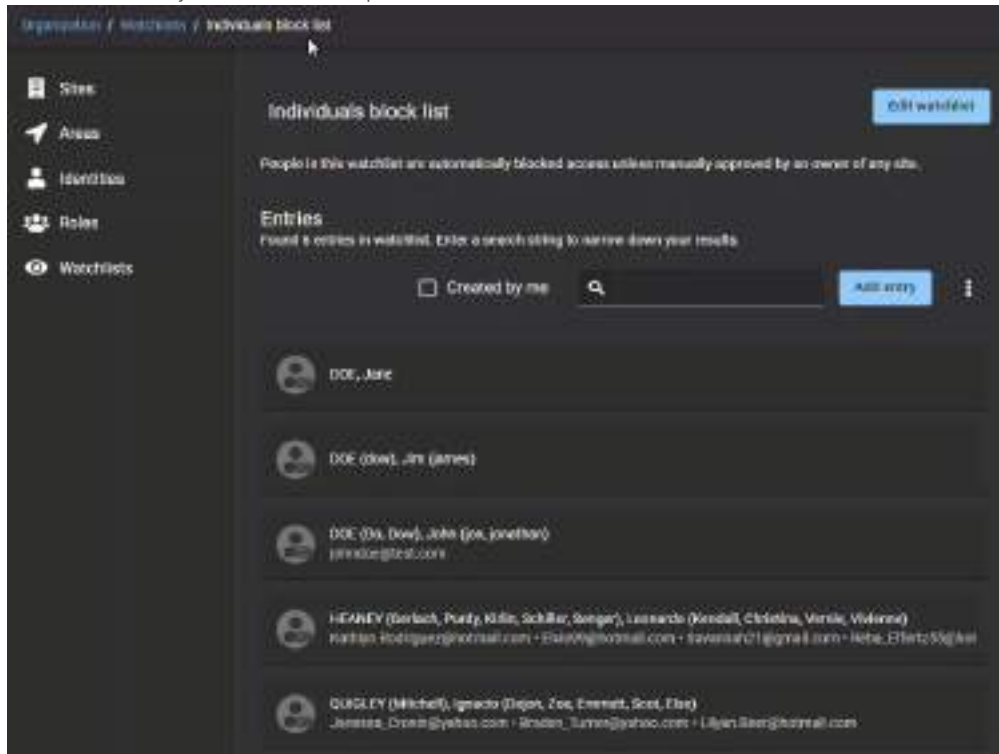


4. (Optional) Click Download a sample CSV file to help you prepare a watchlist entries file in the correct format.

Genetec ClearID™ User Guide

Displayed in the header

NOTE: The columns and entries in the sample CSV file (watchlist-sample.csv) can vary depending on the watchlist type (Individuals or Companies) you have selected when you download the sample.

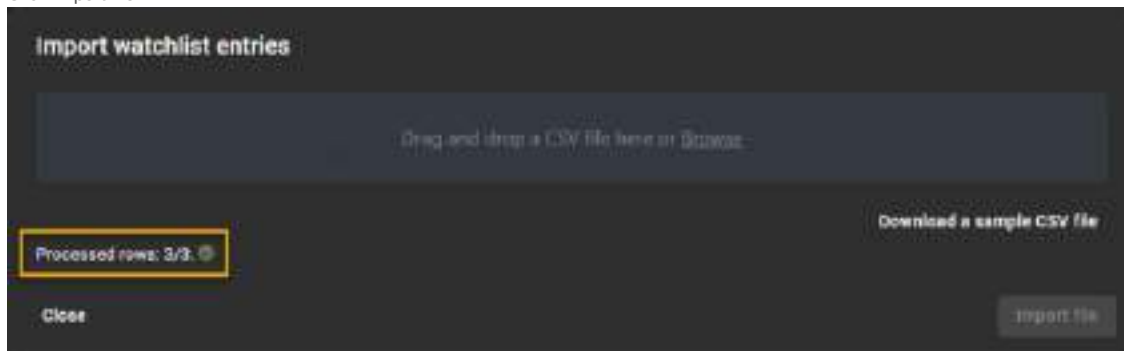


Tip: Click the animation to view full size.

5. In the Import watchlist entries dialog, drag and drop a CSV file or click Browse to select a file.



6. Click Import file.



NOTE: The Processed rows field in the Import watchlist entries dialog indicates how many watchlist entries have been processed.

After you finish

Test your watchlist entries.

Parent topic: Adding watchlists in ClearID

10.3.4 | Exporting watchlist entries to a file in ClearID

You can export your watchlist entries to a .CSV file for mass editing or backup purposes. For example, you could export your watchlist entries to Microsoft Excel, edit the entries, remove any duplicates, and then merge watchlists or consolidate watchlist entries into a new watchlist.

Before you begin

Do one or more of the following:

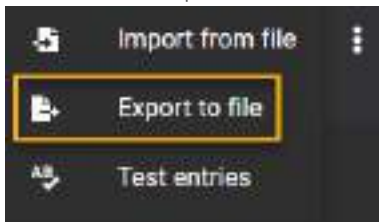
- [Add your individuals watchlist entries.](#)
- [Add your companies watchlist entries.](#)
- [Import your watchlist entries.](#)

What you should know

Only a *watchlist manager* can export watchlist entries.

Procedure

1. Click Organization > Watchlists.
2. Select a watchlist.
3. Click  and click Export to file.



The file is exported as a .CSV file to your browsers default download location. By default the exported file is created using the name of your watchlist. For example, Individuals block list.csv.

4. Follow your browser prompts to complete downloading the exported file.

After you finish

(Optional) Manipulate the watchlist entry data as required.

Parent topic: [Adding watchlists in ClearID](#)

10.3.5 | Testing watchlist entries in ClearID

To test new watchlist entries, you can enter the details of a person of interest or a company of interest to verify if there is a screening match.

Before you begin

Do one or more of the following:

- [Add individuals watchlist entries](#)
- [Add companies watchlist entries](#)

What you should know

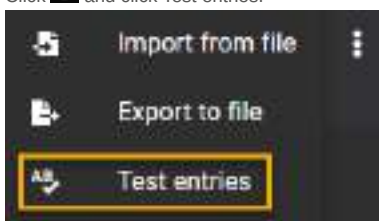
Only a *watchlist manager* can test watchlist entries.

Screening matches only occur when the following applies:

- Individuals: There is a First name and Last name match, First name and Last name alias match, or Email address match.
- Companies: There is a Company name, company domain, or email address domain match.

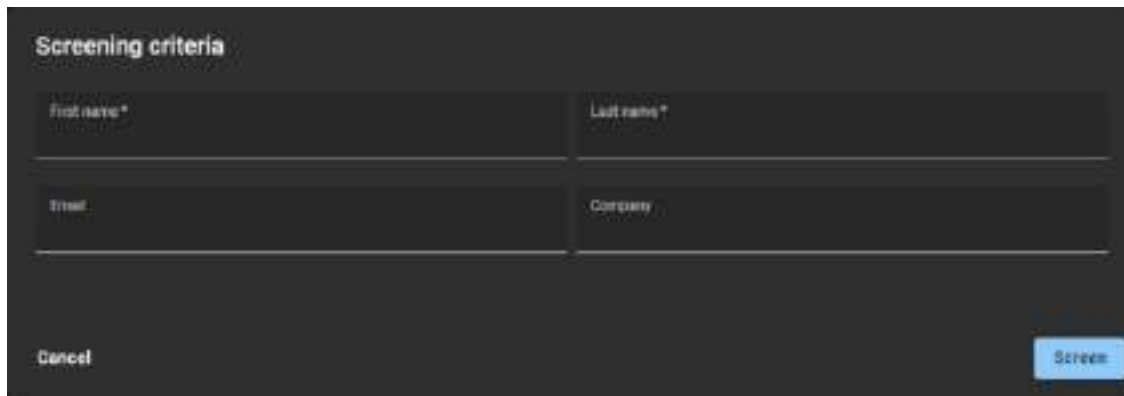
Procedure

1. Click Organization > Watchlists.
2. Select a watchlist.
3. Click  and click Test entries.



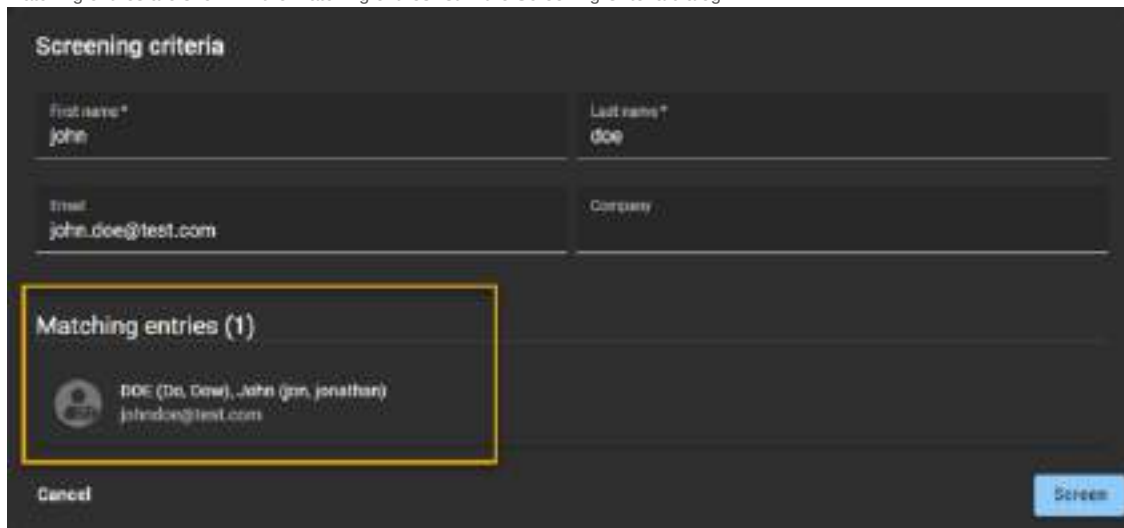
4. In the Screening criteria dialog, enter the details of the entry that you want to test

NOTE: Mandatory fields are highlighted by an asterisk (*).



5. Click Screen.

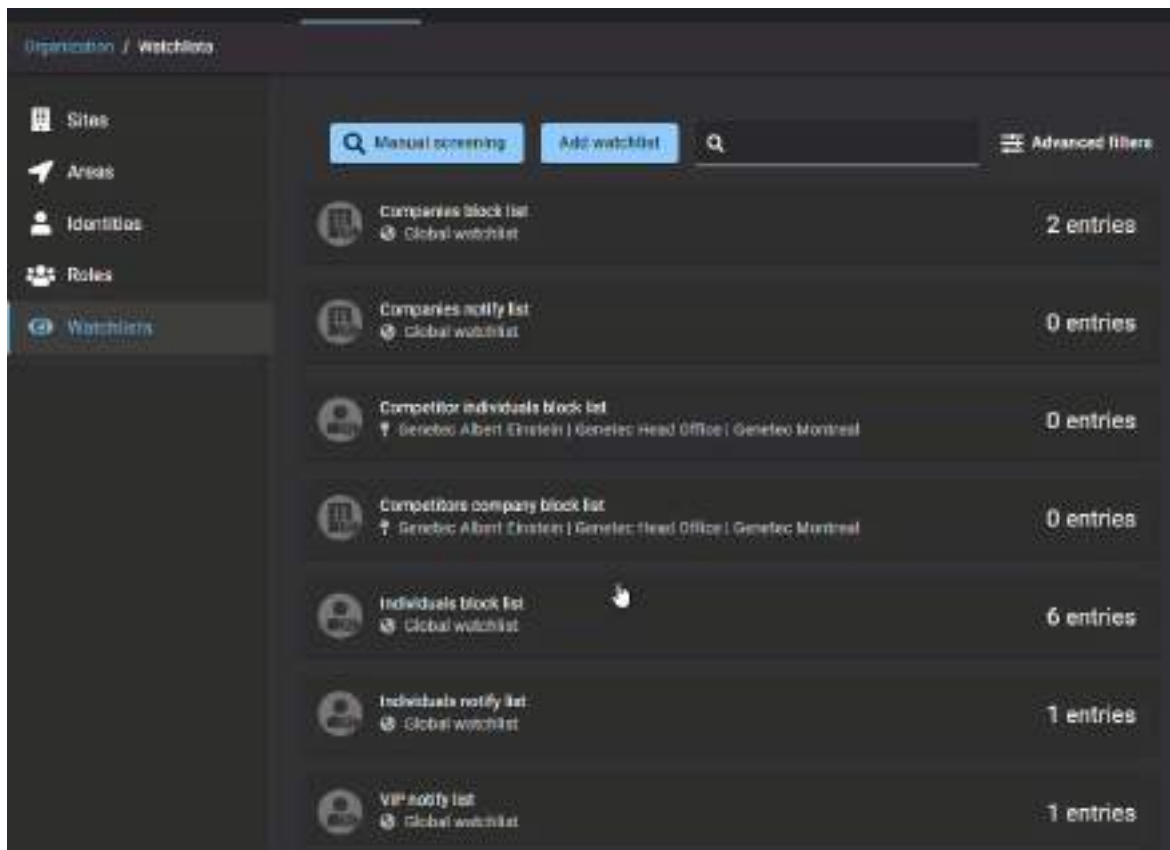
Matching entries are shown in the Matching entries list in the Screening Criteria dialog.



6. (Optional) Click a matching entry in the list to view the complete details of the watchlist entry.

7. Click Cancel to exit the Screening Criteria dialog.

Example



Parent topic: Adding watchlists in ClearID

10.3.6 | Deleting watchlist entries in ClearID

A watchlist manager can delete individuals watchlist entries or companies watchlist entries that have become obsolete or are no longer required.

Before you begin

Do one or more of the following:

- Add individuals watchlist entries
- Add companies watchlist entries

What you should know

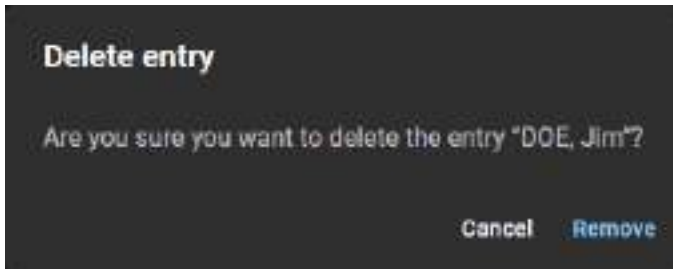
A watchlist entry can only be deleted by the *watchlist manager* who created it.

Procedure

1. Click Organization > Watchlists.
2. Select a watchlist from the list.
3. (Optional) If the watchlist entries list is long, select Created by me to reduce the displayed results.
4. Do one of the following:
 - Click to select a watchlist entry in the list
 - Search for the entry that you want to delete.
5. Scroll to the bottom of the watchlist entry and click Delete entry.

The screenshot shows a 'Delete entry' dialog box for an individual. At the top left, it says 'Individual' with a toggle switch set to 'Enabled'. At the top right is a red 'Delete entry' button. The main section is titled 'Watchlist entry criteria' and contains three input fields: 'First name *' with the value 'Jim', 'Middle name', and 'Last name *' with the value 'Doe'. Below these are two sections for aliases: 'First name aliases' and 'Last name aliases', each with a text input field and a 'done' button. There are also sections for 'Emails' and 'Emails to always allow', each with a text input field. The 'Additional information' section at the bottom includes a profile picture of a man with a beard, a 'Physical description' field, a 'Reason' field, a 'Date of birth' field with a calendar icon, an 'External reference ID' field, and a 'Company name' field. At the bottom left is a 'Cancel' button and at the bottom right is a 'Save' button.

6. In the Delete entry dialog, click Remove to confirm your deletion.



Parent topic: [Adding watchlists in ClearID](#)

10.4 | Modifying watchlists in Genetec ClearID

After you add your watchlists, you can modify some of the watchlist settings. A watchlist manager can disable a watchlist, change the Name or Description, and change watchlist behavior.

Before you begin

[Add your watchlists.](#)

What you should know

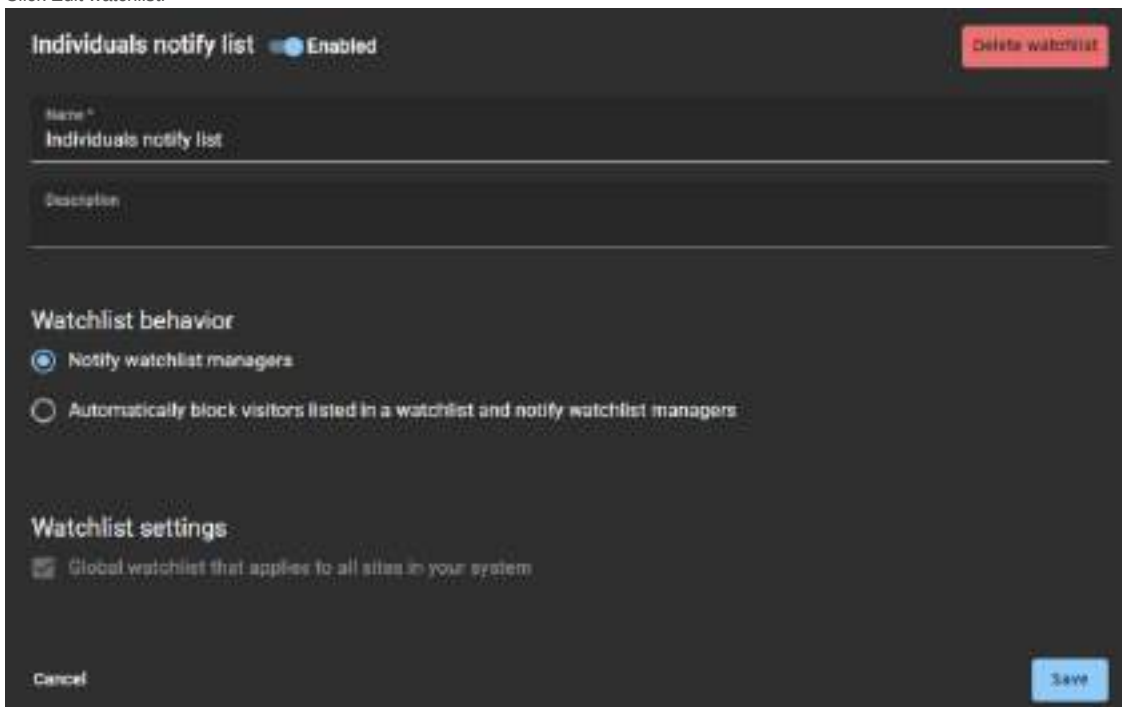
When modifying a watchlist the following applies:

- You cannot change a *global watchlist* to become a *site watchlist*.
- You cannot change a *site watchlist* to become a *global watchlist*.
- You cannot modify Watchlist entry permissions after a watchlist is created.

Any *watchlist manager* or account administrator can modify any watchlist that is configured as a *global watchlist*.

Procedure

1. Click Organization > Watchlists.
2. (Optional) Use the search box to find a specific watchlist.
3. (Optional) Click Advanced filters to filter the list results by Site or Watchlist type.
Select the filter options that you require:
 - a. From the Site list, select a site.
 - b. From the Watchlist types list, select a watchlist type.
 - c. Click Close.
4. Select a watchlist from the list.
5. Click Edit watchlist.



6. Modify the watchlist as required by doing one or more of the following:
 - a. At the top of the Watchlist dialog, click the Enabled slider to enable or disable the watchlist.

For example, you might want to disable a large watchlist and refer to it while restructuring entries into other watchlists.

b. In the Name field, change the watchlist Name.

c. In the Description field, change the watchlist Description.

d. In the Watchlist behavior section, modify the Watchlist behavior. Select either Notify watchlist managers or Automatically block visitors listed in a watchlist and notify watchlist managers.

7. Click Save.

10.5 | Deleting watchlists in Genetec ClearID

A watchlist manager can delete watchlists that have become obsolete or are no longer required. Or a watchlist might need to be deleted in situations where you need to change a *site watchlist* to a *global watchlist* or vice versa.

Before you begin

Add your watchlists.

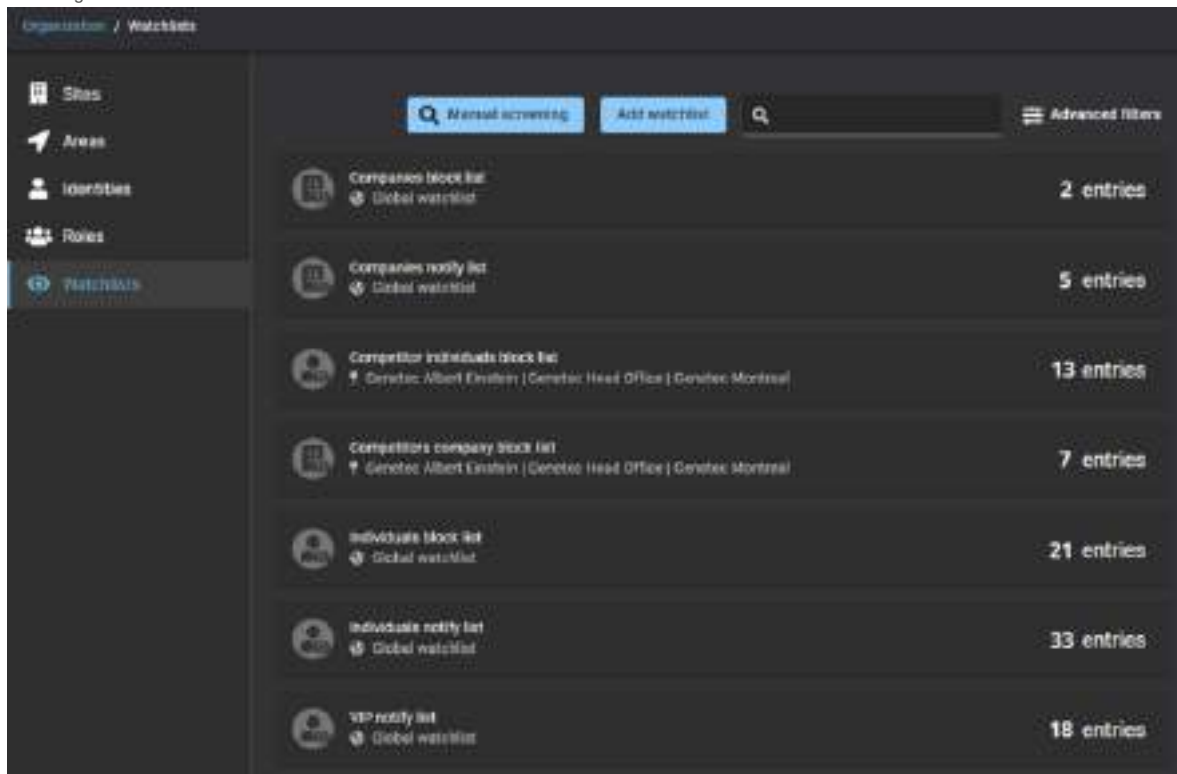
What you should know

A watchlist can only be deleted by the *watchlist manager* who created it.

NOTE: Any watchlist manager or account administrator can delete any watchlist that is configured as a global watchlist.

Procedure

1. Click Organization > Watchlists.



2. (Optional) Use the search box to find a specific watchlist.

3. (Optional) Click Advanced filters to filter the list results by Site or Watchlist type.

Select the filter options that you require:

a. From the Site list, select a site.

b. From the Watchlist types list, select a watchlist type.

4. Select a watchlist from the list.

5. Click Edit watchlist.

6. Verify you have the required watchlist and click Delete watchlist.

Do one of the following:

- a. In the Delete watchlist dialog, click Delete watchlist to confirm the deletion.

- b. (Optional) Click Cancel to abandon the deletion.

10.6 | Screening visitors manually in ClearID

To manually screen a visitor, you can enter the visitor details to check if there is a screening match. For example, testing a new watchlist to find watchlists that contain a person or company of interest, or to validate a new hire against an internal watchlist.

Before you begin

Add your individual watchlist entries.

What you should know

Only *watchlist managers* or account administrators can manually screen visitors for the following:

- Finding watchlists that contain a person of interest.
- Validating a new hire against an internal Individuals watchlist or Companies watchlist.

Screening matches only occur when the following applies:

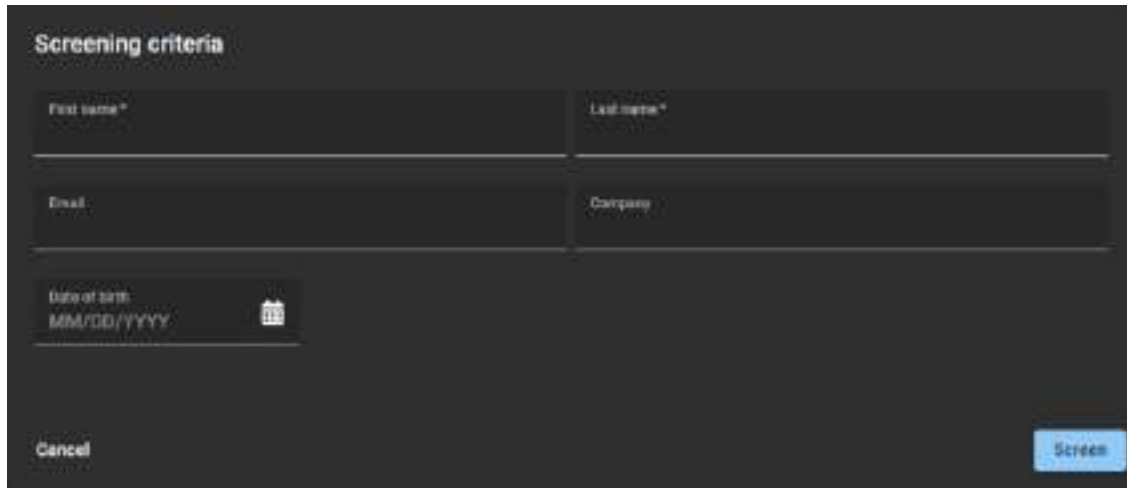
- Individuals: There is a First name and Last name match, First name and Last name alias match, or Email address match.
- Companies: There is a Company name, company domain, or email address domain match.

If *security* or *reception* need to manually screen visitors, the *Watchlist manager* permission must be added to their identity.

Procedure

1. Click Organization > Watchlists.
2. Click Manual screening.
3. In the Screening criteria dialog, complete the details for the visitor that you want to manually screen.

NOTE: Mandatory fields are highlighted by an asterisk (*).



Screening criteria

First name *

Last name *

Email

Company

Date of birth
MM/DD/YYYY

Cancel

Screen

First name

Enter a first name.

Last name

Enter a last name.

Email

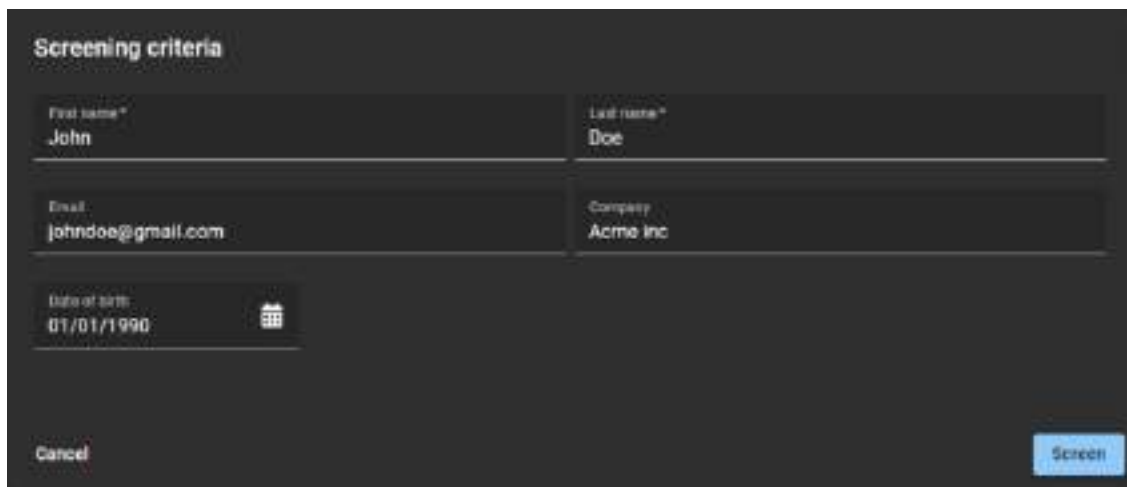
Enter the visitor's email address.

Company

Enter the visitor's company name.

Date of birth

Use the calendar picker to select the visitor's date of birth. The date of birth information is useful additional information when a visitor check-in matches multiple people with the same name. It can be used to validate an identity and also eliminate duplicates or false positive matches.



Screening criteria

First name *

John

Last name *

Doe

Email

johndoe@gmail.com

Company

Acme Inc

Date of birth
01/01/1990

Cancel

Screen

4. Click Screen.

Matching entries for individuals or companies are shown in the *Matching entries* list in the *Screening Criteria dialog*.

Screening criteria

First name *
John

Last name *
Doe

Email
john.doe@gmail.com

Company
Acme inc

Date of birth
01/01/1990

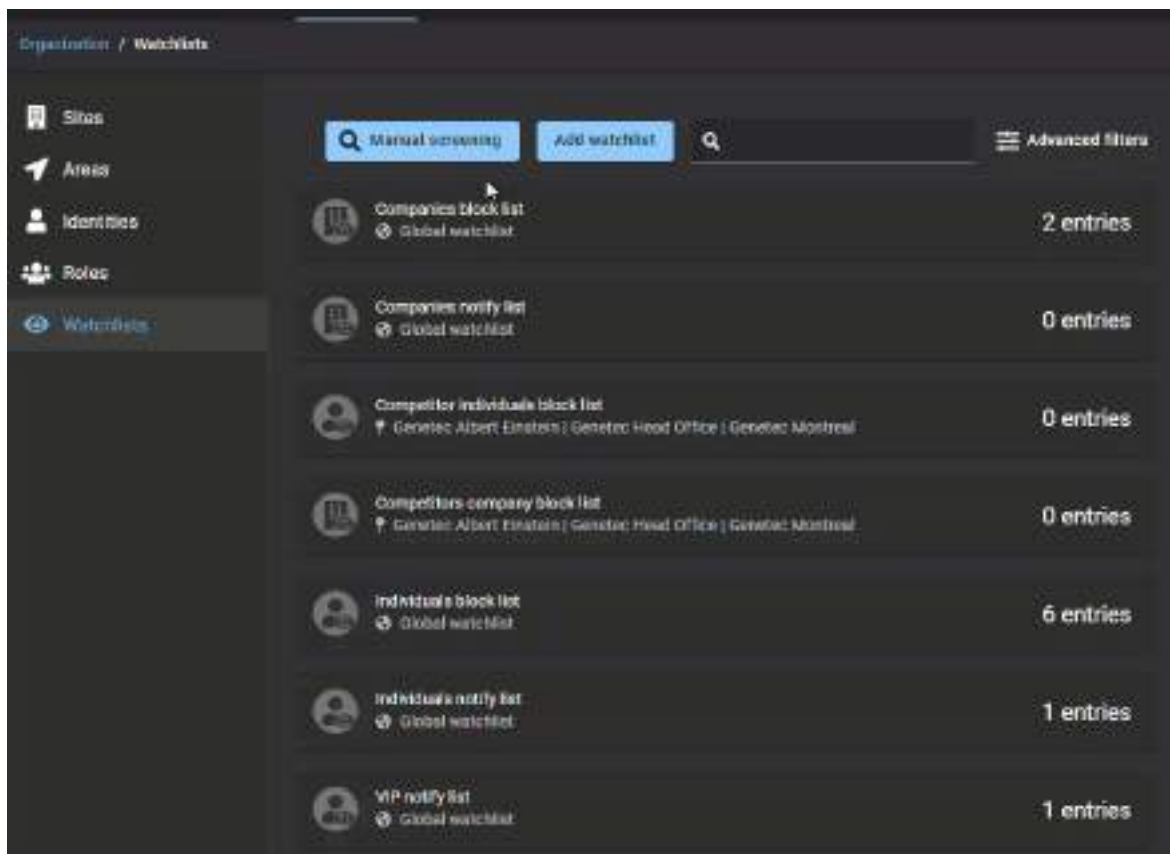
Matching entries (2)

- DOE, John (son, Jonathan, Jonathan)
- Acme inc (some, acme incorporated, Acme inc.)

Cancel Screen

5. (Optional) Click an individual in the Matching entries list to view the complete details of the individuals watchlist entry.
6. (Optional) Click a company in the Matching entries list to view the complete details of the companies watchlist entry.
7. Click Cancel to exit the *Screening Criteria* dialog.

Example



Tip: Click the animation to view full size.

Browse

- Adding watchlist managers in ClearID

10.7 | Unblocking visitors blocked by a watchlist in ClearID

To unblock visitors incorrectly blocked by a watchlist, you can add the visitors email to an always allow list.

Before you begin

Add your individuals watchlist entries.

What you should know

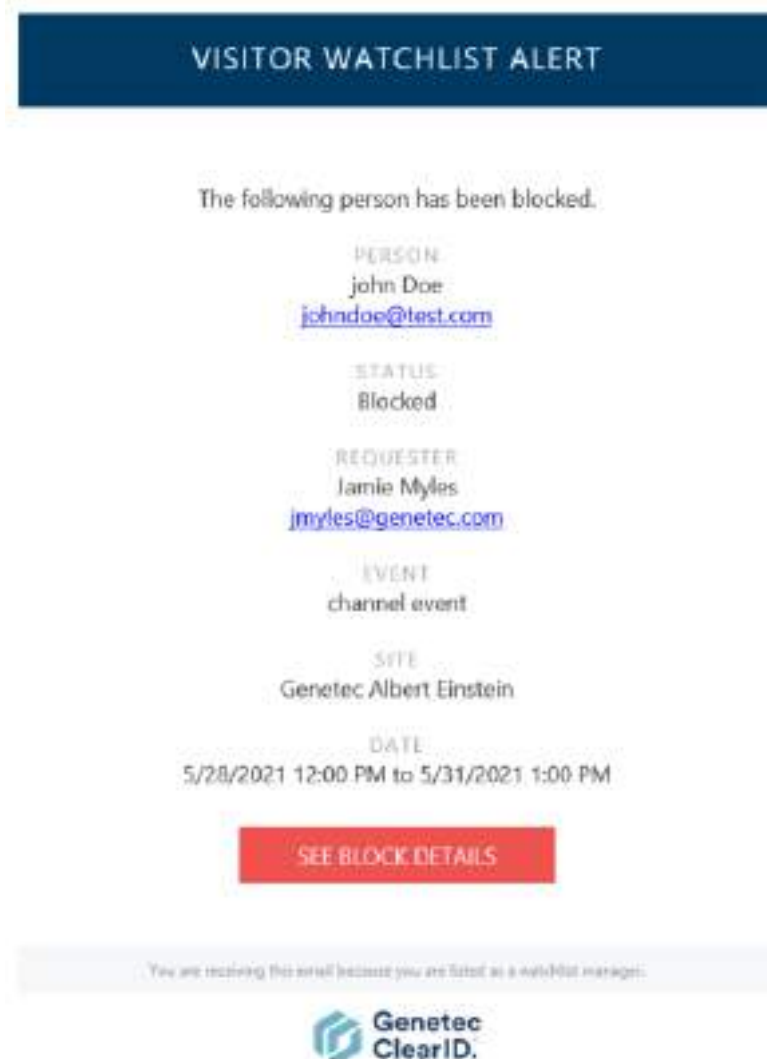
Only a *watchlist manager* or account administrator can unblock a blocked visitor.

- Individuals watchlist email match cannot be set to Always allow.
- Company watchlist entry matches cannot be set to Always allow.
- Notify watchlist entry matches cannot be set to Always allow.

Use this procedure to add any similar emails or false positive email matches for visitors that you might want to allow once or always allow. For example, a possible match that happens to have the same name details, but is a different person with a different email address that should be allowed.

Procedure

1. In your Visitor watchlist alert for <person or company of interest> email, click SEE BLOCK DETAILS.



The visitor watchlist alert dialog opens in the Genetec ClearID™ web portal.

Visitor watchlist alert

Requested by Jamie Myles

Site and areas
Genetec Albert Einstein (America/Toronto)
Main Entrance

Event date and time
From: May 28, 2021 12:00 PM
To: May 31, 2021 1:00 PM

Visitor
First name: John
Last name: Doe
Email: johndoe@test.com
Company:

Hosts • 1 Hosts
Jamie Myles

Matching watchlist entries Always allow all

	DOE, John (Joh, Jonathan, Jonathan) johndoe@test.com	Individuals notify list	John Doe	☐	
	DOE (Do, Dow), John (Jon, Jonathan) johndoe@test.com	Individuals block list	John Doe	☐	

Close Allow entry

- In the Matching watchlist entries section, hover over the info icon to see the watchlist entry details that matched this visitor.
- (Optional) Click a matching watchlist entry in the list to open and view the watchlist entry details.

The watchlist entry opens in a new browser tab.

- Choose whether you want to allow entry one time or always allow entry. Do one of the following:
 - If you want to allow entry one time only for this visitor watchlist alert, click Allow entry.
 - If you want to always allow specific future matching entries for this visitor, in the Matching watchlist entries list, move the Always allow slider to the enabled position for each entry you want to always allow, then click Allow entry.
 - If you want to always allow all future matching watchlist entries for this visitor, in the Matching watchlist entries section, move the Always allow all slider to the enabled position, then click Allow entry.

NOTE: Only the slider controls for the watchlist entries that can be set to Always allow will be moved to the enabled position.

- In the Reason field, enter a reason why the blocked visitor was unblocked and allowed to visit.

Visitor watchlist alert

? Requested by: Jamie Myles

Blocked

Site and areas
Genetec Albert Einstein (America/Toronto)
Main Entrance

Event date and time
From: May 28, 2021 12:00 PM
To: May 31, 2021 1:00 PM

Visitor

First name	Last name
John	Doe
Email	Company
johndoe@test.com	

Hosts + 1 Hosts
Jamie Myles

Matching watchlist entries Always allow all

	DOE, John (Jon, Jonathan, Jonathan) johndoe@test.com	Individuals notify list	John Doe		
	DOE (Do, Dow), John (Jon, Jonathan) johndoe@test.com	Individuals block list	John Doe		

Allow reason ✕

Reason:
johndoe@test.com is not the BLOCKED johndoe@competitor.com and should always be allowed.

88 / 300

Confirm

- (Optional) In the Allow reason section, click  to cancel the unblock, then click Close.
- Click Confirm.

Example

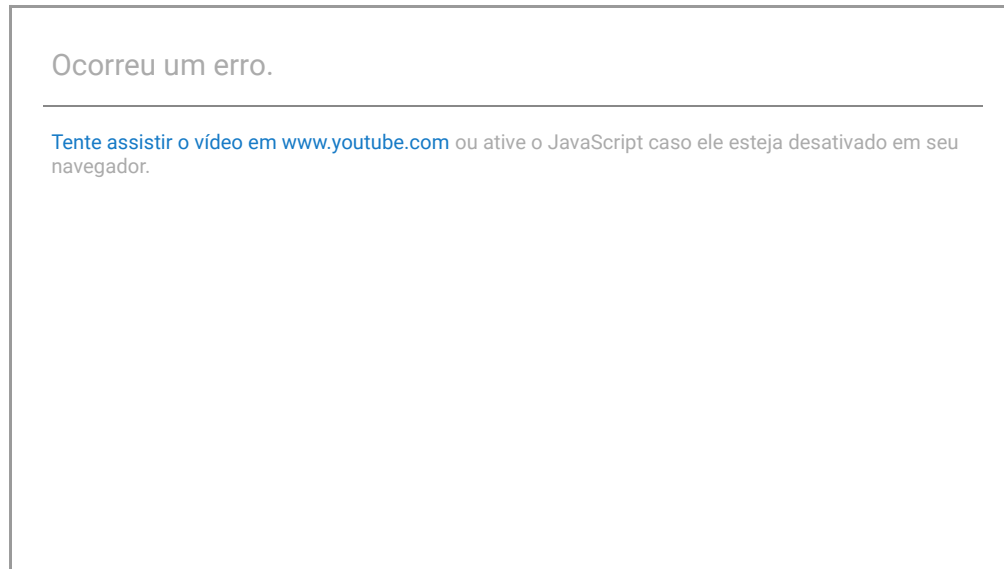
Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

11 | Role-based access control

11.1 | About role-based access control in ClearID

Role-based access control uses identities with various attributes to automatically manage access control. Defining provisioning policies ensures that people in your organization always have up-to-date access permission levels. If an employee changes job title, department, or moves to a different site, the system automatically adjusts their access when their identity attributes are changed.



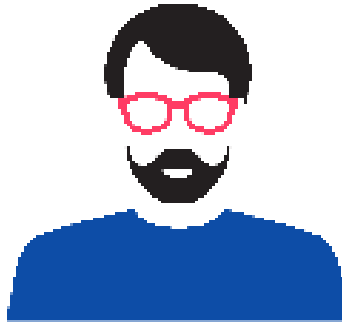
Role-based provisioning policies can be used to automatically assign or revoke access in different situations:

- Grant or revoke access based on employees locations.
- Grant or revoke access based on specific *roles* or job titles in the organization, or who they report to.
- Grant access to a zone only if people have specific training or certifications.
- Grant or revoke access based on a list of custom attributes synchronized from an external source.

NOTE: Many other scenarios might also be possible depending on your requirements and current setup. You can also manually add, modify, or remove access at any time.

What is an identity?

In Genetec ClearID[™], an identity represents a person and defines what they can do across various platforms, security systems, business systems, and functions. Each identity has one or more access control badges (credentials) and is linked to a cardholder in Synergis[™]. For example, these credentials could be a Windows user (Active Directory), an employee (Human Resources and Payroll), a sales person (CRM and Quoting Tool), and a cardholder (Physical Security).



An identity interacts across many security and business systems and functions

A windows user

Microsoft Active Directory

An employee

Employee roles

A cardholder

Physical security

An identity is much more than the profile of a cardholder, it is a unique digital profile. The identity represents a person that either has an access control badge, uses the self-service portal, or both.

NOTE: In ClearID, a visitor or a temporary badge holder is not an identity.

- An identity is a person who has a permanent badge assigned to them.
- A visitor is a person who has a paper badge or a temporary badge credential assigned to them.
- A contractor can be either an identity or a visitor. When a contractor is defined as a visitor, they receive a one-day HID card entered as a visitor in ClearID.

Access is typically permanent for employees, semi-permanent for contractors, and temporary for guests.

Identity attributes

In Genetec ClearID™, attributes are the traits or characteristics that make up an identity. Examples of attributes include department, location, role, seniority, pay grade, training certifications, and security clearance.

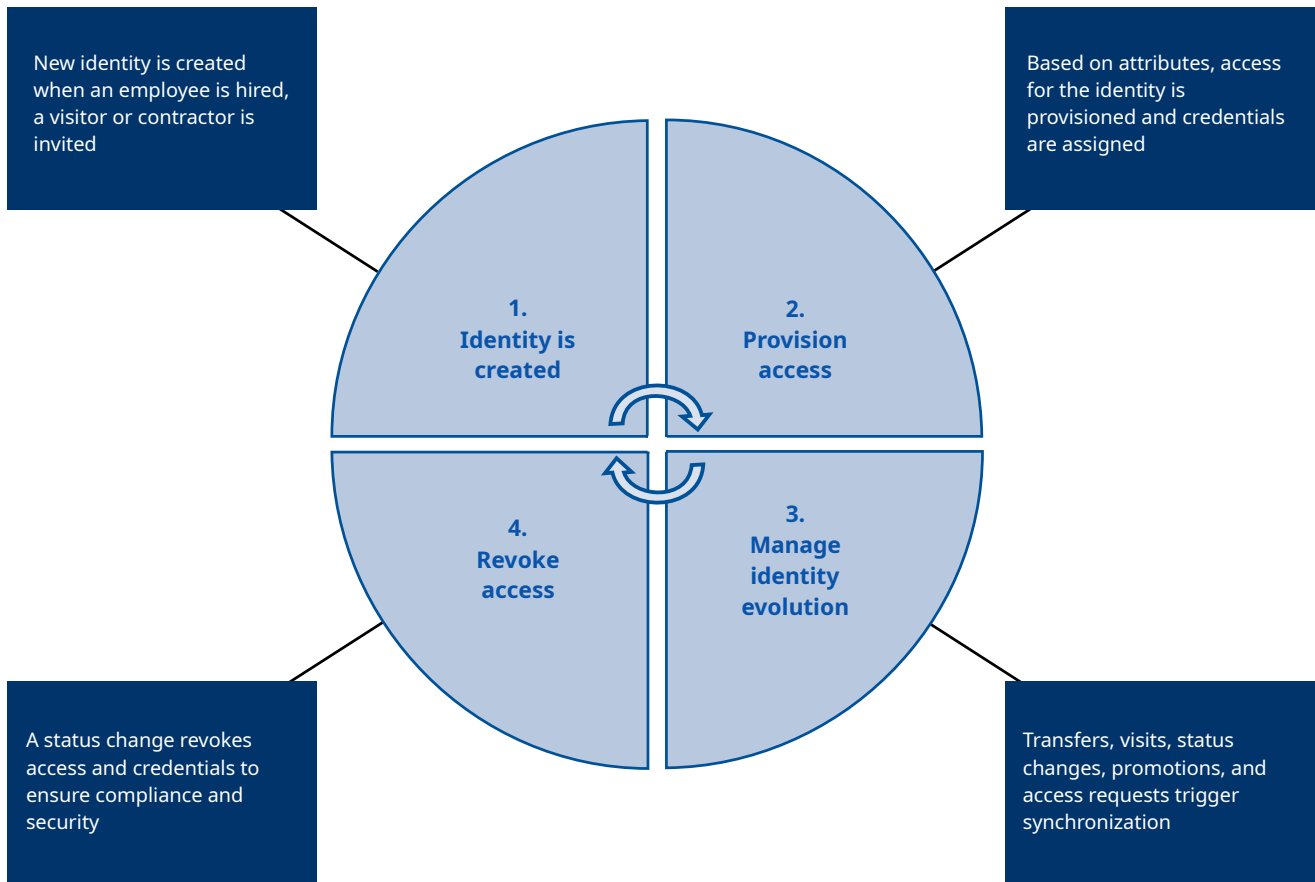
Role based access control relies on policies (*provisioning rules*) that automatically assign rights to identities (people) based on attributes (traits or characteristics).

In Genetec ClearID™, a role manager is an identity that has authority over who is assigned to a role. A role manager can add people to and remove people from a role. They are also responsible for role access review approvals.

The life cycle of an identity

In ClearID, the entire life cycle of an identity can be automatically managed.

The following diagram illustrates the life cycle of an identity when a provisioning policy is activated:



11.2 | Adding roles in ClearID

Before you can configure your role-based automatic access control policies, you must define your roles.

Before you begin

Familiarise yourself with role-based access control.

What you should know

In Genetec ClearID™, a role is a group of people who are assigned the same access. A person can be assigned multiple roles. Roles are linked to cardholder groups in Synergis™. A role manager controls who is granted access to the group.

- Only account administrators can add roles.
- Consider creating roles for each department, group, or job title in your organization. For example, you might create roles for HR, IT, marketing, developer teams, payroll, contractors, and so on.

Procedure

1. From the homepage, click Organization > Roles.
2. Click Add role.
3. In the General section, complete the fields.
 - a. Enter a name for the role.
 - b. Enter a meaningful description.
 - c. Add any internal notes.

NOTE: The internal notes field is used to store special instructions or details only visible to the account administrator, role owner, and role manager. Other users of the system cannot view internal notes. For example, the internal notes field could contain the following:

Only permanent employees based in Montreal should be in this role. Discuss with security before adding employees to this role.

4. (Optional) In the Notifications section, Select the notifications options that you require.

The screenshot shows the 'General' tab for a role named 'Information Technology'. The left sidebar contains links for 'General', 'Managers', 'Members', and 'Provisioning policy'. The main content area has a 'Name' field with the value 'Information Technology', a 'Description' field with the value 'IT department', and a 'Internal roles' field with the value 'N/A'. Below these fields is a 'Notifications' section with a description: 'Send an email notification to the associated role members and their supervisors, role owners, and role managers when:'. There are two checkboxes: 'Role members are manually added' and 'Role members are manually removed', both of which are currently unchecked. A red 'Save role' button is located in the top right corner.

5. Click Save.

Example

The screenshot shows an error message in Portuguese: 'Ocorreu um erro.' (An error occurred.). Below the message is a link to a video: 'Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.' (Try watching the video on www.youtube.com or enable JavaScript if it is disabled in your browser.).

After you finish

Configure your role-based access control policies.
Browse

- [Viewing a role activity report in ClearID](#)

11.3 | Configuring role managers in ClearID

Role managers are composed of two distinct roles: role owners and role managers. Before you can define policies for a role or add or remove identities from a role, you must assign one or more employees as role managers.

Before you begin

[Add your roles.](#)

What you should know

- Only role owners can configure role managers.

Procedure

1. From the Home page, click Organization > Roles and select a Role.
2. Click Managers to configure role manager settings.
 - a. Use the search field to find existing managers, or click Add (+).
 - b. Select the required user or users and click Confirm.
3. Choose the Role type for the user or users you just added from the following:

Manager

A role manager is an identity that has authority over who is assigned to a role. A role manager can add people to and remove people from a role.

Owner

A role owner is responsible for assigning role managers and configuring role-based policies.

Both

Use when one person is responsible for managing roles, assigning role managers, and configuring policies.



4. (Optional) To remove any managers that you no longer require, hover over a name and click ✖.
5. Click Save.

Results

The selected people are added to the list as either a manager, an owner, or both.

After you finish

Add role members.

Browse

- Viewing a role activity report in ClearID

11.4 | Configuring role-based access control policies in ClearID

To ensure that people in your organization always have up-to-date access permission levels, you can define provisioning policies that automatically assign people to specific roles based on their identity attributes. If an employee changes job title, department, or moves to a different site, the system automatically adjusts their access.

Before you begin

- Add your roles.

What you should know

- Only account administrators, or role owners can create or modify provisioning policies that automatically associate people with a specific role.
- A maximum of 25 policies with a maximum of 25 policy conditions can be defined for each role.

Procedure

1. From the Home page, click Organization > Roles and select a Role.
2. Click Provisioning policy and click or slide the toggle to Active.
3. In the Description field, enter a meaningful policy description.
4. (Optional) Configure your automatic removal settings for role members:



- a. Select the Automatically remove members that no longer match checkbox option.
- b. Specify when to automatically remove your role members. Choose one of the following:
 - o After a specified number of days. The default is 7 days.
 - o Immediately.

For example, an IT role with access to server rooms. When an IT role member moves to a Developer job, they might still require access to server rooms for 7 days for support or skill transfer purposes. Role members are removed when their identity settings no longer match the policy settings for role-based access control.

5. Add the policy rules for the role that you are configuring.

- a. Select the Property type that you require.

The property types listed here are the default identity field attributes that can be found in the General details of any identity.

NOTE: Only roles that you are a role manager for can be selected.

Company

Enter the company name.

Country

Select a country from the list.

Department

Enter a department name.

Description

Enter a description.

Extended grant time

Used to select True or False.

External ID

Enter an external ID

Job title

Enter a job title.

Primary site

Enter or select the primary office location.

Provisioning attributes

Type a custom provisioning attribute and press enter. Some examples might include: background check, drug and alcohol tests, NDA, Safety training, site induction training, and so on.

Status

Choose either Active or Inactive.

Supervisor name

Enter a name.

Supervisors

Add multiple supervisors.

Worker type code

Enter a worker type code

Worker type description

Enter a meaningful description for the worker type.

- b. Select an Operator from the following:

Genetec ClearID™ User Guide

Displayed in the header

- o Contains
- o Does not contain
- o Is
- o Is not

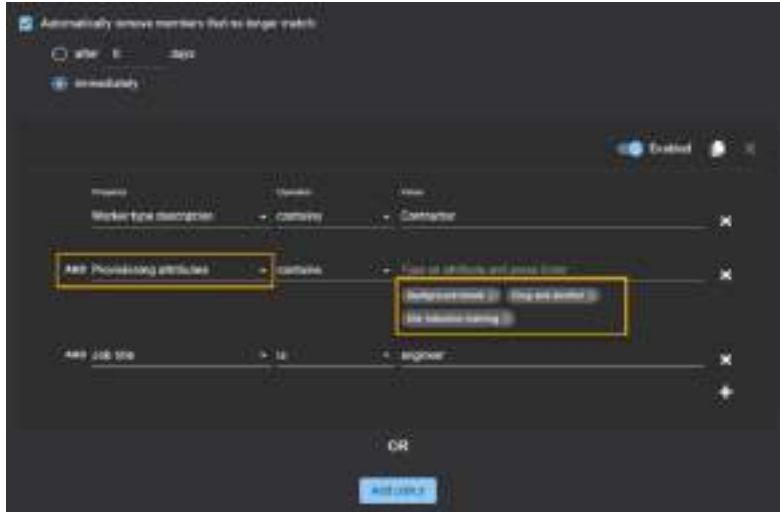
NOTE: The Operators that are displayed vary depending on the Property type that you select.

- Enter a value or select an option that relates to the Property type you selected.

NOTE: The Value options or fields that are displayed vary depending on the Property type that you select.

6. (Optional) Add custom provisioning attributes to your provisioning policy.

- Select the Provisioning attributes property.
- Select an Operator from the following:
 - Contains
 - Does not contain
- Enter the custom attribute values that you require.



NOTE: For custom attributes, the provisioning policy is only triggered when an identity includes as a minimum all the provisioning attribute values specified in this policy.

- (Optional) To temporarily disable a policy rule, set the Enabled slider to Disabled.
- (Optional) Click Copy policy (📋) when you want to copy a rule or set of rules.
- (Optional) Click ✕ to remove any policy rules that you no longer require.
- Click Save.

Results

Users can now be automatically assigned to or removed from specific roles based on their identity attributes.

Example



After you finish

Add role managers.
Browse

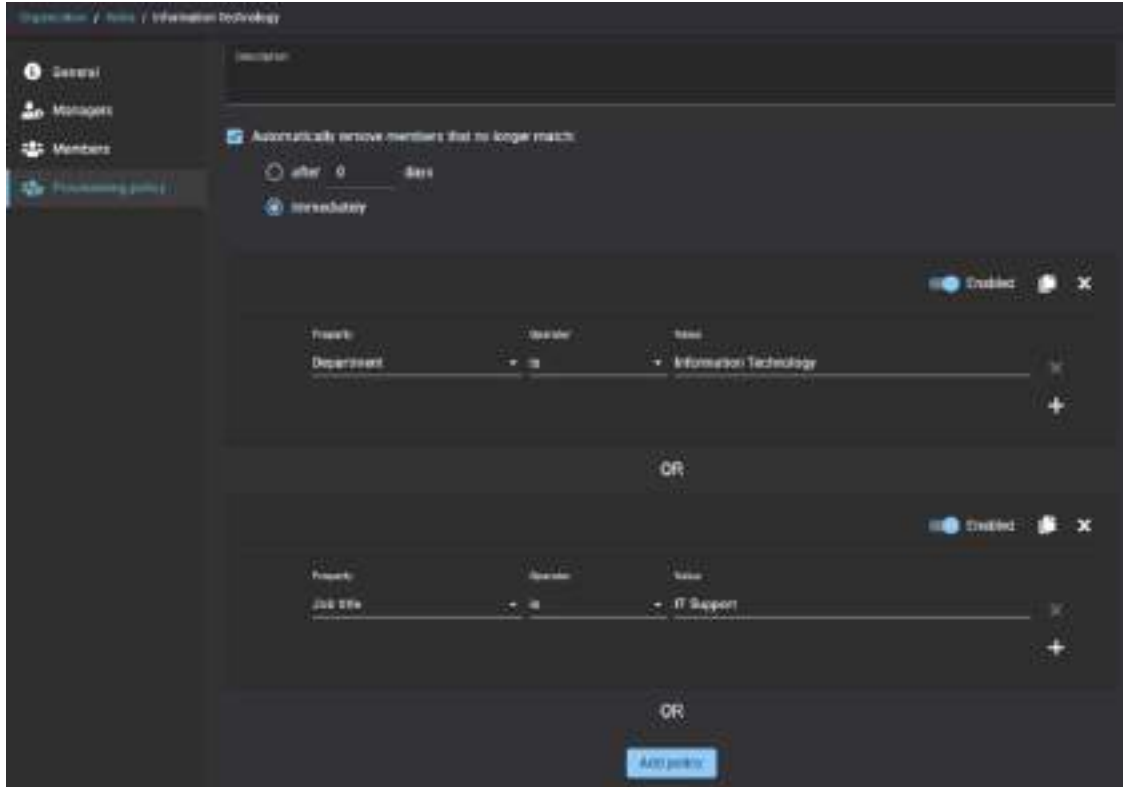
- Adding roles in ClearID
- Identity fields in ClearID

11.4.1 | Scenario 1: Adding employees to an IT role in ClearID

In this example, a policy is used to automatically assign employees to an IT role based on their identity attributes.

The following example shows a policy configured to automatically add employees to an Information Technology role if the following policy rule criteria are met:

- Department is Information Technology
- Job title is IT Support.



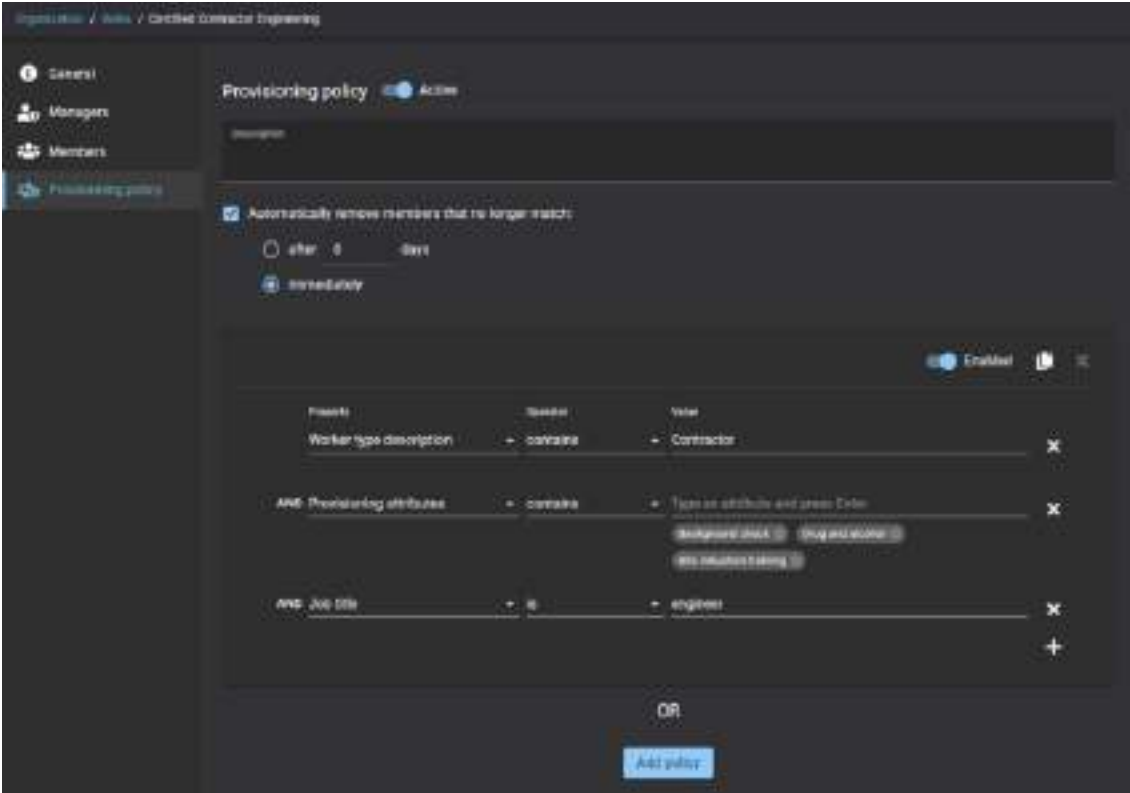
Parent topic: [Configuring role-based access control policies in ClearID](#)

11.4.2 | Scenario 2: Adding contractors to a certified contractor engineering role in ClearID

In this example, a policy is used to automatically assign contractors to a certified contractor engineering role based on their identity attributes.

The following example shows a policy configured using custom attributes to automatically add contractors to a certified contractor engineering role if the following policy rule criteria are met:

- Identity contains worker type contractor
- Provisioning attributes are found
- Their job title is engineer.

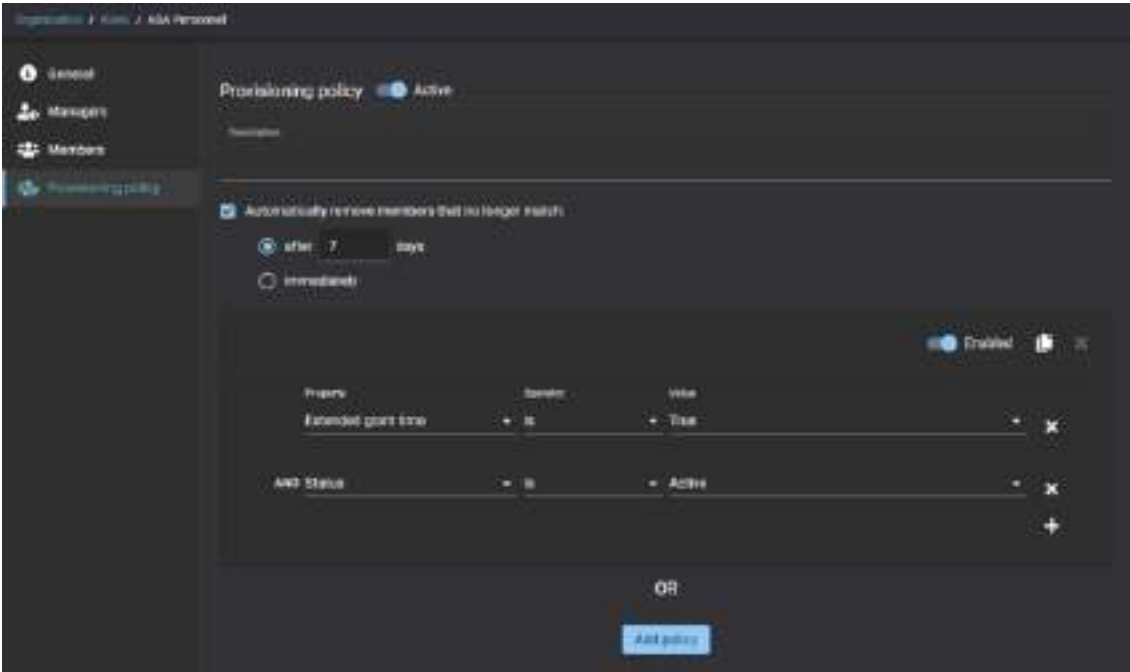


Parent topic: Configuring role-based access control policies in ClearID

11.4.3 | Scenario 3: Adding employees to an ADA personnel role in ClearID

In this example, a policy is used to automatically assign employees that require accessibility assistance to an ADA personnel role based on their identity attributes. The following example shows a policy configured to automatically add employees to an ADA personnel role if the following policy rule criteria are met:

- The extended grant time property is found.
- Their status is active.



Parent topic: Configuring role-based access control policies in ClearID

11.5 | Adding custom provisioning attributes to an identity in ClearID

When the default Genetec ClearID™ policy attributes do not meet your needs, you can manually assign custom provisioning attributes to an employee's identity record. These attributes can then be used in a role-based access control policy.

Before you begin

- Add your roles.

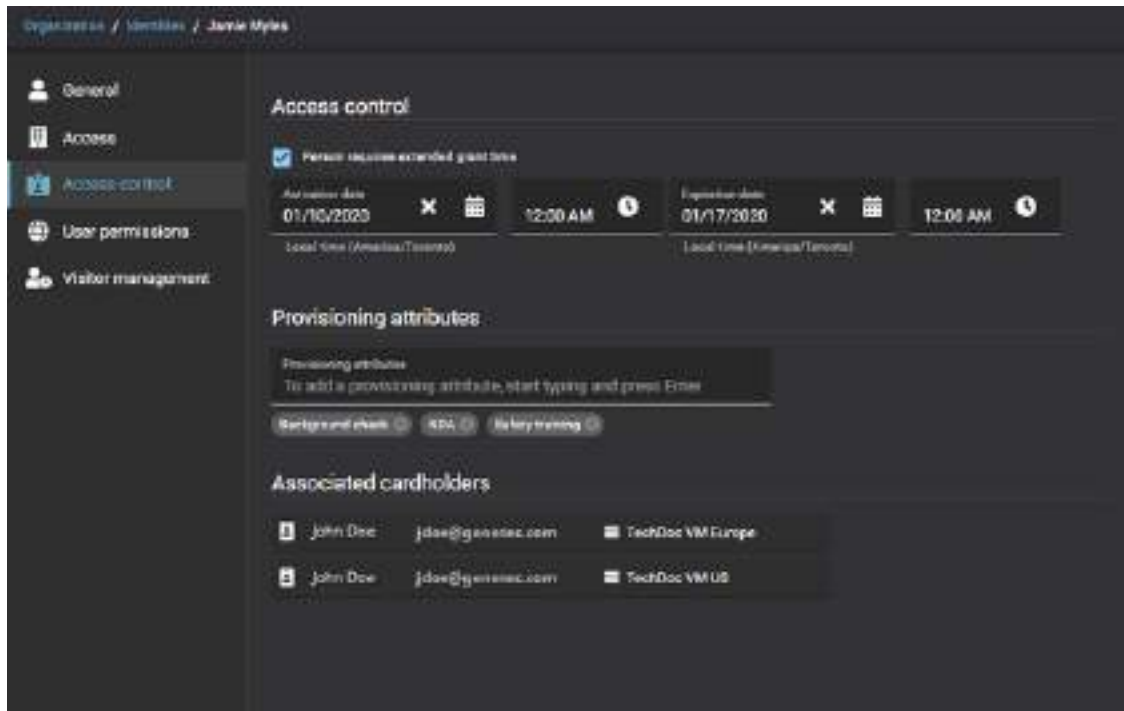
What you should know

- Only account administrators can add custom attributes.
- Custom attributes are typically used when you import or synchronize your attributes from an external source.
- The current status of custom attributes can be managed using an integration, and any that become obsolete are removed automatically.
- Custom attributes can also be added or removed manually.

Some example custom provisioning attributes might include: background checks, drug and alcohol tests, NDA, safety training, site induction training, and so on.

Procedure

1. From the Home page, click Organization > Identities and select an identity.
2. Click Access control.
3. In the Provisioning attributes section, start typing and press enter to add your custom attributes.
4. (Optional) Add additional custom attributes if required.
5. (Optional) Click  to remove any attributes that have expired or are no longer applicable.
6. Click Save.



11.6 | Adding role members in ClearID

To add role members who do not fit the default role-based provisioning policy criteria, you must add them manually.

Before you begin

Add role managers.

What you should know

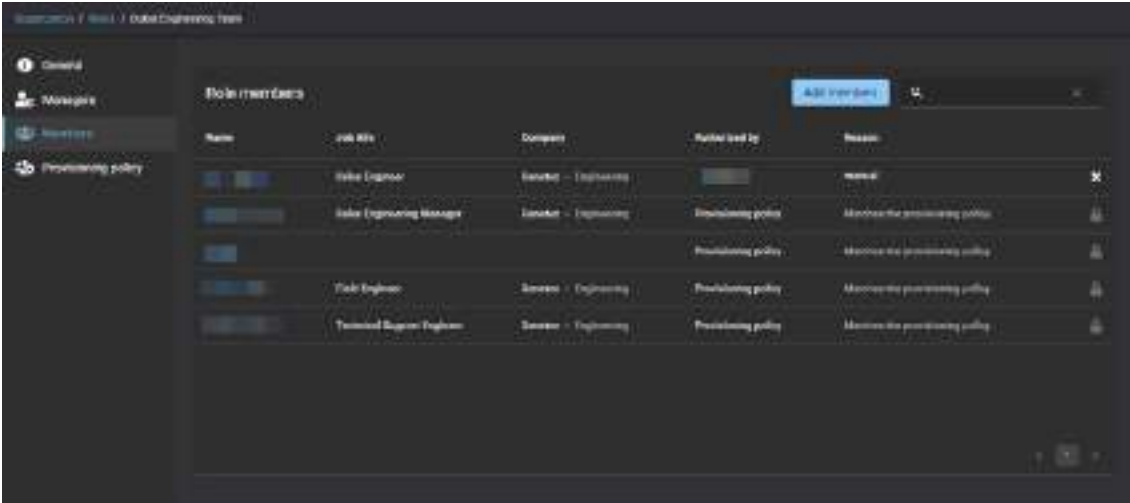
- Only role managers can add role members.
- When a provisioning policy is enabled, role members are added automatically based on rules defined in the policy. Role members that are automatically added are shown in Authorized by column as Provisioning policy.
- Role members can also be added manually. Role members that are manually added are shown in the Authorized by column as Manual.
- Role members that match a provisioning policy are locked and cannot be removed.
- Role members that no longer match a provisioning policy are immediately unlocked. They are automatically removed after the period specified in a provisioning policy.

Procedure

1. From the Home page, click Organization > Roles and select a role.
2. Click Members to configure the list of role members.
3. Click Add members.
4. Search for or select one or more members.
5. Enter a reason and click Add.

The following example shows the Dubai Engineering Team role members.

NOTE: The Authorized by column shows four members that were added automatically (Provisioning policy) and one that was added manually (Manual).



Tip: You can click the blue text in the Name column to view or modify the identity details.

6. (Optional) To immediately remove any role members who no longer meet the policy criteria, or role members that were added manually, click  then click Remove.

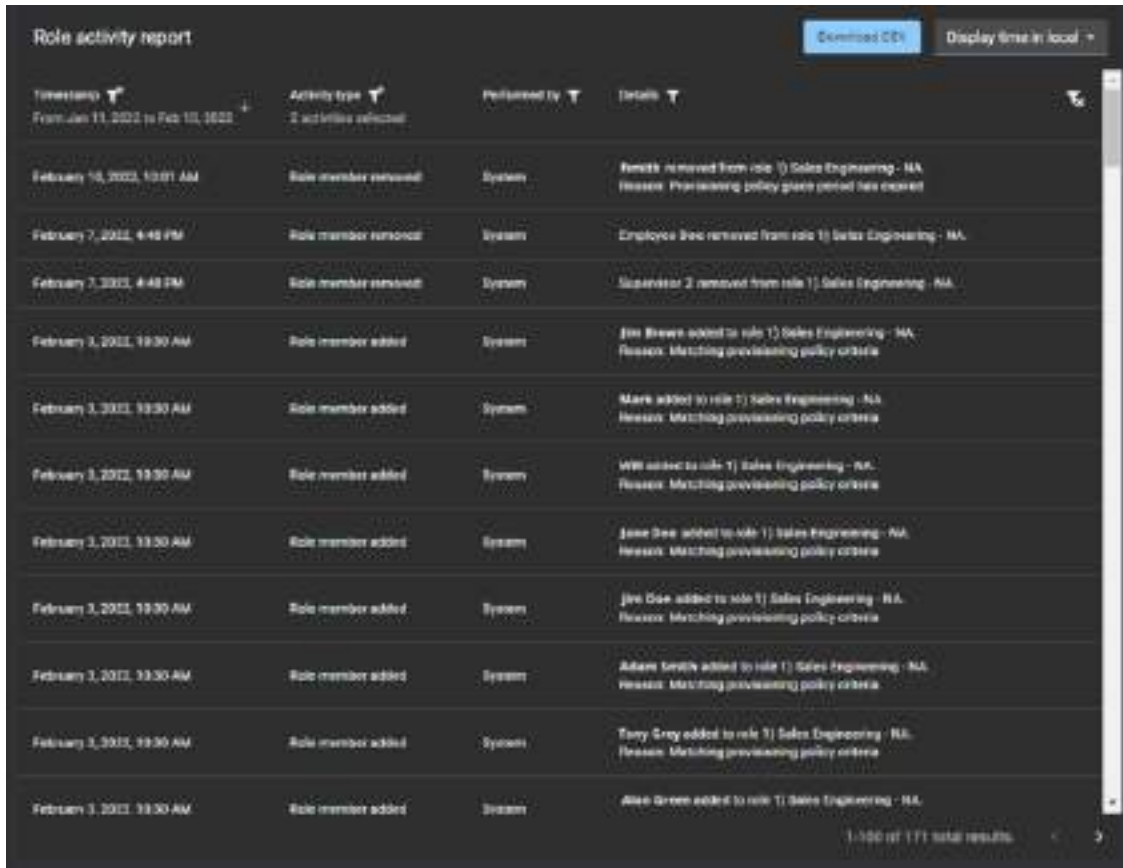
Browse

- Viewing a role activity report in ClearID

11.7 | About role activity report in ClearID

In Genetec ClearID™, a role activity report is an audit trail of all activities related to roles. The report includes timestamp information, activity type, who activity was performed by, and a details section including reason information.

Role activity report



Role activity report			
Timestamp	Activity type	Performed by	Details
February 10, 2022, 10:01 AM	Role member removed	System	Breath removed from role 1) Sales Engineering - NA. Reason: Provisioning policy grace period has expired
February 7, 2022, 4:48 PM	Role member removed	System	Employee Doc removed from role 1) Sales Engineering - NA.
February 7, 2022, 4:48 PM	Role member removed	System	Supervisor 2 removed from role 1) Sales Engineering - NA.
February 3, 2022, 10:30 AM	Role member added	System	Jim Brown added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Mark added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Will added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	June Doe added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Jim Doe added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Adam Smith added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Tony Gray added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Alice Green added to role 1) Sales Engineering - NA.

The role activity report is used by account administrators to review all activities related to roles. When the report is used by role managers or role owners, only the activity for their roles is shown. For example, role access granted or removed, role manager added or removed, role owner added or removed, and role member added or removed.

Filters can be used to help refine the report search results by timestamp, activity type, performed by, and details.

Browse

- [Viewing a role activity report in ClearID](#)

11.8 | Viewing a role activity report in ClearID

As an *Account administrator*, *Role manager*, or *Role owner*, you can view an audit trail of role-related activities such as timestamp information, activity type, who performed the activity, and more.

Before you begin

You must be an *Account administrator*, *Role manager*, or *Role owner* to view a Role activity report and review audit trail information for role-related activities.

Procedure

1. From the Home page, click Organization > Roles.
2. Search for or select the role that you require from the Name column.
3. Click Role activity.
4. From the Display time menu, select the required display time format.

Display time in local

Report times are displayed using the system time from the computer of the logged-in user.

Display time in UTC

Report times are displayed using Coordinated Universal Time (UTC).

5. Filter the report based on your required criteria:

Role activity report			
Timestamp 		Activity type 	Performed by 
From: Jan 11, 2022 to Feb 10, 2022 		Details 	
		2 activities selected	
February 10, 2022, 10:01 AM	Role member removed	System	Remith removed from role 1) Sales Engineering - NA. Reason: Provisioning policy grace period has expired
February 7, 2022, 4:48 PM	Role member removed	System	Employee Bcc removed from role 1) Sales Engineering - NA.
February 7, 2022, 4:48 PM	Role member removed	System	Supervisor 2 removed from role 1) Sales Engineering - NA.
February 3, 2022, 10:30 AM	Role member added	System	Jim Brown added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Mark added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Will added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Jose Bae added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Jim Doe added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Adam Smith added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Tony Gray added to role 1) Sales Engineering - NA. Reason: Matching provisioning policy criteria
February 3, 2022, 10:30 AM	Role member added	System	Alan Green added to role 1) Sales Engineering - NA.
1/100 of 171 total results			

Timestamp

In the Timestamp column, click  to filter the results by date. Select a pre-defined date range from the choices available or enter a specific date range using the date range picker.

☐ Last 24 hours
 ☐ Last 7 days
 ☐ Last 30 days
 ☐ Last 90 days
 ☐ Last 365 days

☒ Date range (UTC)

From *
 10/21/2021 

From *
 6:25 PM 

To *
 10/22/2021 

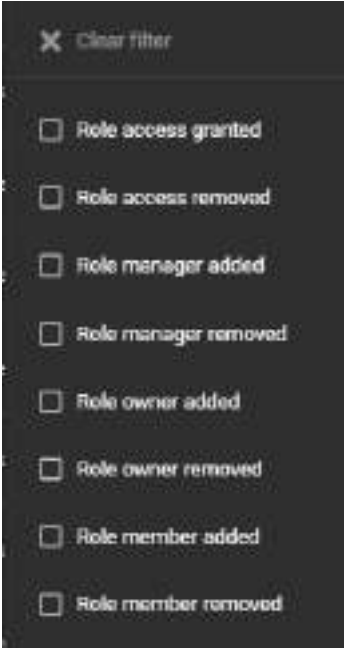
To *
 6:25 PM 

Time period limited to a maximum of one year

(Optional) Use the sort icons ( and ) to display the results in descending or ascending order.

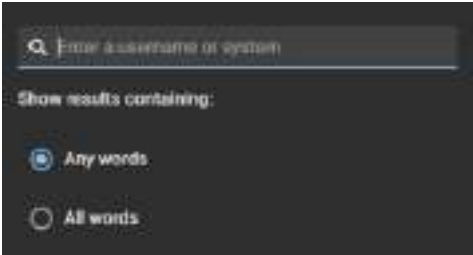
Activity type

(Optional) Use the sort icons  and  to display the results in descending or ascending order.



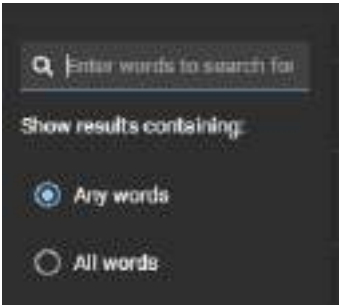
Performed by

In the Performed by column, click  to open a search dialog and filter the results by who performed an activity. For example, tasks performed by a particular user, or tasks performed automatically by the system.



Details

In the Details column, click  to open a search dialog to search the details or reason using a search criteria.



(Optional)

Click  to reset filter selections.

6. Click Download CSV, to download a copy of the role activity report in CSV format. The report can then be used for auditing purposes, to keep a physical copy, to attach to an audit request, to review offline, or to manipulate or consolidate data in a spreadsheet for other audiences.
 - a. Follow your browser prompts to complete downloading the exported file.

The file is exported as a .CSV file to the default download location for your browser. By default the exported file is created using the name of your site. For example, RoleActivity_rolename_fromdate_to_todate_SiteActivityReport.csv (RoleActivity_All active contracotrs_2024-09-23.csv).

NOTE: The columns and entries in the CSV file can vary depending on the filters you've selected when you download the report.

Browse

- About role activity report in ClearID
- Adding role members in ClearID
- Configuring role managers in ClearID
- Adding roles in ClearID

12 | Connecting to other systems

12.1 | Authenticating your connection with ClearID

Before you can connect with Genetec ClearID™ to synchronize data or issue API commands, you must first authenticate your applications (or API environment) so that your applications or API can communicate with ClearID.

What you should know

Use the API integration key to authenticate your applications when making requests to your ClearID account.

- The OAUTH 2.0 protocol is used to authenticate non-user system communications or connections with ClearID.
- Store your key securely and don't share it.

IMPORTANT: When you regenerate your key, you must update any applications that access this account to use the new key.

You can create an API integration to authenticate communications for the following:

- Genetec ClearID™ API
- System for Cross-domain Identity Management (SCIM) integration
- Genetec ClearID™ One Identity Synchronization Tool (Azure AD, Database, File)
- Genetec ClearID™ LDAP Synchronization Agent

Procedure

1. Add an API integration.
 - a. In ClearID, click Administration > API integrations.
 - b. Click Add API integration.

Name
Enter a name for the API integration. For example, Active Directory LDAP Synchronization, API user connection, or One Identity Synchronization.
Description
Enter a meaningful description for the API integration.
 - c. Click Save.
2. Select a user from the API integration list.
 - a. Click Generate key and then click Confirm, to generate the authentication key for your API integration.

CAUTION:
The current API integration key immediately becomes invalid and isn't recoverable.
 - b. Click Download authentication key.

Tip: Make a note of the downloaded file location for later use.

By default, the authentication key for your API integration is named key-systemID-APIintegrationname.json.

Results

You're now ready to configure your applications to synchronize data or issue API commands.

Example



After you finish

Depending on how attributes are set up in your organization, do one of the following:

- Synchronize identity attributes using REST API commands.
- Synchronize identity attributes using the SCIM integration.
- Synchronize identity attributes using One Identity (Azure AD, Database, File).
- Synchronize identity attributes using LDAP.

Browse

- [About ClearID information security](#)
- [Logging on to ClearID](#)

12.2 | Setting up data synchronization

Setting up data synchronization in Genetec ClearID™ involves learning some concepts, configuring the synchronization solution for your identity data, and the webhook integration options that are relevant for your organization.

1. Review the firewall port requirements.
2. Sign in to ClearID.
3. Grant access to the web portal.
4. Authenticate your non-user system connections to synchronize data or issue API commands.
5. Choose a synchronization solution for your identity data:
 - Synchronize identity attributes using the ClearID API:
 - Synchronize identities using an API.
 - [Learn about the ClearID API.](#)
 - Synchronize identity attributes using the ClearID SCIM integration:
 - Synchronize identities using the SCIM Integration.
 - [Learn about the SCIM standard.](#)
 - [Learn about Microsoft Entra ID attribute fields.](#)
 - [Configure the ClearID SCIM integration.](#)
 - [Generate a SCIM key.](#)
 - [Create a Microsoft Azure enterprise application.](#)
 - [Connect your ClearID SCIM integration to Microsoft Azure.](#)
 - [Disable your Microsoft Entra ID groups setting.](#)
 - [Configure your Microsoft Entra ID user settings.](#)
 - [Configure your ClearID SCIM integration synchronization settings.](#)
 - (Optional) [Reset your ClearID SCIM integration identity data.](#)
 - [Review the ClearID SCIM integration synchronization status.](#)
 - Synchronize identity attributes using the ClearID One Identity Synchronization Tool:
 - Synchronize identities using the One Identity Synchronization Tool.
 - [Learn about the One Identity Synchronization Tool.](#)
 - [Learn about the One Identity Synchronization Tool Attribute fields.](#)
 - [Learn about the Azure web app.](#)
 - [Install the One Identity Synchronization Tool.](#)
 - [Configure the One Identity Synchronization Tool.](#)
 - [Review your synchronization status.](#)
 - [Learn about One Identity Synchronization Tool logs.](#)
 - [View the One Identity Synchronization Tool logs.](#)
 - [Update existing identities from an external data source.](#)
 - Synchronize identity attributes using the ClearID LDAP Synchronization Agent:
 - [Learn about the ClearID LDAP Synchronization agent.](#)
 - [Learn about LDAP attributes to ClearID attribute mapping.](#)
 - [Configure the ClearID LDAP Synchronization Agent.](#)
6. Configure and manage your webhook integrations:
 - [Learn about webhooks.](#)
 - [Create your webhooks.](#)
 - [Modify your webhooks.](#)
 - [View the webhook logs.](#)
7. (Optional) Troubleshooting information.
 - a. [One Identity Synchronization Tool: Connectivity issues](#)
 - b. [One Identity Synchronization Tool: Data Synchronization issues](#)

12.3 | Synchronizing identities using an API in ClearID

Use the Genetec ClearID™ API to code your own solutions to automate various functions in ClearID. The primary use for the REST API is synchronizing identities, however many other scenarios are also possible.

12.3.1 | About the ClearID API

The Genetec ClearID™ API is an Application Programming Interface that developers can use to help customers and partners integrate additional software or perform custom functions.

For more information about automating functions using the ClearID REST API, see the [Genetec™ Developer](#) documentation.

Parent topic: [Synchronizing identities using an API in ClearID](#)

12.4 | Synchronizing identities using the SCIM integration in ClearID

To synchronize external system attributes from a supported identity provider into Genetec ClearID™ identity attributes, you can use the System for Cross-domain Identity Management (SCIM) integration. These identity attributes can then be used in ClearID to assign people to roles and automate role-based access control.

What you should know

Only Microsoft Entra ID is currently supported. If you want to integrate another supported identity provider, contact your deployment representative.

Procedure

- 1. Learn about the SCIM standard.
- 2. Learn about Microsoft Entra ID attribute fields.
- 3. Configure the SCIM integration.
- 4. (Optional) Reset the SCIM integration identity data.
- 5. Review SCIM integration synchronization status.

12.4.1 | About the SCIM standard in ClearID

The System for Cross-domain Identity Management (SCIM) standard is an open-standard protocol for exchanging identity information between entities. It's widely used to automate the process of managing user identities in IT systems. The SCIM integration ensures that any changes are automatically synchronized to other systems when identity attributes change.

System

SCIM creates a common format for how identity data is exchanged.

Cross-domain

SCIM securely communicates identity data across platforms.

Identity management

SCIM automates the flow of information between an identity provider or [identity and access management \(IAM\) system](#) and cloud-based applications.

Benefits

- Using SCIM reduces the effort that it takes to create, modify, and synchronize identity data.
- Because the SCIM integration uses Microsoft Entra ID in the cloud, there's no machine or infrastructure to manage.
- There are no firewall ports to configure.

NOTE: The SCIM integration only synchronizes the identity attributes that have changed. This approach results in a significant reduction in throughput and processing overheads. Other solutions typically synchronize all identity attributes at a specified time to get all the latest identity data.

Parent topic: [Synchronizing identities using the SCIM integration in ClearID](#)

12.4.2 | About Microsoft Entra ID attribute fields in Microsoft Azure

When you synchronize an external system with Genetec ClearID™ using the System for Cross-domain Identity Management (SCIM) standard, your external system attributes are imported into ClearID identity attributes. The import uses the field mappings in Microsoft Entra ID.

Most of the ClearID identity fields are created as custom attributes.

You must prefix each field with: `urn:ietf:params:scim:schemas:extension:clearid:2.0:User`

Identity attributes	
Attribute fields	Notes

Genetec ClearID®; User Guide

Displayed in the header

Attribute fields	Notes
Basic fields: active username displayName	- These basic fields are the only fields that we use from the SCIM base schema. - displayName is required in the mapping.
Base identity fields: urn:ietf:params:scim:schemas:extension:clearid:2.0:User:description urn:ietf:params:scim:schemas:extension:clearid:2.0:User:firstName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:lastName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:middleName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:countryCode urn:ietf:params:scim:schemas:extension:clearid:2.0:User:email	- firstName or lastName must be supplied in the mapping (the same as in the portal identity form). - email must be a valid email format to be created in the identity properly. - countryCode must be a 3-letter code. It's best to use a constant value from Microsoft Entra ID for now.
CompanyData fields: urn:ietf:params:scim:schemas:extension:clearid:2.0:User:employeeNumber urn:ietf:params:scim:schemas:extension:clearid:2.0:User:secondaryEmail urn:ietf:params:scim:schemas:extension:clearid:2.0:User:cityOfResidence urn:ietf:params:scim:schemas:extension:clearid:2.0:User:stateOfResidence urn:ietf:params:scim:schemas:extension:clearid:2.0:User:zipCode urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberPrimary urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberSecondary	secondaryEmail must be a valid email format to be created in the identity properly.
PrivateData fields: urn:ietf:params:scim:schemas:extension:clearid:2.0:User:supervisorName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:departmentName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:jobTitle urn:ietf:params:scim:schemas:extension:clearid:2.0:User:companyName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeDescription urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeCode	
SystemData fields: urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasExtendedTime urn:ietf:params:scim:schemas:extension:clearid:2.0:User:externalId	- Boolean fields only work with the SCIM 2.0 feature flag. - externalId is required and needs to be unique. This value is used to manage the creation of identities (same way in Onelidentity). The easiest way to use this value is to map with an email or username.
Other custom fields: (that aren't directly part of the identity model) urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasWebPortalAccess urn:ietf:params:scim:schemas:extension:clearid:2.0:User:isAdmin	Boolean fields only work with the SCIM 2.0 feature flag.

Attribute fields that are not supported

Date fields:

- birthday
- activationDateUtc
- expirationDateUtc
- externalSyncTimeUtc

Fields with ids (reference to identityIds):

- creationOnBehalf
- approvers
- siteId
- provisioningAttributes
- customFields

Parent topic: [Synchronizing identities using the SCIM integration in ClearID](#)

12.4.3 | Configuring the SCIM integration in ClearID

Before you can synchronize an external system with Genetec ClearID™, you must first configure the System for Cross-domain Identity Management (SCIM) integration in ClearID and Microsoft Azure.

Before you begin

- [Learn about the SCIM standard.](#)
- [Learn about Microsoft Entra ID attribute fields.](#)

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

Only Microsoft Entra ID is currently supported. If you want to integrate another supported identity provider, contact your deployment representative.

IMPORTANT: Do not skip the disable groups step. ClearID does not support the synchronization of groups.

Procedure

1. Generate your SCIM key.
2. Create your Microsoft Azure enterprise application.
3. Connect your ClearID SCIM integration to Microsoft Azure.
4. Configure your attribute mappings.
 - a. Disable the Microsoft Entra ID groups setting.
 - b. Configure the Microsoft Entra ID user settings.
5. Configure the ClearID SCIM integration synchronization settings.

After you finish

Review the SCIM integration synchronization status.

Parent topic: [Synchronizing identities using the SCIM integration in ClearID](#)

12.4.3.1 | Generating a SCIM key in ClearID

[Synchronizing identities using the SCIM integration in ClearID](#) >

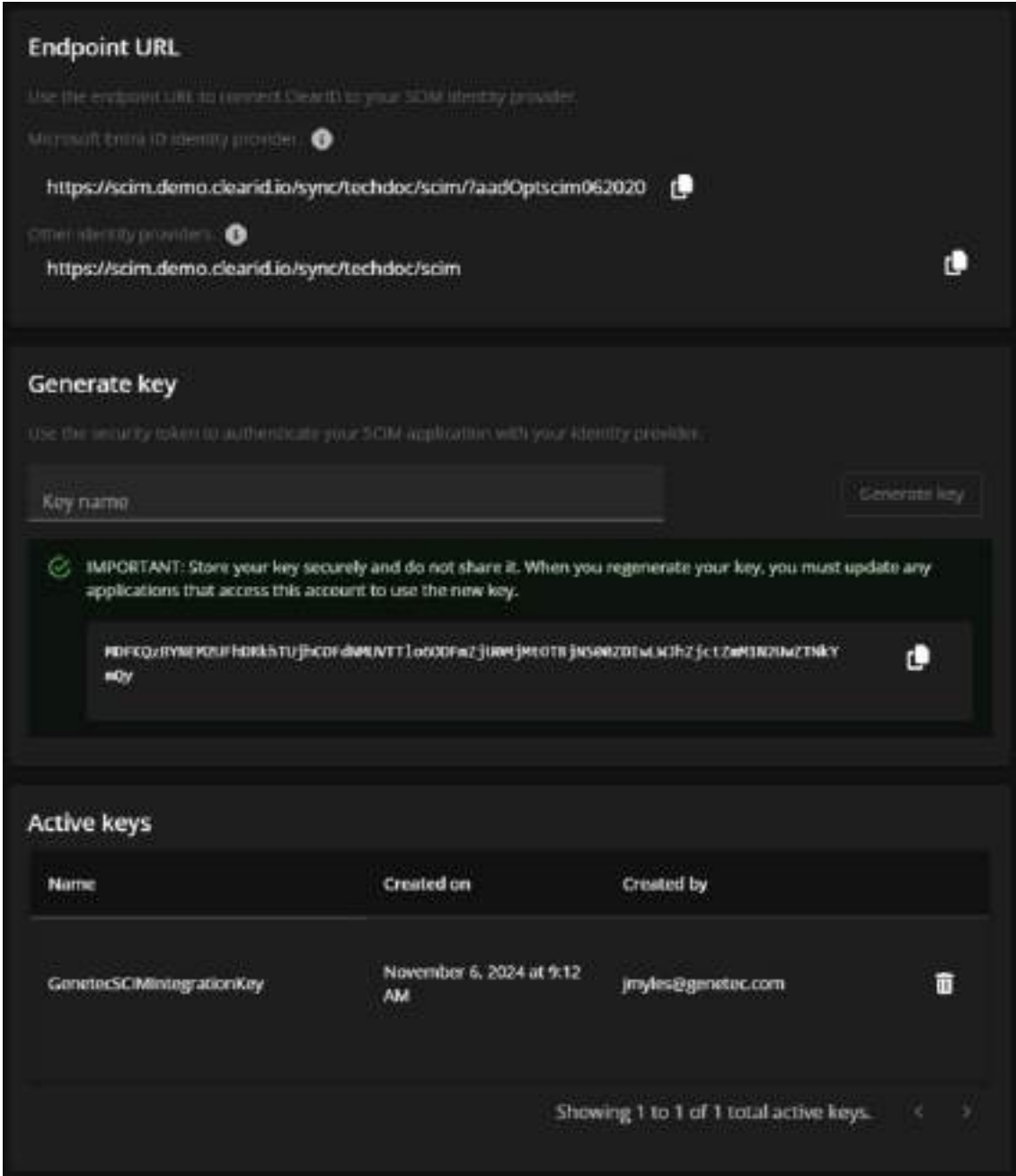
For your Genetec ClearID™ SCIM integration to communicate with Microsoft Entra ID, you must generate a System for Cross-domain Identity Management (SCIM) key.

What you should know

Only a ClearID portal *administrator* can perform this task.

Procedure

1. In the ClearID portal, click Administration > SCIM Integration.
2. In the Generate key section, enter a key name and click Generate Key.
For example, the key name could be GenetecSCIMIntegrationKey.



After you finish

Create your Microsoft Azure enterprise application.
Parent topic: Configuring the SCIM integration in ClearID

12.4.3.2 | Creating an enterprise application in Microsoft Azure

Synchronizing identities using the SCIM integration in ClearID >

Your organization can automate identity attribute provisioning using the Genetec ClearID™ SCIM integration with Microsoft Entra ID as the identity provider. To use the integration, you must first create an enterprise application in Microsoft Azure.

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

Procedure

- 1. In the Microsoft Azure portal, search for and click Enterprise applications.
- 2. In the Enterprise applications section, click New application.
- 3. Click Create your own application.

4. Select Integrate any other application you don't find in the gallery (Non-gallery).
5. Enter your application name and click Create.

For example, the application name could be ClearID SCIM Integration.

Create your own application

[Got feedback?](#)

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

ClearID SCIM Integration ✓

What are you looking to do with your application?

☐ Configure Application Proxy for secure remote access to an on-premises application

☐ Register an application to integrate with Microsoft Entra ID (App you're developing)

☒ Integrate any other application you don't find in the gallery (Non-gallery)

Create

NOTE: Watch for a successfully added notification in the upper right of the screen.

After you finish

Connect your ClearID SCIM integration to Microsoft Azure.

Parent topic: Configuring the SCIM integration in ClearID

12.4.3.3 | Connecting your ClearID SCIM integration to Microsoft Entra ID

Synchronizing identities using the SCIM integration in ClearID >

Before you can use the SCIM integration in Genetec ClearID™ to synchronize identity attributes, you must provide your credentials that connect the ClearID SCIM Integration API to Microsoft Entra ID.

Before you begin

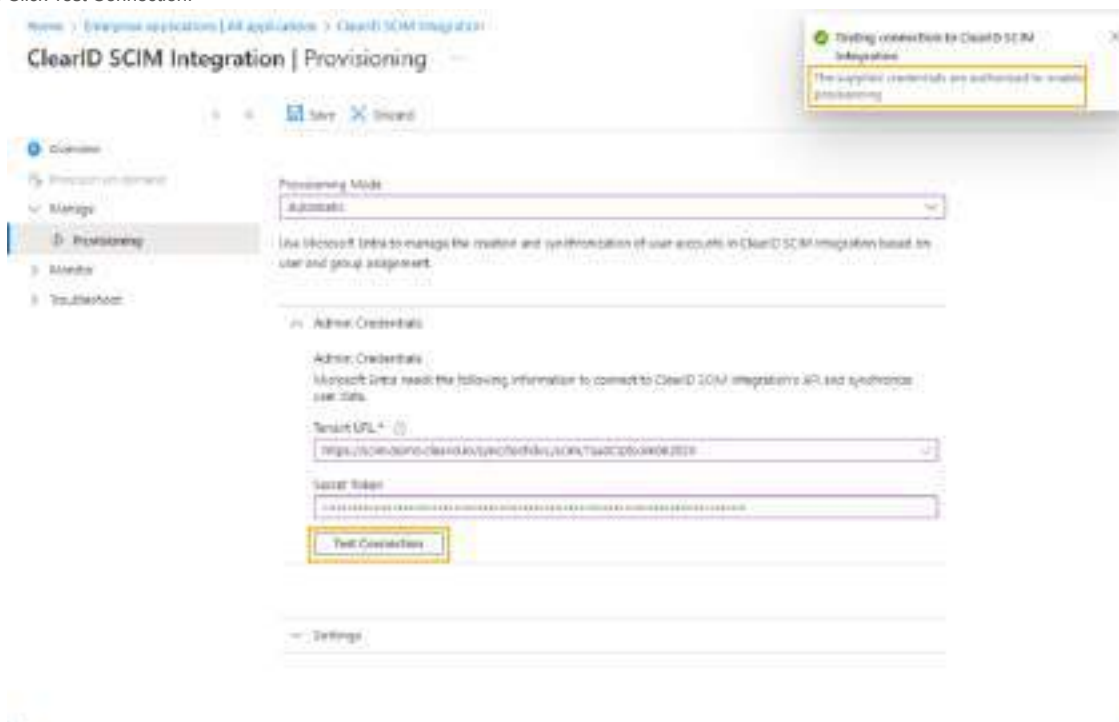
Create your Microsoft Azure enterprise application.

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

Procedure

1. In the Microsoft Entra ID portal, find and click Enterprise applications.
2. In the Enterprise applications section, search for and select your ClearID SCIM integration application.
3. In the Manage section, click Provisioning and then click Provisioning again.
4. From the Provisioning Mode list, select Automatic.
5. Expand the Admin Credentials section.
6. In the ClearID portal SCIM integration tab, locate the Endpoint URL section and click Copy to clipboard next to the Microsoft Entra ID identity provider.
The endpoint URL is copied to your clipboard.
7. Return to the Microsoft Entra ID Provisioning page and paste into the Tenant URL.
8. In the ClearID portal SCIM integration tab, locate the Generate key section and click Copy to clipboard.
9. Return to the Microsoft Entra ID Provisioning page and paste into the Secret Token field.
The SCIM key is used to authenticate your application with Entra ID.
10. Click Test Connection.



11. Click Save.
Tip: Watch for a successful update notification in the upper right of the screen.

After you finish

Disable your Microsoft Entra ID group settings.
Parent topic: [Configuring the SCIM integration in ClearID](#)

12.4.3.4 | Disabling Microsoft Entra ID groups setting in Microsoft Azure

[Synchronizing identities using the SCIM integration in ClearID](#) >

Genetec ClearID™ doesn't support the synchronization of groups. To prevent group settings or attributes from being synchronized, disable the Microsoft Entra ID Groups setting in your Microsoft Azure enterprise application.

Before you begin

[Connect your ClearID SCIM integration to Microsoft Azure.](#)

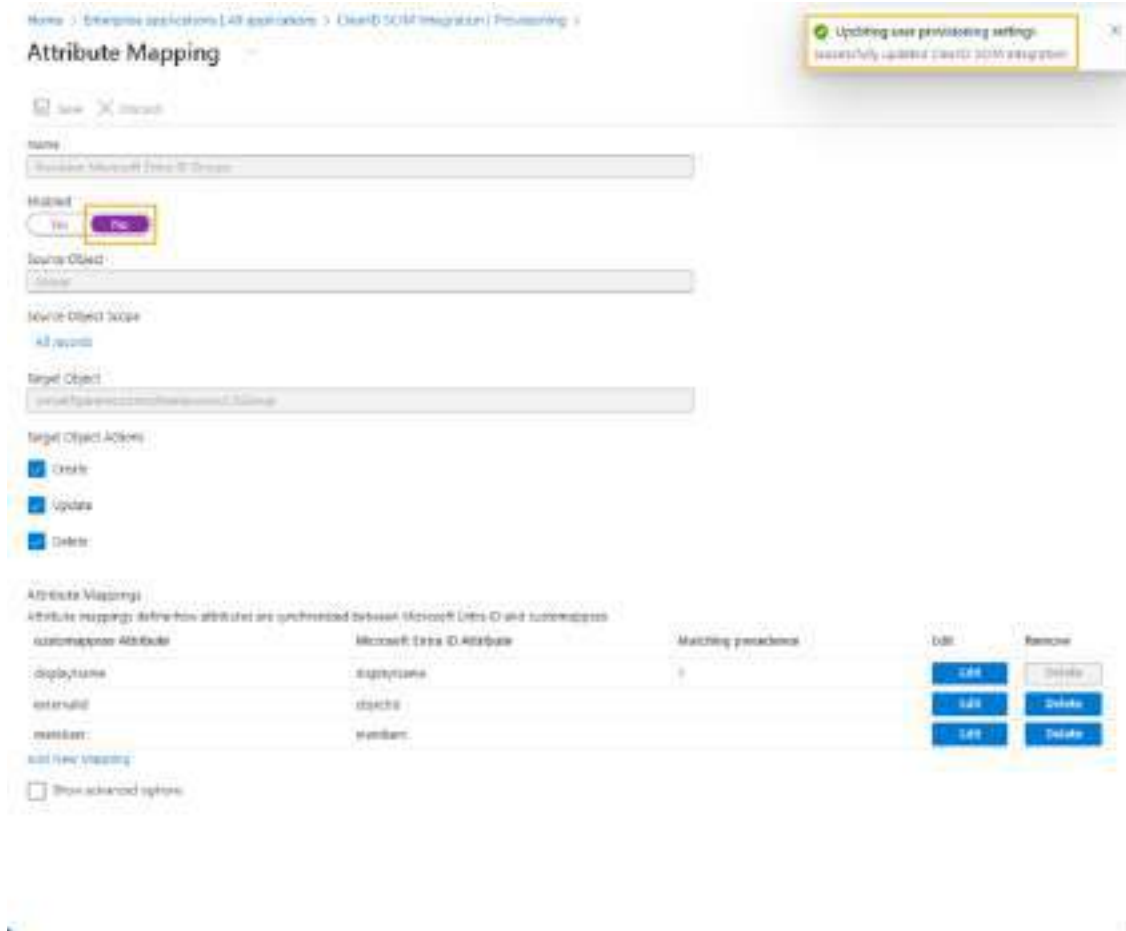
What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.
IMPORTANT: ClearID doesn't support group synchronization. This setting must be disabled.

Procedure

1. In the Microsoft Azure portal, search for and click Enterprise applications.
2. In the Enterprise applications section, search for and select your ClearID SCIM integration application.

3. In the Manage section, click Provisioning and then click Provisioning again.
4. Expand the Mappings section of the Provisioning page.
5. Click Provision Microsoft Entra ID Groups.
6. Move the Enabled slider to No.



7. Click Save and then click Yes to confirm your changes.
8. Close the window and return to the Provisioning page.
It might take a moment to refresh the page.

After you finish

Configure your Microsoft Entra ID user settings.

Parent topic: Configuring the SCIM integration in ClearID

12.4.3.5 | Configuring Microsoft Entra ID user settings in Microsoft Azure

Synchronizing identities using the SCIM integration in ClearID >

To define how identity data flows between Microsoft Entra ID and Genetec ClearID™, you must configure your user settings and map attributes for automatic synchronization.

Before you begin

Disable your Microsoft Entra ID groups setting.

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

Procedure

1. In the Microsoft Azure portal, search for and click Enterprise applications.
2. In the Enterprise applications section, search for and select your ClearID SCIM integration application.
3. In the Manage section, click Provisioning and then click Provisioning again.
4. Expand the Mappings section and click Provision Microsoft Entra ID Users.
5. Modify the default attribute mappings.
 - a. On the Attribute Mapping page, click Delete to remove unused default attributes.

Only keep the following:

- userName
- active
- displayName

Home > Enterprise applications > All applications > ClearID SCIM Integration > Provisioning > Attribute Mapping

Attribute Mapping

Save X Discard

Name:

Physical: ☒ Yes ☐ No

Source Object:

Source Object Scope:

Target Object:

Target Object Action: ☒ Create ☒ Update ☒ Delete

Attribute Mapping: Define how attributes are synchronized between Microsoft Entra ID and customappsso

Customappsso Attribute	Microsoft Entra ID Attribute	Mapping operation	Id	Remove
displayName	displayName	Equal	Edit	Delete
active	isActive	Equal	Edit	Delete
displayName	displayName	Equal	Edit	Delete

Click here to add new mapping.

☐ Show advanced options

b. Click Save and then click Yes to confirm your changes.

6. Modify the customappsso user attributes.

a. On the Attribute Mapping page, click Show advanced options.

b. Click Edit attribute list for customappsso, and then click Delete to remove all the unused default attributes.

Only keep the following:

- id
- active
- displayName
- title
- userName

Home > Enterprise applications > All applications > ClearID SCIM Integration > Provisioning > Attribute Mapping > Edit Attribute List

Edit Attribute List

Save X Discard

Customappsso User Attributes

Name	Type	Memory key?	Required?	Multi-valued	Start date?	API Expression	Reference class
id	String	☒	☒	☐	☐		
active	Boolean	☐	☐	☐	☐		
displayName	String	☐	☐	☐	☐		
title	String	☐	☐	☐	☐		
userName	String	☐	☒	☐	☐		
	String	☐	☐	☐	☐		

Type

- Setting the attribute to inform the provisioning server what attributes exist in your system. Setting this for user attributes will result in the system of that system.
- Users' Profile: View for user attributes unless indicated by documentation. Requires a JSON-encoded object.
- Leave Reference Class attribute blank unless the "Type" is set to "Reference". Enter referenced attribute in the form of objectName.className or just className.
- See the online documentation on attribute editing.

c. Click Save and then click Yes to confirm your changes.

7. Add the ClearID schema attributes.

Only include the list of attributes available to ClearID:

Code

```
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:description
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:firstName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:lastName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:middleName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:countryCode
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:email
```

Genetec ClearID®; User Guide

Displayed in the header

```
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:employeeNumber
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:secondaryEmail
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:cityOfResidence
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:stateOfResidence
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:zipCode
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberPrimary
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberSecondary
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:supervisorName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:departmentName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:jobTitle
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:companyName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeDescription
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeCode
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasExtendedTime
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:externalId
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasWebPortalAccess, Boolean
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:isAdmin, Boolean
```

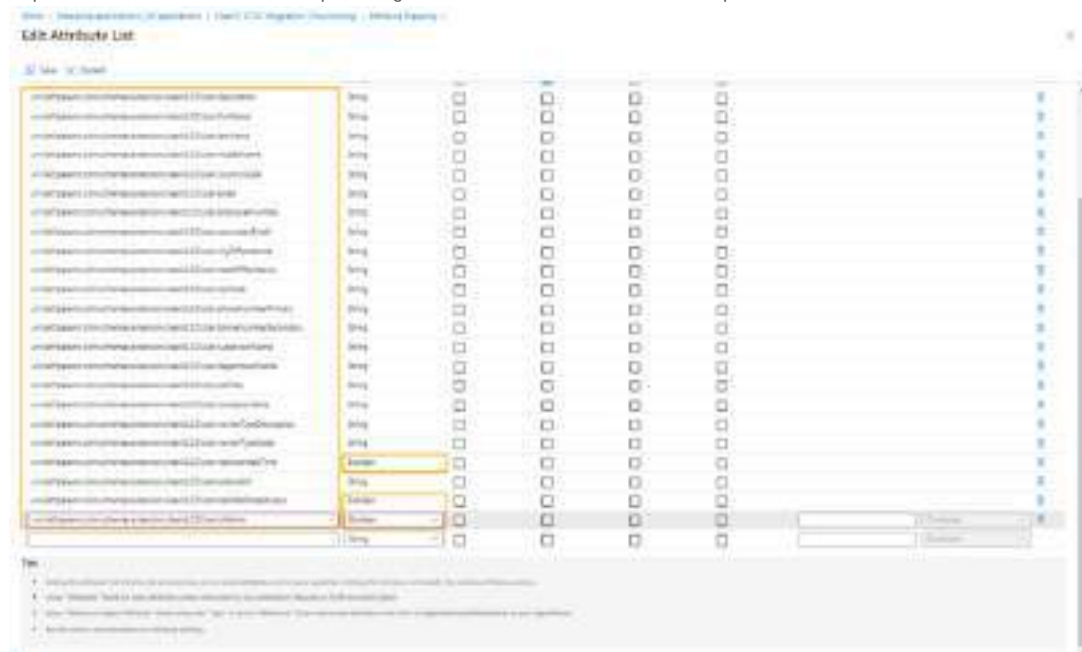


- a. On the Edit Attribute List page, copy and paste an attribute name from the preceding ClearID schema attributes code example into the Name field and select the attribute Type.

Almost every attribute has the type String, except for three attributes that have the Boolean type: hasExtendedTime, hasWebPortalAccess, and UserisAdmin.

IMPORTANT: The ClearID externalId attribute is the unique identifier that ClearID uses for synchronization. It's mapped to the unique objectId attribute in Microsoft Entra ID.

- b. Repeat for each attribute listed in the preceding ClearID schema attributes code example.



- c. Click Save and then click Yes to confirm your changes.

8. Add the ClearID attribute mappings.

- a. On the Attribute Mapping page, click Add New Mapping.
- b. On the Edit Attribute page, add the attributes that you require from the attributes added earlier in step 7.

Include the following:

- Mapping type: Direct
- Source attribute: objectId
- Target attribute: <your attribute value>

- c. Click OK.

- d. Repeat for each attribute added earlier and replace the target attribute value with the next attribute you want to add.

For a successful first synchronization, you need the following attributes. You can add more attributes later.

Attribute Mapping

Name: [Text Field]

Source: [Dropdown Menu]

Source Object: [Text Field]

Source Object Label: [Text Field]

Target Object: [Text Field]

Target Object Label: [Text Field]

Attribute Mapping

Source Object Attributes	Target Object Attributes
displayName	displayName
mail	mail
givenName	givenName
sn	sn
surname	surname
objectid	objectid
givenName	givenName
sn	sn
surname	surname
objectid	objectid

Mapping precedence

Add	Remove
[Add]	[Remove]
[Add]	[Remove]
[Add]	[Remove]
[Add]	[Remove]
[Add]	[Remove]

Advanced options

Supported attributes

The attributes for Microsoft Entra ID are listed in the table below. Select the attributes you want to synchronize.

NOTE: The objectid is the GUID in azure. There's no way to manipulate the objectid of a user in Azure. It's a hard-coded field that can't be modified.

e. Click Save and then click Yes to confirm your changes.

You can now close the window and return to the Provisioning page.

After you finish

Configure the ClearID SCIM integration synchronization settings.

Parent topic: Configuring the SCIM integration in ClearID

12.4.3.6 | Configuring the ClearID SCIM integration synchronization settings in Microsoft Azure

Synchronizing identities using the SCIM integration in ClearID >

To determine what identity data is synchronized to Genetec ClearID™, you must select the required synchronization settings and activate provisioning in Microsoft Azure.

Before you begin

Configure your Microsoft Entra ID user settings.

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

Procedure

1. On the Provisioning page, click Settings and choose which users to synchronize to ClearID:

Sync all users and groups

Synchronizes everything in Microsoft Entra ID.

Sync only assigned users and groups

Only selected users and groups are synchronized.

IMPORTANT: ClearID doesn't support group synchronization. Depending on the provisioning settings that you select, either all users identity data or only selected users identity data is synchronized.

2. If you chose Sync all users and groups, in the Provisioning status section, move the slider to On and click Save.

Home > Enterprise applications > All applications > ClearID SCIM integration

ClearID SCIM Integration | Provisioning

Save Discard

- Overview
- Provision on demand
- Manage
 - Provisioning
 - Users and groups
 - Expression builder
- Monitor
- Troubleshoot

Provisioning Mode:
Automatic

Use Microsoft Entra to manage the creation and synchronization of user accounts in ClearID SCIM integration based on user and group assignment.

Admin Credentials

Mappings

Mappings allow you to define how data should flow between Microsoft Entra ID and your app.

Name	Enabled
Provision Microsoft Entra ID groups	No
Provision Microsoft Entra ID users	No

☐ Restore default mappings

Settings

☐ Send an email notification when a failure occurs

☐ Prevent accidental deletion

Scope
Sync all users and groups

Provisioning Status
☒ On ☐ Off

3. If you chose Sync only assigned users and groups, complete the provisioning settings.
 - a. Click Users and groups in the left navigation bar.
 - b. Click Add group.
 - c. Click None selected, search for and select the group you want to add, and click Select.
 - d. Click Assign and repeat for each group that you want to add.
 - e. Return to the Provisioning page and click Settings.
 - f. In the Provisioning status section, move the slider to On and click Save.

Home > Enterprise applications > All applications > ClearID SCIM integration

ClearID SCIM Integration | Provisioning

Save Discard

- Overview
- Provision on demand
- Manage
 - Provisioning
 - Users and groups
 - Expression builder
- Monitor
- Troubleshoot

Provisioning Mode:
Automatic

Use Microsoft Entra to manage the creation and synchronization of user accounts in ClearID SCIM integration based on user and group assignment.

Admin Credentials

Mappings

Settings

☐ Send an email notification when a failure occurs

☐ Prevent accidental deletion

Scope
Sync only assigned users and groups

Provisioning Status
☒ On ☐ Off

After you finish

Review the ClearID SCIM integration synchronization status.
Parent topic: [Configuring the SCIM integration in ClearID](#)

12.4.4 | Resetting SCIM integration identity data in ClearID

To resolve issues with identity data, you can reset and replace all System for Cross-domain Identity Management (SCIM) integration identity data in Genetec ClearID™. This reset process uses the latest values from Microsoft Entra ID.

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

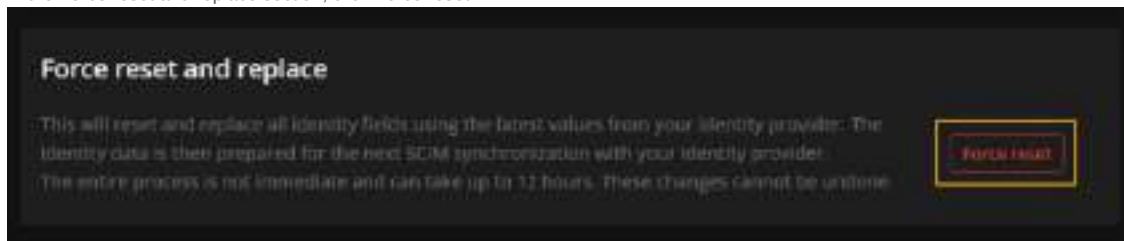
Only use this reset to resolve an identity data issue. For example, after your identity data has been manually manipulated, when there's a discrepancy, or when identity data has been deleted in ClearID.

The reset will prepare identity data for the next SCIM synchronization between ClearID and Microsoft Entra ID. This process only pushes identity data changes in one direction, to Entra ID.

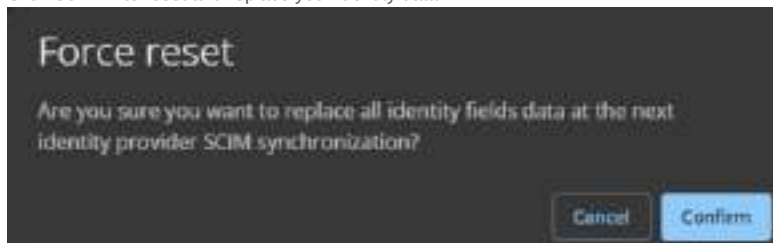
IMPORTANT: The entire process can take up to 12 hours. These changes can't be undone.

Procedure

1. In the ClearID portal, click Administration > SCIM Integration.
2. In the Force reset and replace section, click Force reset.



3. Click Confirm to reset and replace your identity data.



After you finish

Check the SCIM integration synchronization status to confirm that your identity data has been reset.
Parent topic: [Synchronizing identities using the SCIM integration in ClearID](#)

12.4.5 | Reviewing the SCIM integration synchronization status in Microsoft Azure

You can check the overall status of the System for Cross-domain Identity Management (SCIM) integration identity synchronization. You can also review the provisioning logs in Microsoft Azure to see more granular details about Genetec ClearID™ SCIM integration synchronization activities related to a specific person or identity.

What you should know

This procedure is for the ClearID deployment team, your IT department, or the people responsible for administering Microsoft Entra ID in your organization.

The provisioning logs can be used to verify whether the ClearID SCIM integration is correctly configured and operational. If there are any issues with the configuration, error messages are generated and recorded in the provisioning logs.

Procedure

1. In the Microsoft Azure portal, find and click Enterprise applications.
2. In Enterprise applications, select your SCIM integration application.

3. On the Overview page, check whether the last synchronization completed successfully and when the last synchronization occurred.



4. (Optional) Click View provisioning logs to see more granular information about identity synchronization.



NOTE: If the log details are long, the Provisioning Logs page includes useful filters to manipulate the data for your needs.

Parent topic: Synchronizing identities using the SCIM integration in ClearID

12.5 | Synchronizing identities using One Identity Synchronization Tool in ClearID

Use the Genetec ClearID™ One Identity Synchronization Tool to synchronize external system attributes into Genetec ClearID™ identity attributes. These identity attributes in ClearID can then be used to assign people to roles and automate role-based access control.

What you should know

Using the One Identity Synchronization Tool you can synchronize external system attributes from the following data sources:

- Azure AD
- Database (Microsoft SQL Server, Oracle Database, ODBC)
- File (CSV)

Procedure

1. Learn about the One Identity Synchronization Tool.
2. Learn about One Identity attribute fields.
3. Learn about the Azure web app.
4. Install the One Identity Synchronization Tool.
5. Configure the One Identity Synchronization Tool.
6. Review synchronization status.

Browse

- ClearID One Identity Synchronization Tool connectivity issues
- ClearID One Identity Synchronization Tool data synchronization issues

12.5.1 | About the ClearID One Identity Synchronization Tool

The Genetec ClearID™ One Identity Synchronization Tool is a Windows service that you can use to import identities information from an external system into Genetec ClearID™.

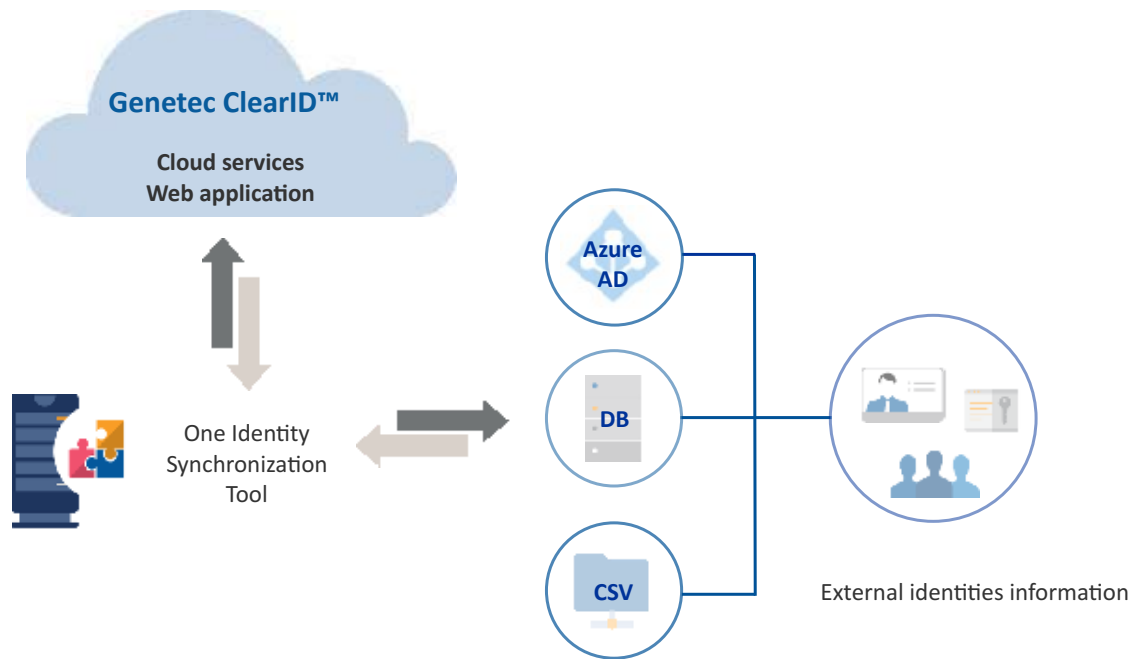


The ClearID One Identity Synchronization Tool includes the following components:

- Genetec.ClearID.OneIdentity.SynchronizationTool (OneIdentityConfigurationTool.exe) is the user interface component of the windows application that is used to configure the Synchronization Tool.
- Genetec.ClearID.OneIdentity.SynchronizationService (OneIdentityService.exe) is the Windows service component of the application that performs external system attributes to ClearID identity attributes synchronization automatically in the background at intervals specified in the Synchronization Tool.

Data sources

You can select one or more data sources to be synchronized from an external system. Using the Data sources configuration dialog you configure the Data sources and map the One Identity attributes to their associated external system attributes.



Azure Active Directory

The Azure AD data source is an Azure Active Directory that you can import identities information from. For example, importing identities, credentials, and pictures into ClearID.

Database

The database data source can be a Microsoft SQL Server database, an Oracle database, or an ODBC-compliant database that follows the one identity attribute mapping. The database must be accessible from the server where the ClearID One Identity Synchronization Tool is installed. One database can contain one table or view for identities information.

File

The file data source is a delimited text file. For example, a CSV file that follows the one identity attribute mapping, and must be accessible from the server where the ClearID One Identity Synchronization Tool is installed. Each file contains identities information.

Synchronization

Identities in ClearID can come from a variety of data sources (Databases, HR, External Sources) and can be synchronized using various tools (Genetec ClearID™ LDAP Synchronization Agent, Genetec ClearID™ API, or Genetec ClearID™ One Identity Synchronization Tool).

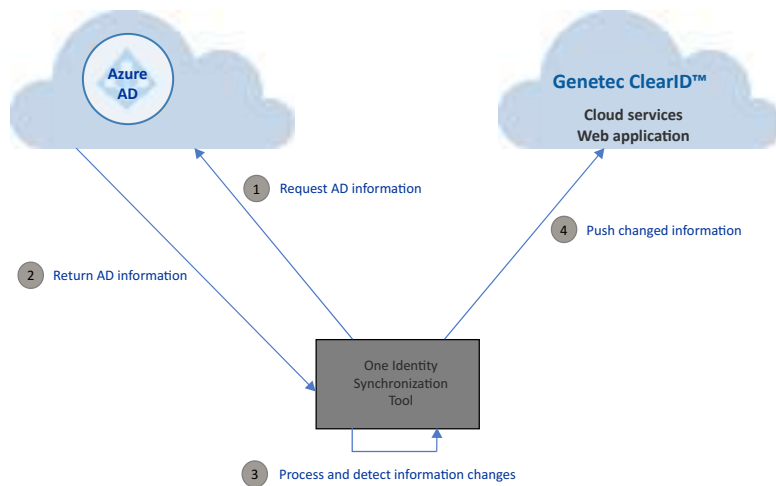
- LDAP is typically used for Active Directory attributes synchronization into ClearID identities.
- API is typically used for real-time updates. For example, to remove people quickly. This API synchronization option is the most flexible but it is expensive.
- One Identity is typically used for HR systems. For example, to synchronize all employees every day or every 4hrs. The ClearID One Identity Synchronization Tool is configured to synchronize at the same frequency.

One Identity data synchronization

The following information describes One Identity synchronization:

- Synchronization of external system attributes into ClearID identity attributes is INBOUND only.
CAUTION:
Any changes only made to identities in ClearID can be overwritten by the next synchronization from the external system.
- Synchronization can be performed manually using the Synchronize now (🔴) option, or automatically at the Automatic synchronization intervals specified in the One Identity Synchronization Tool.
 - For each One Identity field that is configured, a custom mapping to the External field in the external system is created. This mapping ensures that the external system attributes can be synchronized into the One Identity attribute fields.

The following diagram illustrates an Azure AD data synchronization:



The synchronization workflow is essentially the same for all data sources:

1. Data source information is requested.
2. Data source information is returned.
3. Any information changes are processed and detected.
4. Data source information is pushed to the ClearID web application.

Sample SQL files

For the Database data source option, sample SQL script files are provided with the tool and can be found here:

Code

C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service



- Identities_Oracle.sql
- Identities_SqlServer.sql

The sample SQL script files can be used to test the Database data source solution, or to help you understand the SQL data format.

Sample CSV files

For the File data source option, a sample CSV file is provided with the tool and can be found here:

Code

C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service



- Identities.csv

The sample CSV files can be used to test the File data source solution, or to help you understand the CSV data format.

Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.2 | About ClearID One Identity Synchronization Tool attribute fields

When you synchronize an external system with Genetec ClearID™ using the Genetec ClearID™ One Identity Synchronization Tool, your external system attributes are synchronized (imported) into ClearID identity attributes using the field mappings in the One Identity Synchronization Tool.

NOTE: The data source order is important because the first data source always overrides common fields.

Identity attributes

One Identity field	Data type	Description
Unique ID*	Text field	A unique ID for the identity. The unique ID can be an alphanumeric code or an email address. For example, Employee number xyz12345. IMPORTANT: (Azure Active Directory only) If you ever change the mapping of the Unique ID it can cause duplicate data issues.
* This field is mandatory.		

Genetec ClearID®; User Guide

Displayed in the header

One Identity field	Data type	Description
Activation date	DateTime	The date that the identity is activated. For example, 1/11/2022. NOTE: All invariant culture DateTime formats are supported.
City	Text field	The city where the identity is located. For example, Paris.
Company	Text field	The company name. For example, Genetec™.
Country code	Text field	The three letter country code (UPPERCASE). For example, the USA or CAN. NOTE: The three-letter country codes are based on the Alpha-3 codes in the ISO 3166-1 country codes standard.
Date of birth	DateTime	The identity's date of birth. For example, 7/21/2022. NOTE: All invariant culture DateTime formats are supported.
Department	Text field	The department name. For example, IT or Marketing.
Description	Text field	The identity description.
Email address	Text field	The primary email address (business email) for the identity. For example, johndoe@test.com
Employee number	Text field	The identity's employee number.
Expiration date	DateTime	The date that the identity expires. NOTE: All invariant culture DateTime formats are supported.
First name	Text field	The first name of the identity.
Job title	Text field	The job title of the identity.
Last name	Text field	The last name of the identity.
Middle name	Text field	The middle name of the identity
Mobile phone number	Text field	The secondary phone number (Mobile phone number) For example, 555-555-5555.
Personal email	Text field	The secondary email address (personal email) for the identity. For example, johndoe2@test.com
Phone number	Text field	The primary phone number (Office phone number) For example, 555-555-5555.
Picture	Image	A picture in the format of a blob, a base64 string, or a path to an image. Supported values: - File path - uses a standard windows file path. The path must be accessible from the server. - base64 encoded string - uses a standard base 64 encoding. - Binary - binary data. Supported Image formats: png, jpeg, and bmp.
Preferred name	Text field	The preferred name of the identity.
Provisioning attributes	Text field	Provisioning attributes as defined and configured by the customer for their environment. The list items are separated by a pipe character " ". For example, A1 A2 A3.
State or province	Text field.	The state or province where the identity is located.
Status	Text field	The Identity activation status. For example, Active or Inactive.
Supervisor name	Text field	The name of the identity's supervisor.
Supervisors	Text field	The list of unique supervisor IDs for the identity. The list items are separated by a pipe character " ". For example, A1 A2 A3.
Use extended grant time	Boolean value	The value that enables or disables the Use extended grant time option. For example, TRUE or FALSE.

One Identity field	Data type	Description
User type	Text field	The type of user. For example, Admin or User.
Username	Text field	The email used by the identity to log on to ClearID.
Web portal access	Text field	The value that enables or disables web portal access. For example, 0 FALSE or 1 TRUE.
Worker type code	Text field	The worker type code.
Worker type description	Text field	The worker type description.
Zip or postal code	Text field.	The Zip or postal code of the identity's location.

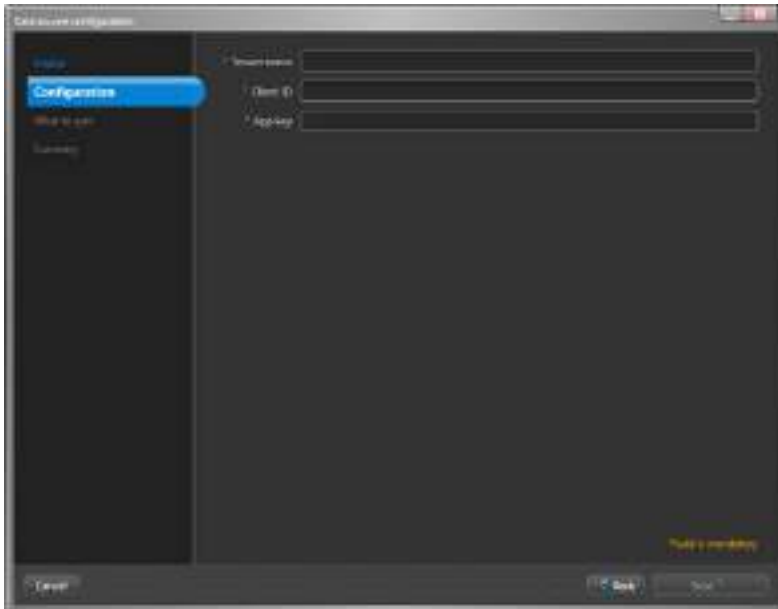
Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.3 | About the Azure web app for ClearID One Identity Synchronization Tool

The Azure web app is a web application that is used to connect Genetec ClearID™ One Identity Synchronization Tool to the Azure AD data so that the Active Directory user information can be accessed and synchronized.

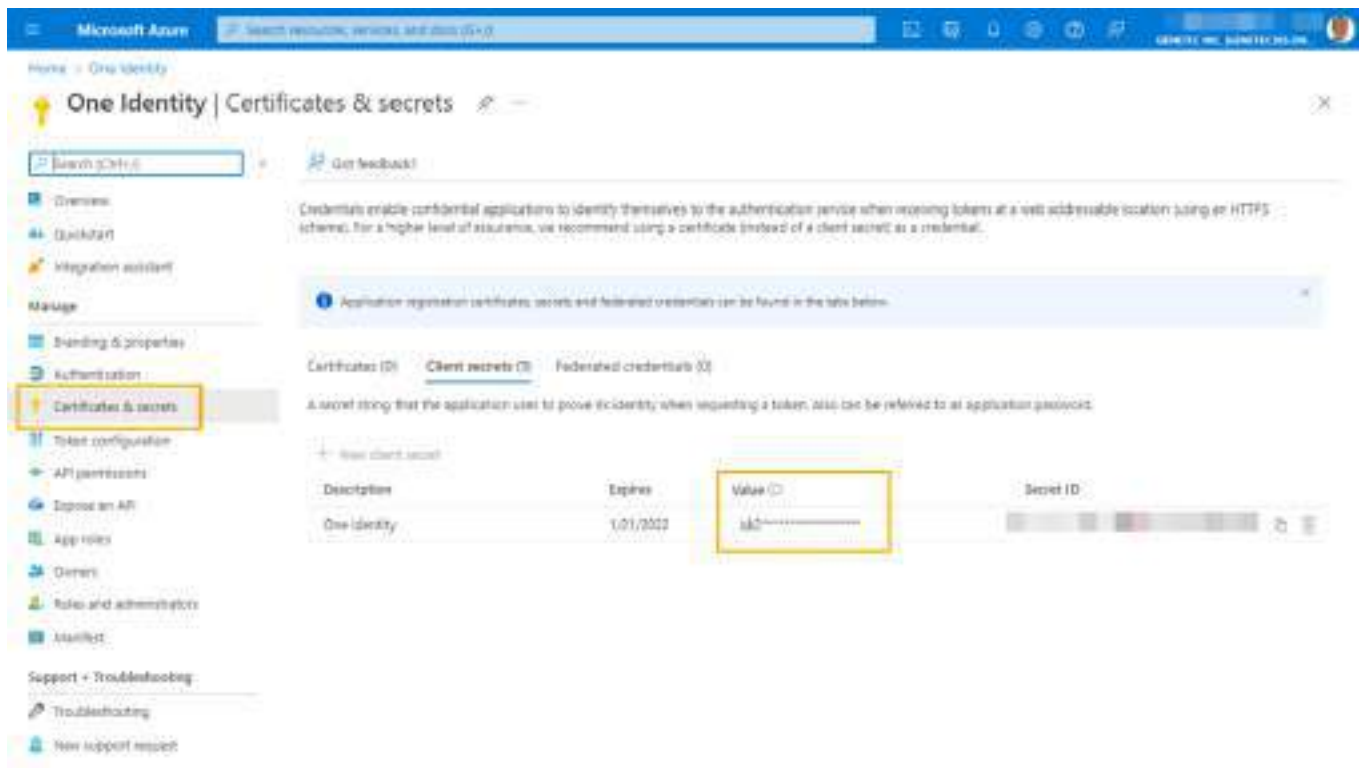
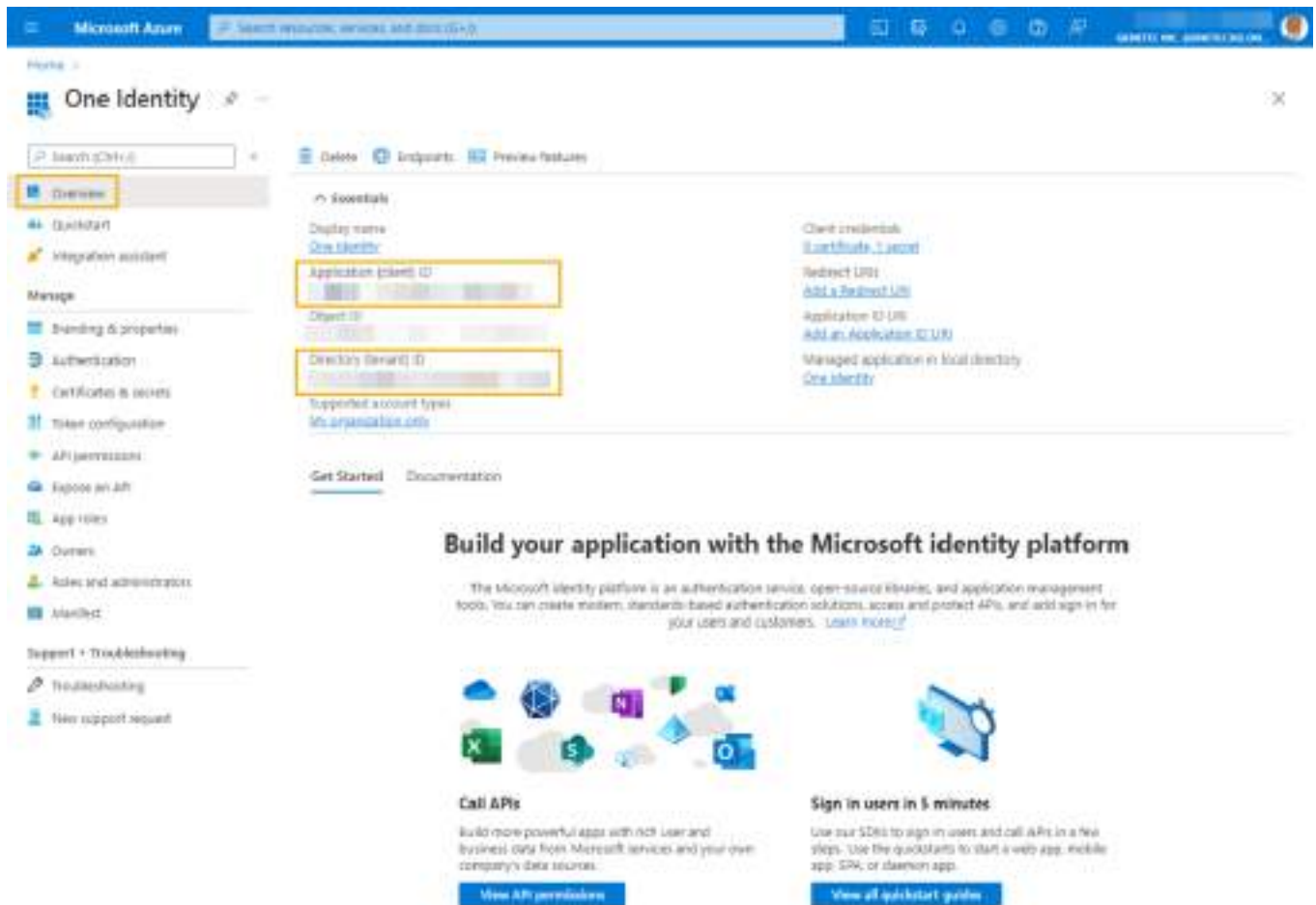
Connection information for Azure web app

To connect the Azure web app to the ClearID One Identity Synchronization Tool, you need the following information:



- Tenant name (Directory ID for account)
- Client ID (Application ID)
- App key (Client secret value)

Tip: The Tenant name, Client ID, and App key can be obtained from your Azure Active Directory application registration.



Azure AD API permissions

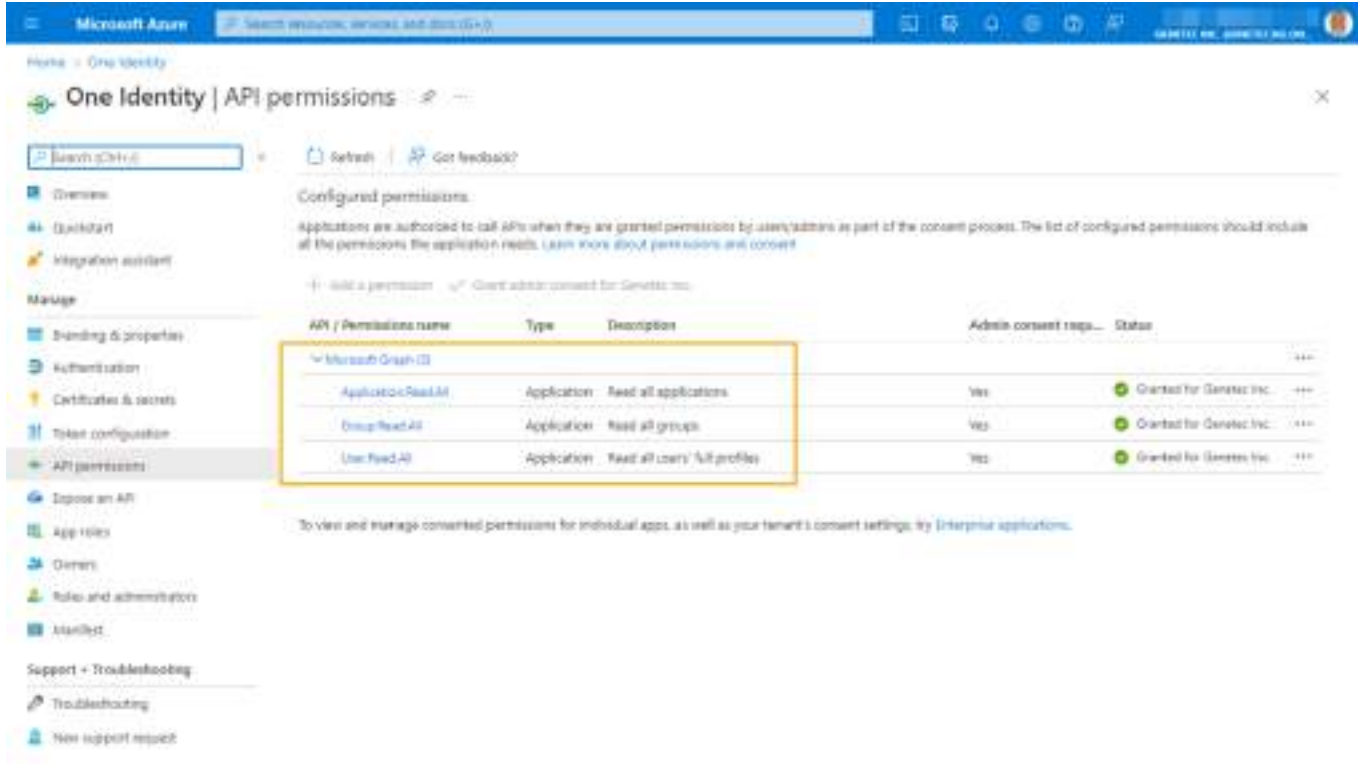
Before you can synchronize data with ClearID, an external system attributes administrator (IT or security personnel) must set up and configure the following API read permission privileges in Azure AD.

Microsoft Graph (minimum requirements):

- *Application.Read.All* - Used to get extensions attributes.
 - Allows the app to read applications and service principals without a signed-in user.

For more information, see [List extensionProperties \(directory extensions\)](#)

- *User.Read.All* - Used to get user information.
 - Allows the app to read identity user risk information for all users in your organization without a signed-in user.
- *Group.Read.All* - Used to get group information.
 - Allows the app to read group properties and memberships, and read conversations for all groups, without a signed-in user.



For more information, see [Microsoft Graph permissions reference](#).

Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.4 | Installing the ClearID One Identity Synchronization Tool

Before you can import identities information from an external system into Genetec ClearID™, you must first install the Genetec ClearID™ One Identity Synchronization Tool.

Before you begin

Obtain the latest installer package from your deployment contact.

What you should know

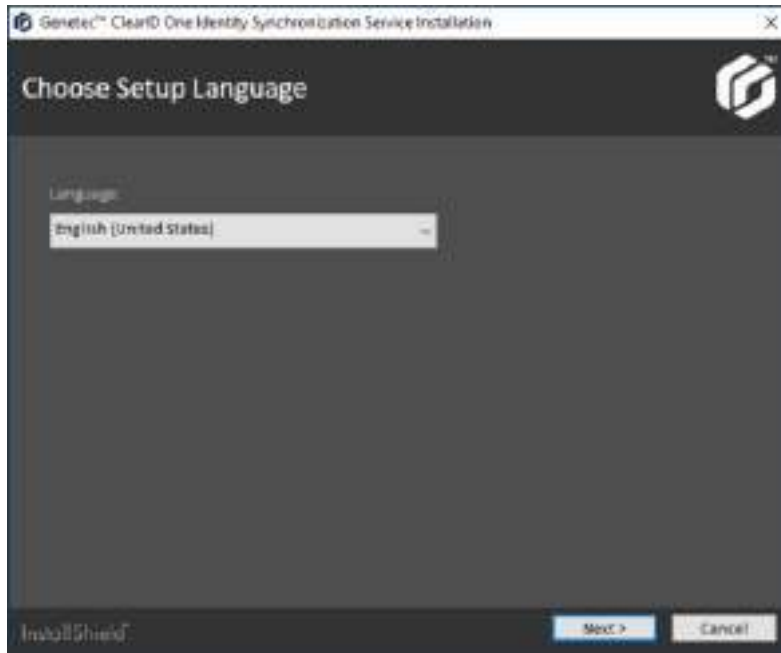
This procedure is for IT or security personnel responsible for external system attributes administration.

Install the One Identity Synchronization Tool on its own dedicated server. It does not require a Security Center server.

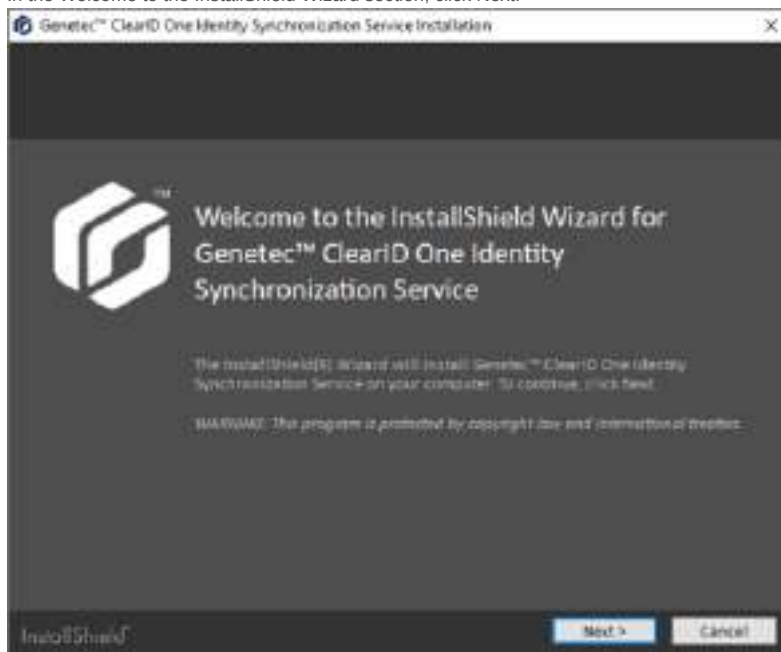
NOTE: The One Identity Synchronization Tool is not generally available as a public download. The synchronizer download is supplied by your Deployment contact when needed.

Procedure

1. Navigate to the ClearID One Identity Synchronization Tool installer supplied by your deployment contact.
2. Right-click the setup.exe file. Then click Run as administrator and follow the installation instructions.
3. In the Genetec ClearID™ One Identity Synchronization Service Installation dialog, select a setup language and click Next.



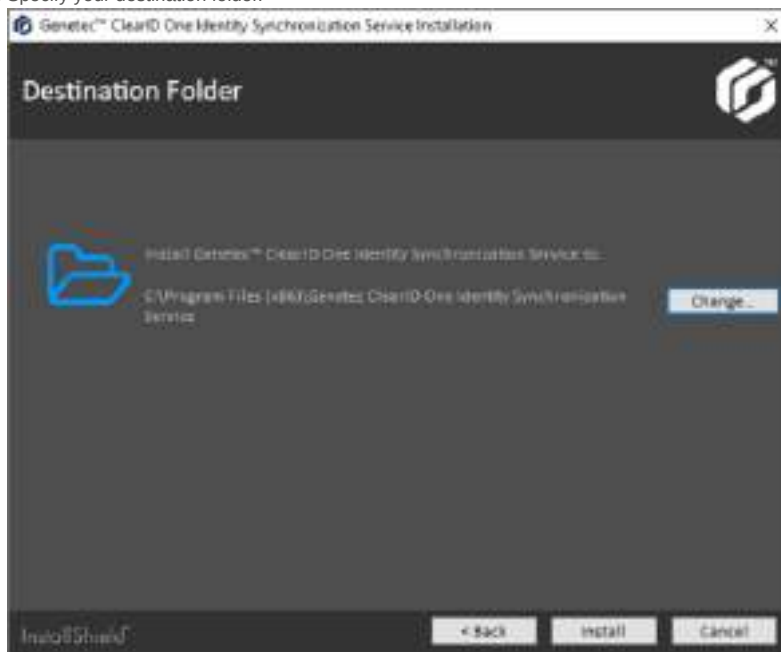
4. In the Welcome to the InstallShield Wizard section, click Next.



5. Review and accept the license agreement, then click Next.



6. Specify your destination folder.

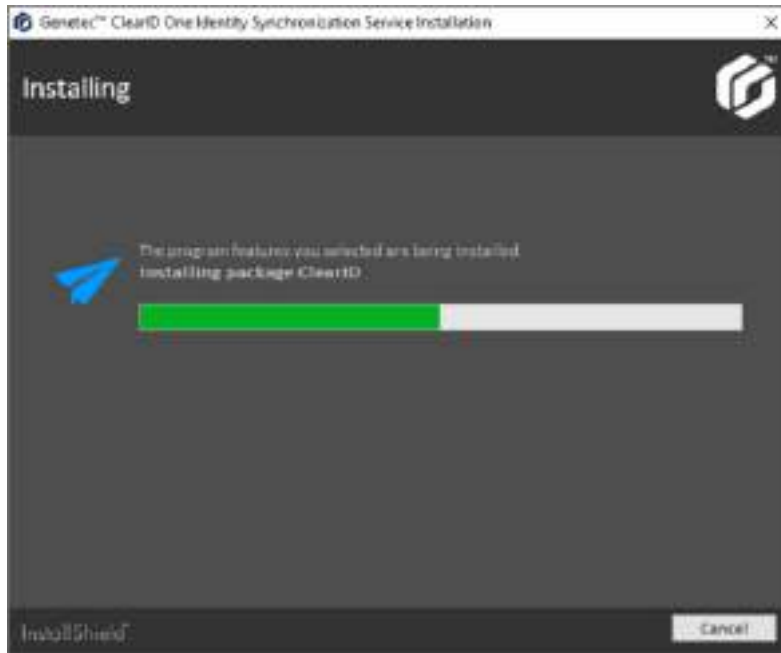


By default the service is installed at C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service.

7. (Optional) Click Change to modify the destination folder.

a. In the Browse For Folder dialog, browse to and select the folder where you want the service installed and click OK.

8. Click Install.



9. Click Finish to complete the installation.



Results

The ClearID One Identity Synchronization Tool is now installed.

After you finish

Configure the synchronization tool.

Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.4.1 | Uninstalling the ClearID One Identity Synchronization Tool

[Synchronizing identities using One Identity Synchronization Tool in ClearID](#) >

From time to time, you might want to uninstall the Genetec ClearID™ One Identity Synchronization Tool to fix a problem or install an updated version.

Before you begin

The Genetec ClearID One Identity Synchronization Tool must be installed.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

Genetec ClearID®; User Guide

Displayed in the header

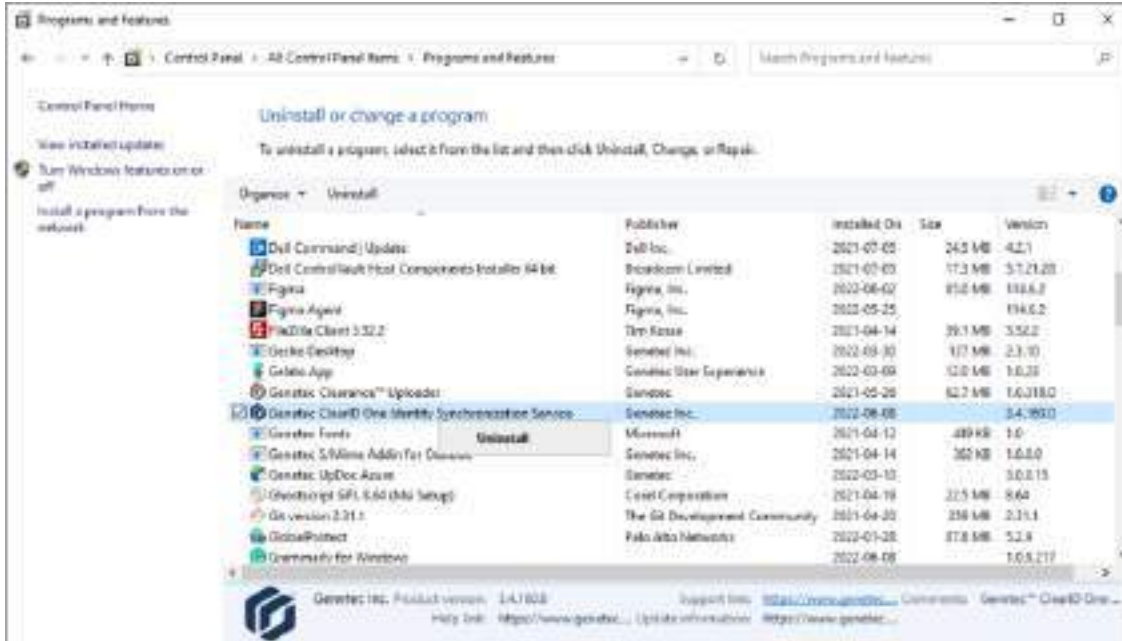
- The options that you encounter while uninstalling a program (service) might vary depending on the version of Windows that you are running.
- This procedure describes how to uninstall the synchronization tool (service) from a Windows 10 client.

CAUTION:

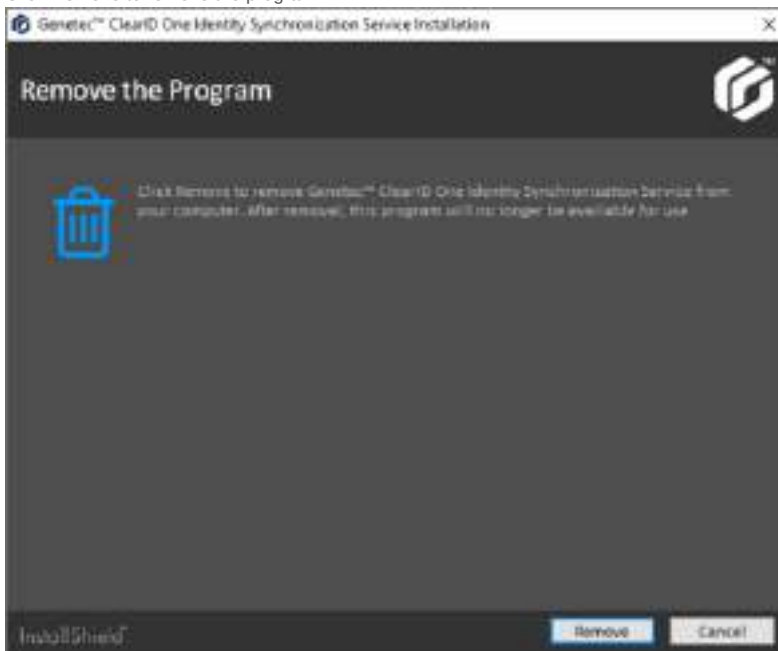
The uninstall process deletes all configuration data. If you are upgrading, make sure that you back up your program data in the configuration folder C:\ProgramData\Genetec\OneIdentity\Configuration.

Procedure

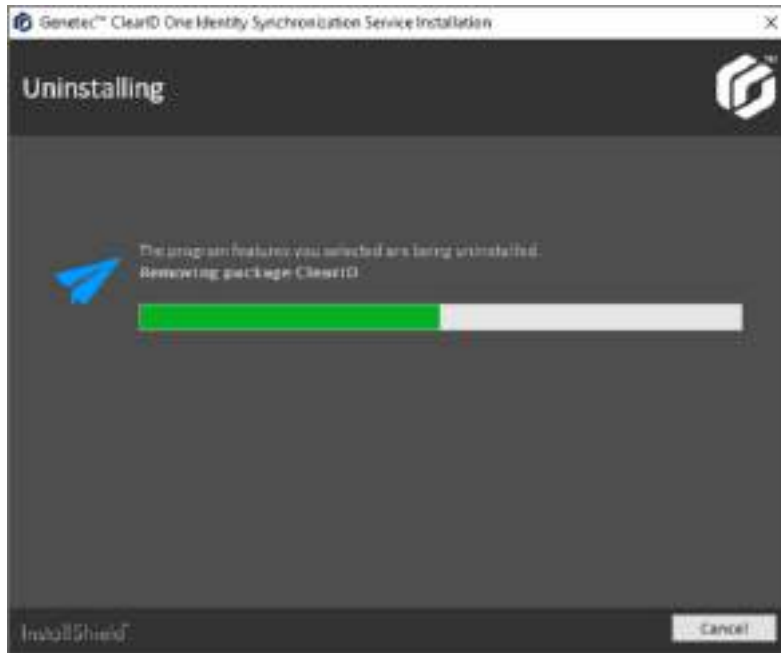
1. Open the Windows Control Panel, and in the Programs section click Uninstall a program to access Programs and Features.
2. Find the ClearID One Identity Synchronization Tool service and right-click to display the Uninstall option, then click Uninstall.



3. Click Remove to remove the program.



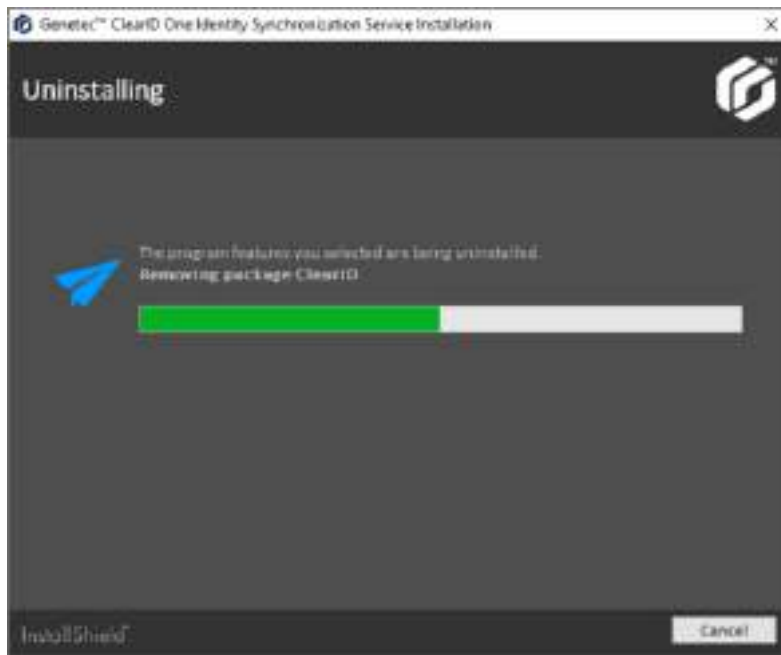
The program uninstall begins.



4. (Optional) If the following dialog is displayed, select Automatically close and attempt to restart applications then click OK.



The package continues to uninstall.



5. Click Finish to complete the uninstall.



Results

The ClearID One Identity Synchronization Tool has now been uninstalled.
Parent topic: [Installing the ClearID One Identity Synchronization Tool](#)

12.5.4.2 | Upgrading the ClearID One Identity Synchronization Tool

[Synchronizing identities using One Identity Synchronization Tool in ClearID >](#)

Upgrade Genetec ClearID™ One Identity Synchronization Tool to the latest version when it becomes available so that you can use new features.

Before you begin

The Genetec ClearID One Identity Synchronization Tool must be installed.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

Procedure

1. Back up the configuration folder C:\ProgramData\Genetec\OneIdentity\Configuration.
The folder contains configuration settings. For example, ApiConfiguration.dat, ClearIdEntityMappingFile.xml, Configuration.xml, and SingleCardEntityMapping.xml.
NOTE: The .dat or .xml files that you encounter in the configuration folder vary depending on the settings that you configure in the ClearID One Identity Synchronization Tool.
2. Uninstall ClearID One Identity Synchronization Tool (previous version).
3. Install ClearID One Identity Synchronization Tool (latest version).
4. Validate the ClearID One Identity Synchronization Tool is working as expected.
NOTE: You should have the same data source configurations as before the upgrade.

Results

The ClearID One Identity Synchronization Tool has now been upgraded.
Parent topic: [Installing the ClearID One Identity Synchronization Tool](#)

12.5.5 | [Configuring the ClearID One Identity Synchronization Tool](#)

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool.

Before you begin

- [Familiarize yourself with the One Identity attribute fields.](#)
- Verify the identities attributes values that you want to import and synchronize before synchronizing.
- [Download a service authentication key.](#)
- [Install the One Identity Synchronization Tool.](#)
- Check your license information: Part number CD-IDSYNC-SERVICE-1Y is required for One Identity Synchronization Tool import.

IMPORTANT: Make sure that the file is not being edited and is closed, because the synchronization tool locks the file during the synchronization process.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.
Synchronization of external system attributes into ClearID identity attributes is INBOUND only.
CAUTION:
Any changes only made to identities in ClearID can be overwritten during the next synchronization from the external system.

Procedure

1. [Configure your connection settings.](#)
2. Configure data source settings for one of the following sources:
 - [Azure AD](#)
 - [Database \(Microsoft SQL Server, Oracle Database, ODBC\)](#)
 - [File \(CSV\)](#)
3. Configure your synchronization settings.
4. Click Save.

After you finish

[Verify that the new attributes from the external system have been synchronized and contain the correct attributes.](#)
Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.5.1 | [Configuring connection settings for the ClearID One Identity Synchronization Tool](#)

[Synchronizing identities using One Identity Synchronization Tool in ClearID](#) >

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool connection settings.

Before you begin

- [Verify the identities attributes values that you want to import before synchronizing.](#)
- [Download a service authentication key.](#)
- Check your license information: Part number CD-IDSYNC-SERVICE-1Y is required for One Identity Synchronization Tool import.

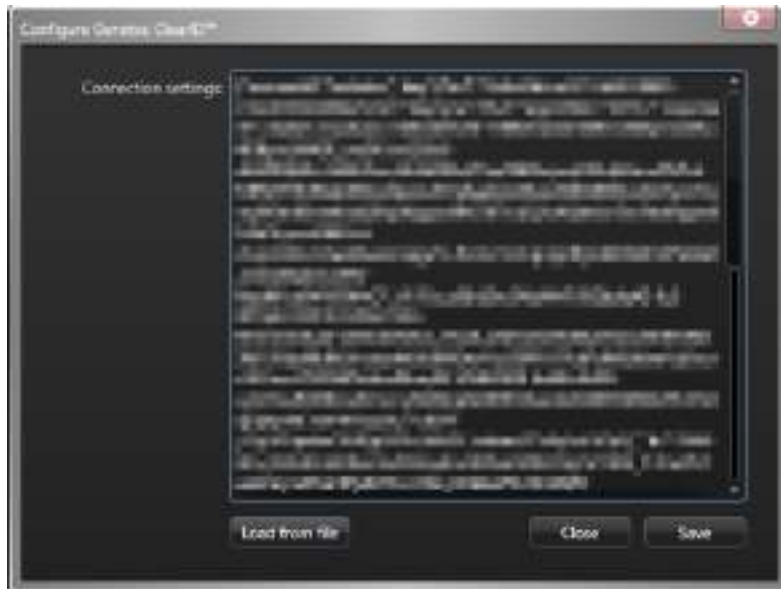
What you should know

Procedure

1. Open the One Identity Synchronization Tool (OneIdentityConfigurationTool.exe) and configure your settings.



2. Configure your connection settings.
 - a. In the One Identity Synchronization Tool, click Configure.
 - b. In the Configure Genetec ClearID™ dialog, click Load from file.
 - c. Navigate to and select your authentication key.



3. Click Save.

NOTE: The One Identity service is automatically restarted when the connection settings for the authentication key are changed.

Results

Your One Identity Synchronization Tool is now connected to ClearID.



After you finish

Configure your data sources. Choose one of the following:

- Configuring the data source for Azure AD synchronization in the ClearID One Identity Synchronization Tool
- Configuring the data source for Database synchronization in the ClearID One Identity Synchronization Tool
- Configuring the data source for File synchronization in the ClearID One Identity Synchronization Tool

Parent topic: Configuring the ClearID One Identity Synchronization Tool

12.5.5.2 | Configuring the data source for Azure AD synchronization in the ClearID One Identity Synchronization Tool

Synchronizing identities using One Identity Synchronization Tool in ClearID >

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool data sources for Azure Active Directory synchronization.

Before you begin

- Familiarize yourself with the One Identity attribute fields.
- Familiarize yourself with the Azure web app.
 - Make a note of the Azure web app connection settings for later use.
 - Make sure that the Azure AD API permissions are set up.
- Prepare an Azure Active Directory containing the identities attributes that you want to import and synchronize.
- Check your license information: Part number CD-IDSYNC-SERVICE-1Y is required for One Identity Synchronization Tool import.

What you should know

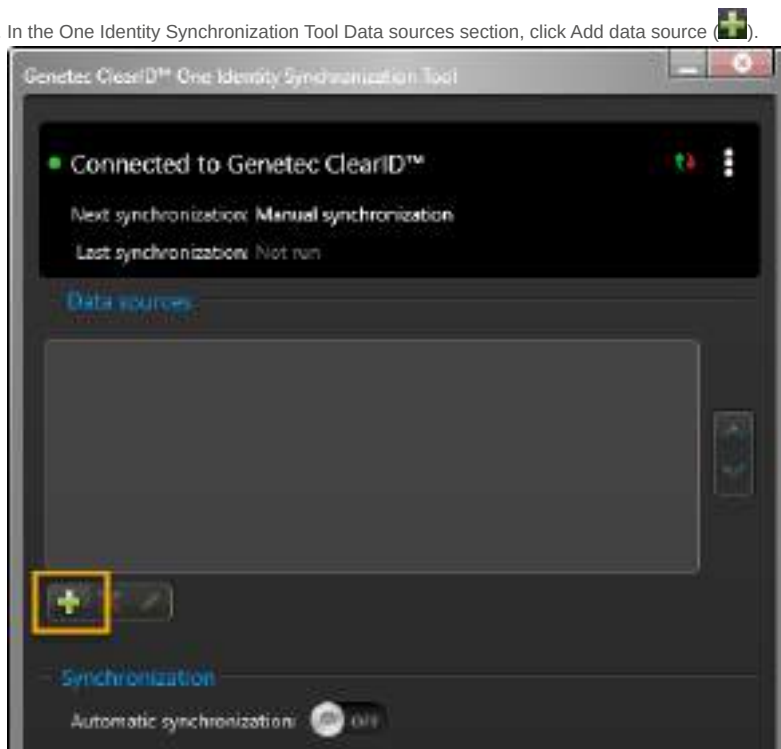
This procedure is for IT or security personnel responsible for external system attributes administration.

This procedure describes how to configure the data source for Azure AD.

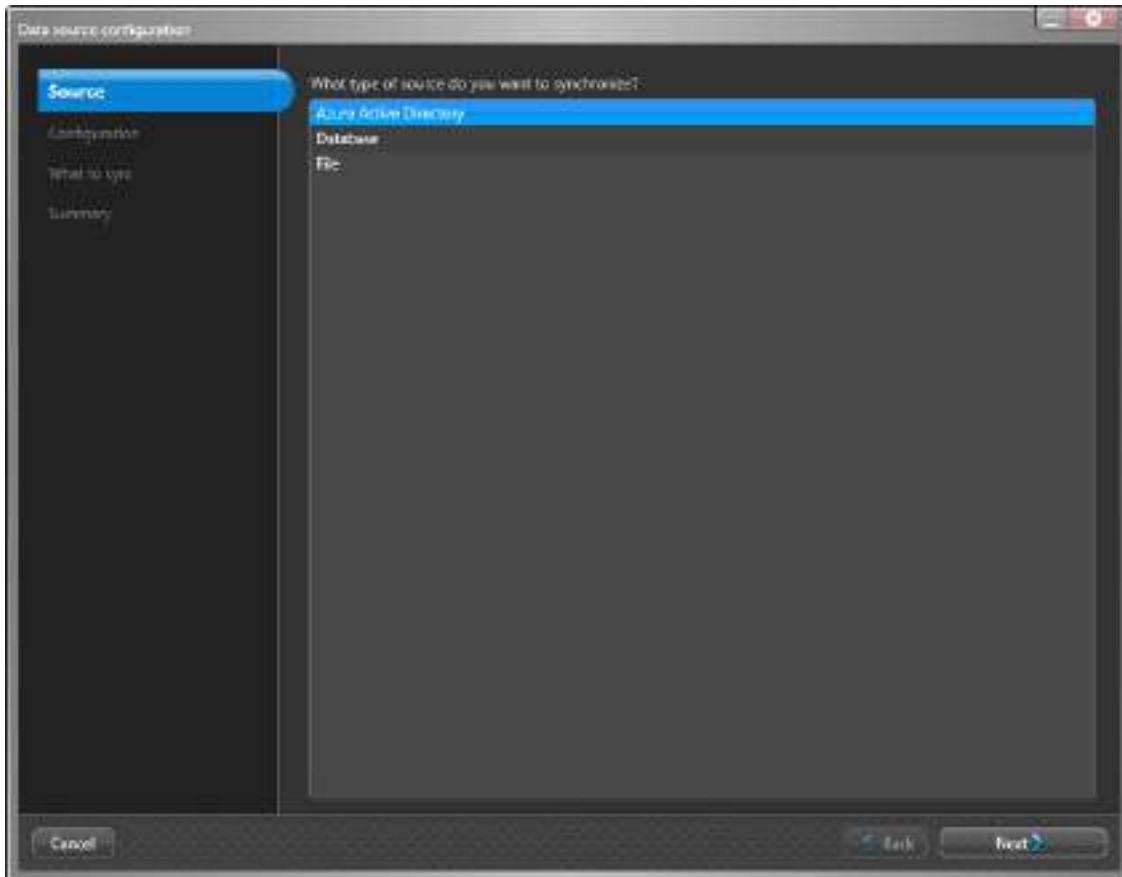
- The data source order is important because the first data source always overrides common fields.
- There is no limit to the number of data sources. However, the larger the data source, the memory requirements increase.
- When using an Azure data source to synchronize identities, the only possible field for Unique ID is the UserId field. When the Azure data source is selected, the Unique ID fields cannot be configured and use of the Azure UserId field is triggered by default.

Procedure

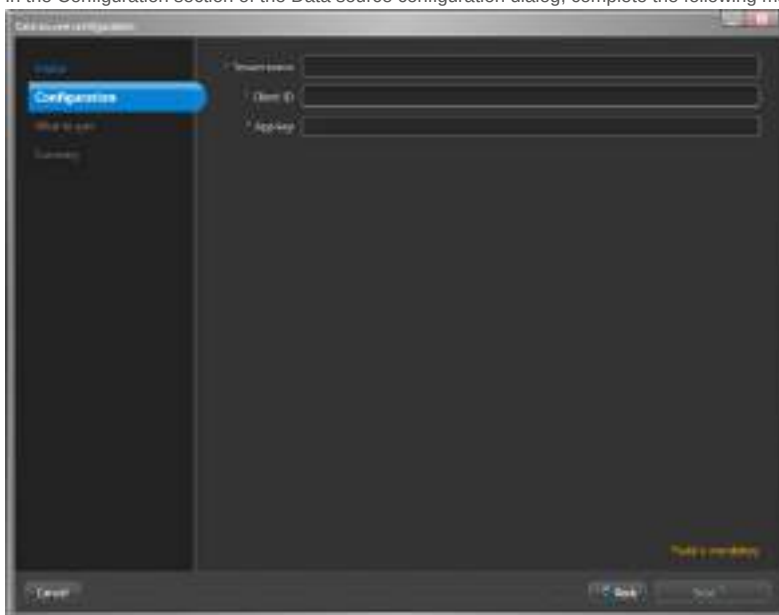
1. In the One Identity Synchronization Tool Data sources section, click Add data source (+).



2. In the Source section of the Data source configuration dialog, select Azure Active Directory and click Next.



3. In the Configuration section of the Data source configuration dialog, complete the following mandatory fields:



Tenant name

In the Tenant name field, enter your tenant name (account name). The tenant name is used to connect to the directory for the account. For example, a host address account.onmicrosoft.com or a GUID nxxxxnxxx-nnnn-nxnn-nnnx-nxxxxnxxxxnnn.

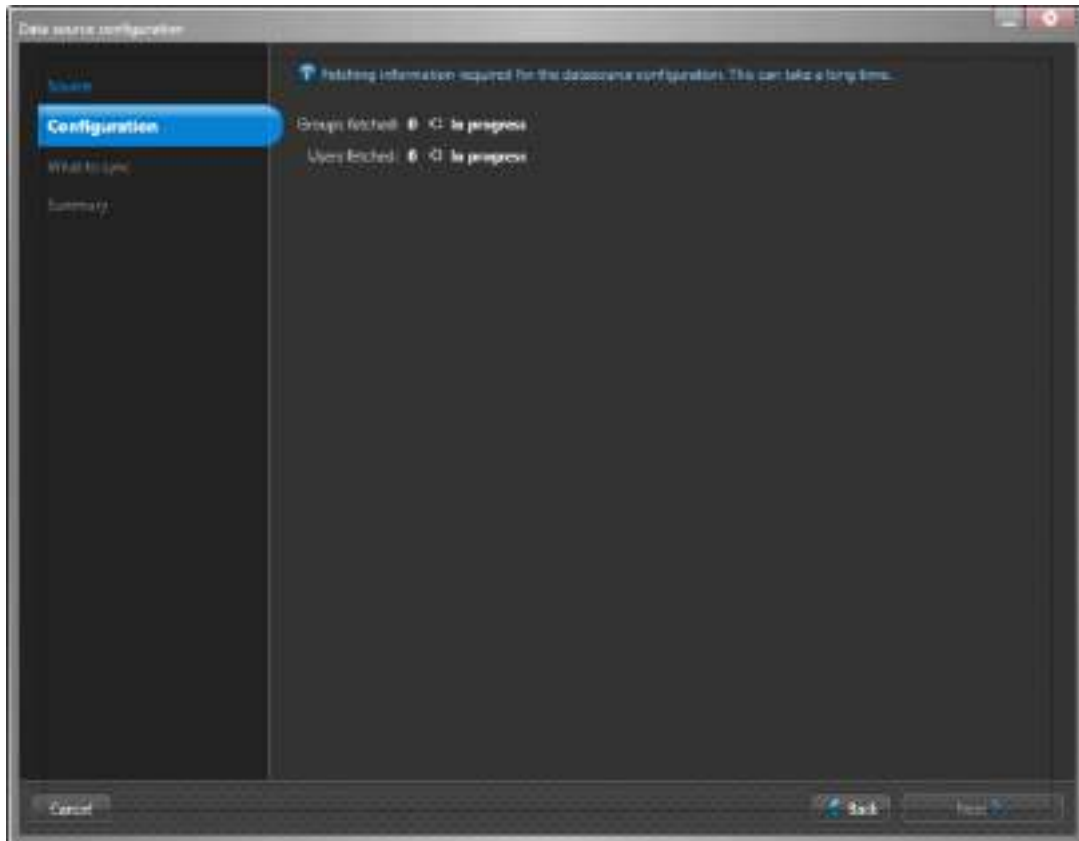
Client ID

In the Client ID field, enter your client ID. The client ID is used to connect to the client application. The Client ID format is an alpha-numeric format as follows: nxxxxnxxx-nxnn-nnnx-nxnn-nxxxxnxxxxnnn.

App key

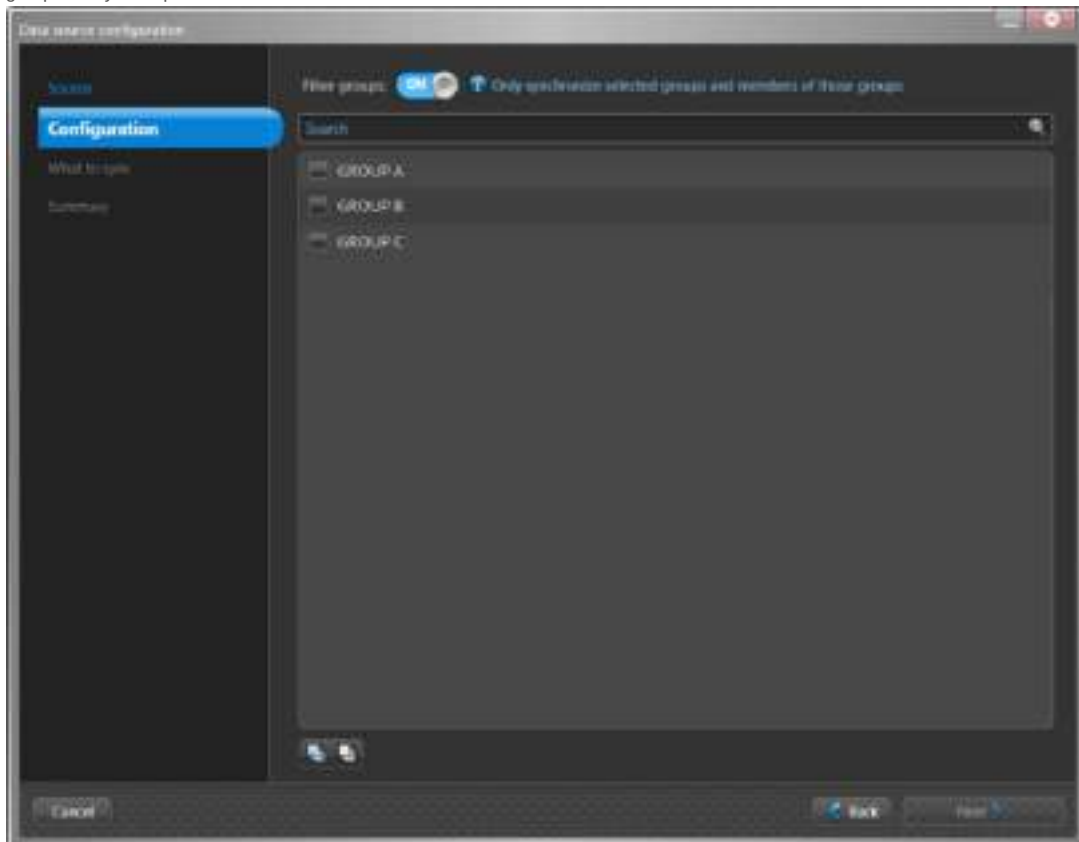
In the App key field, enter your App key. The App key is used to authenticate communications with ClearID. The App key format is an alpha-numeric format as follows: nXnxxxxXxxXnxxxxXXxXnxxxxXXnxxxxXnXXXXXxxx= .

Tip: The Tenant name, Client ID, and App key can be obtained from your Azure Active Directory application registration.
a. Click Next.



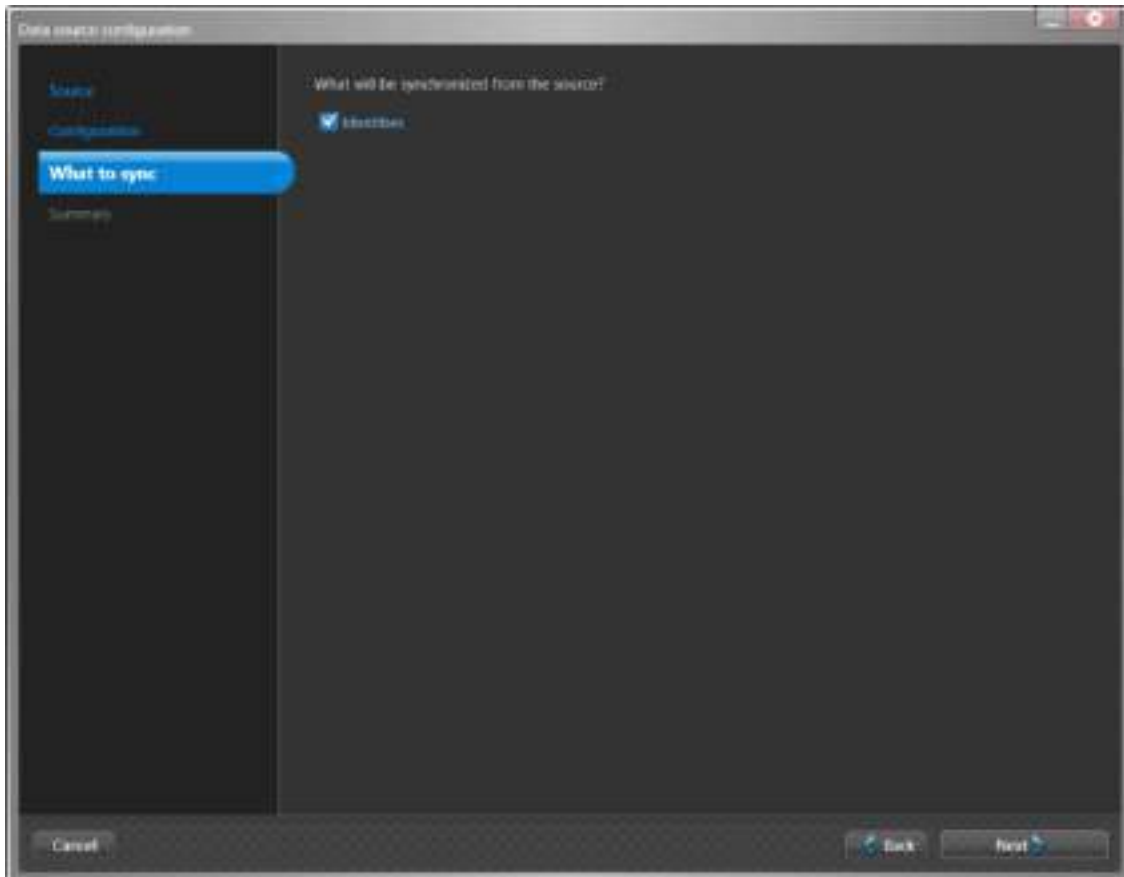
NOTE: Fetching information required for the data source configuration can take a long time and varies depending on the number of groups and users fetched.

- b. (Optional) Use the Filter groups option to only synchronize a subset of selected Azure AD groups and group members. Search for or select the groups that you require and click Next.



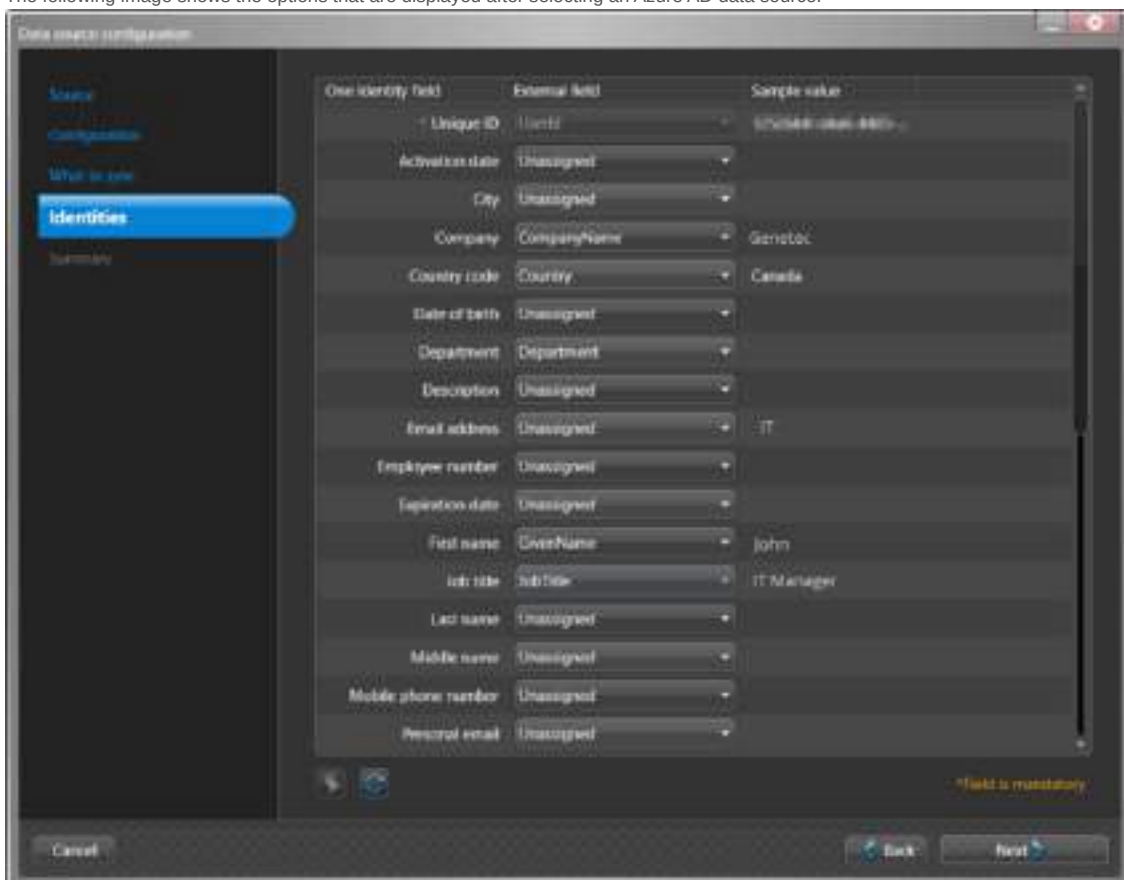
NOTE: If your Azure AD list is long, you can also use the Check all or Uncheck all icon to help you during your selection process.

4. In the What to sync section of the Data source configuration dialog, select Identities to synchronize from the external system data source.



5. If you selected Identities as a data source, in the What to sync section, configure the identity attributes settings.

NOTE: The fields that are displayed in the Identities section vary depending on the data source you selected in the Source section. The following image shows the options that are displayed after selecting an Azure AD data source.



a. Configure your External field attribute mappings.

One Identity field

Displays the ClearID identity attributes. Mandatory fields are highlighted using an asterisk (*).

External Field

Select system attributes in the External field columns that you want to map from the external system to the ClearID identity attributes shown in the One Identity field column.

CAUTION:

When using Azure AD as your data source, the One Identity Unique ID field must be mapped to the Azure AD User ID external field to ensure that the identity attributes are correctly mapped and synchronized.

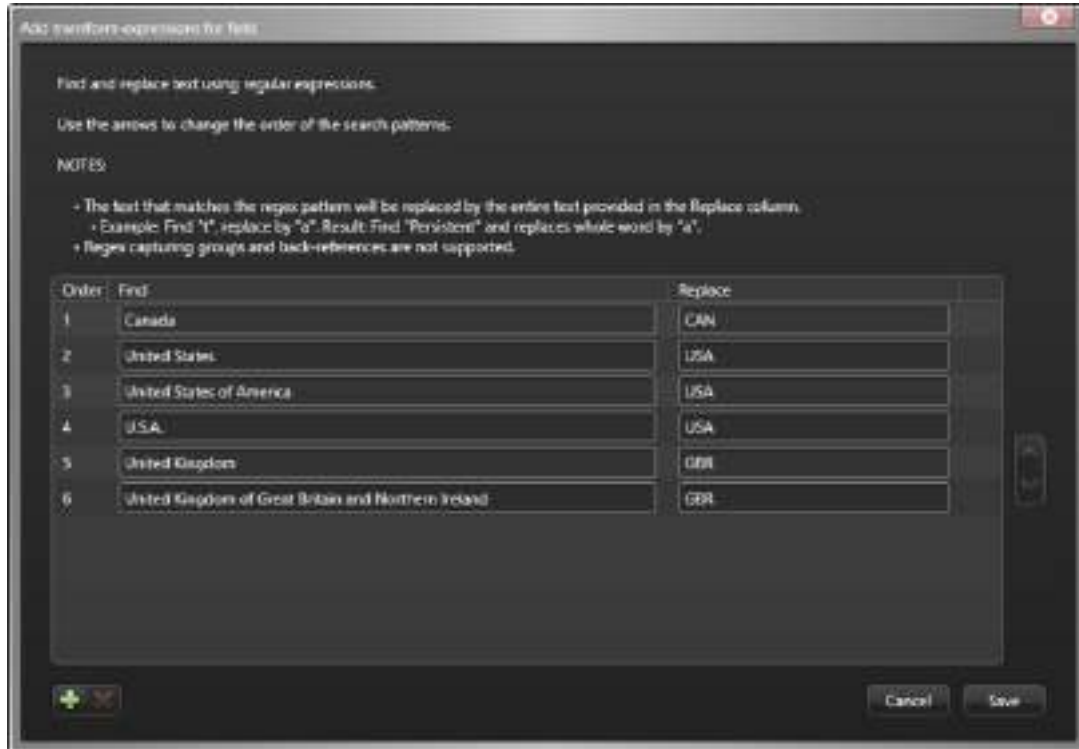
Sample value

If an External field is selected, an example of the selected external field data from your data source is displayed (if available) in the Sample value column next to the External field column.

Tip: Use the sample value column to check the format of the attributes data you are about to import from your external system fields into ClearID.

- b. (Optional) Click Script () to add a transform expression to find and replace external field text using regular expressions.

For example, you can look for variations of a country name to replace with the correct country code.

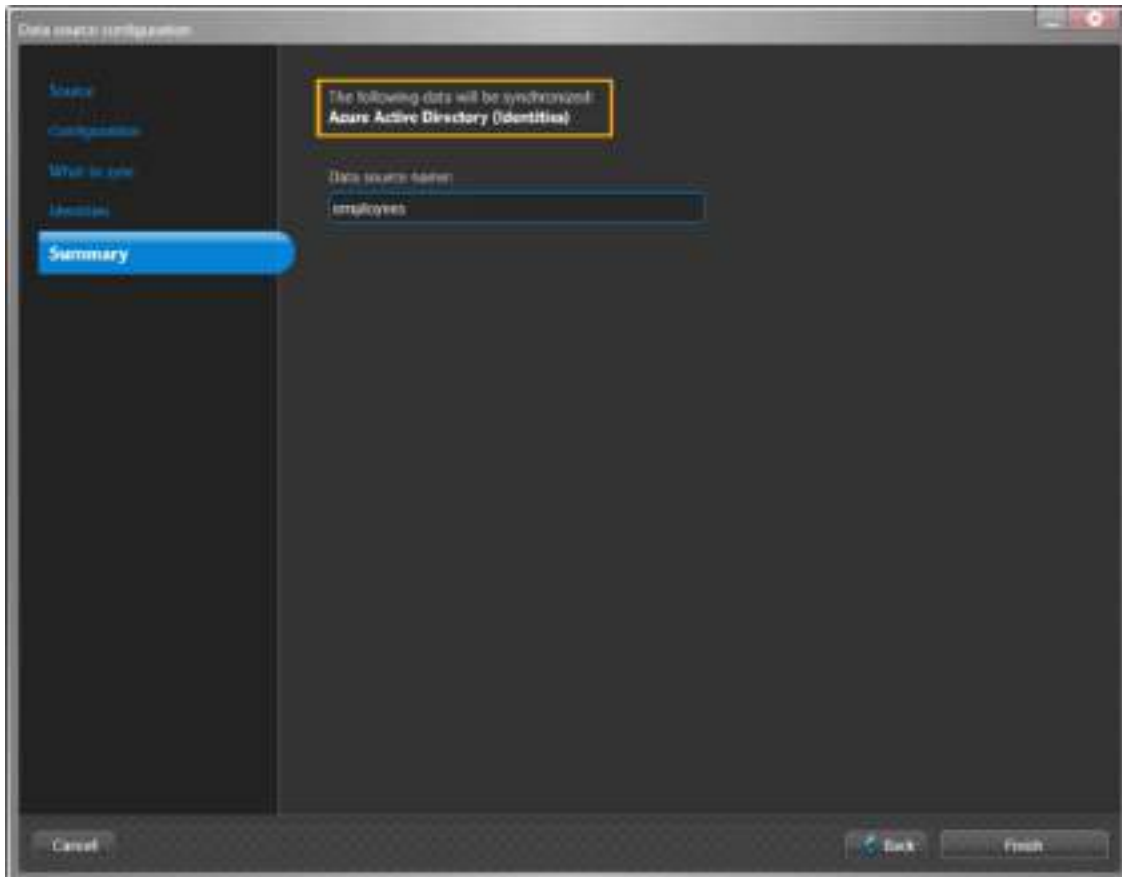


- A script icon () is shown in the Sample value column when the field text is being replaced with a regular expression.
- The transform expressions are processed in the order specified in the Add transform expressions for field dialog.

Tip: If required, you can select the row of any expressions that you no longer require, and click delete (.

- c. (Optional) Click Refresh () to update the external fields data from your data source. This refresh option is used in situations where the existing data has been modified, new data rows have been added, or new attribute columns have been added.
- d. Click Next.

6. In the Summary section, review the data that will be synchronized.



NOTE: If multiple data sources are selected, only the first data source file is displayed in the Summary section Data source name field. If you want each of the data files listed in the Data sources section, you must add them individually.

a. If the data synchronization details look correct, click Finish.

After you finish

Configure your synchronization settings.

Parent topic: [Configuring the ClearID One Identity Synchronization Tool](#)

Browse

- [About ClearID One Identity Synchronization Tool attribute fields](#)

12.5.5.3 | [Configuring the data source for Database synchronization in the ClearID One Identity Synchronization Tool](#)

[Synchronizing identities using One Identity Synchronization Tool in ClearID](#) >

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool data sources for database synchronization.

Before you begin

- [Familiarize yourself with the One Identity attribute fields.](#)
- Prepare a Database containing identities attributes that you want to import and synchronize.
- Check your license information: Part number CD-IDSYNC-SERVICE-1Y is required for One Identity Synchronization Tool import.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

This procedure describes how to configure the data source for a Database (Microsoft SQL Server, Oracle Database, ODBC).

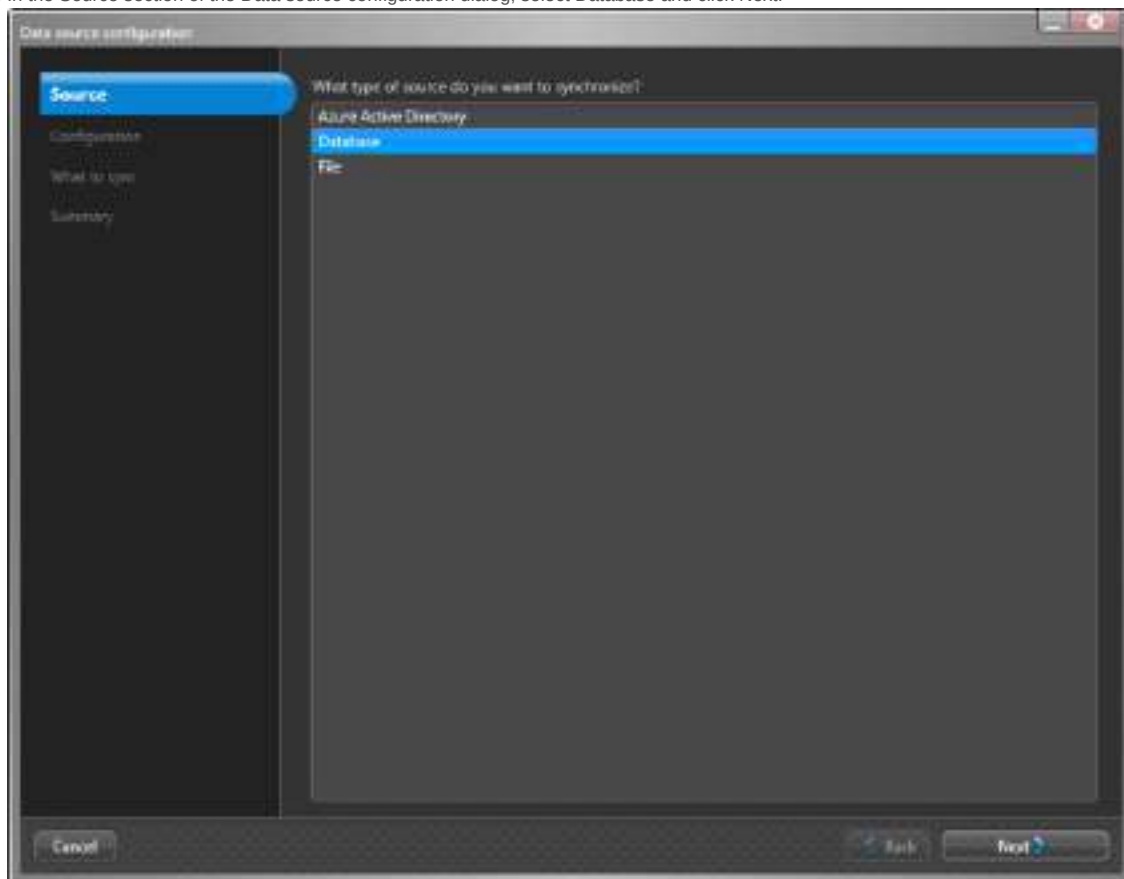
- The data source order is important because the first data source always overrides common fields.
- There is no limit to the number of data sources. However, the larger the data source, the memory requirements increase.

Procedure

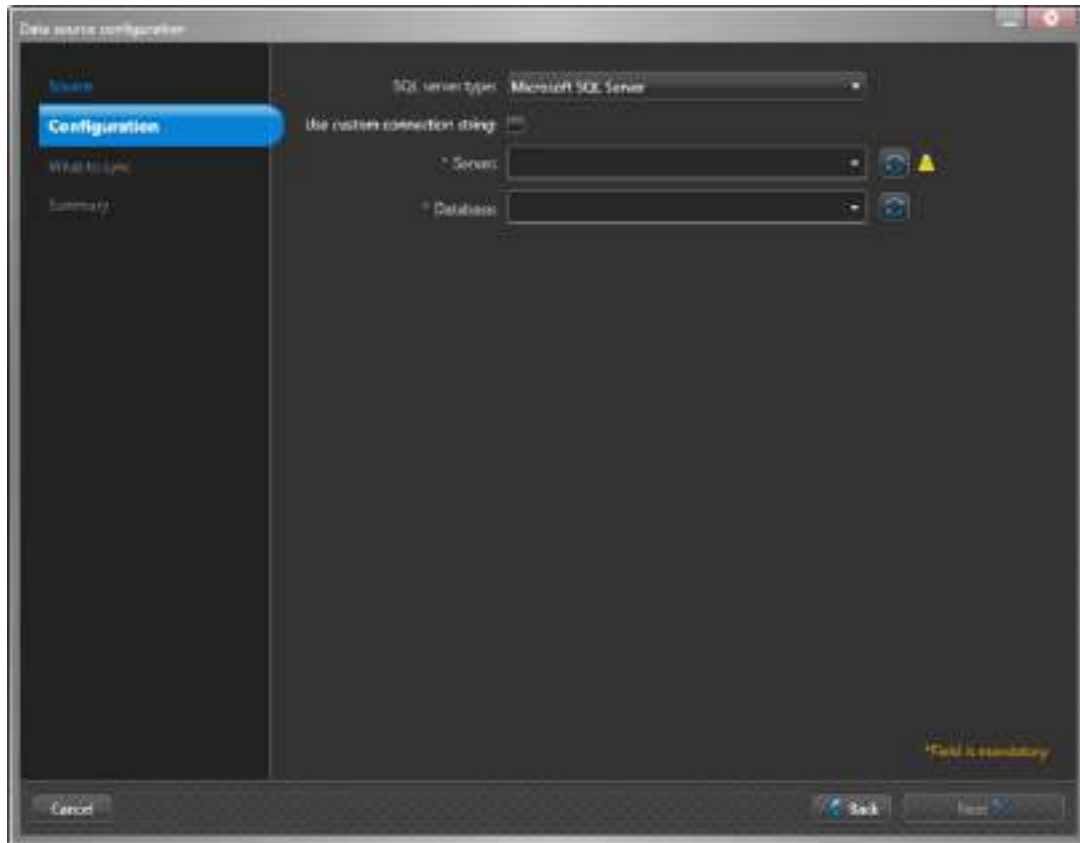
1. In the One Identity Synchronization Tool Data sources section, click Add data source ()



2. In the Source section of the Data source configuration dialog, select Database and click Next.



3. In the Configuration section of the Data source configuration dialog, configure the database settings.
- Select an SQL server type:
 - Microsoft SQL Server
 - Oracle Database (only views are currently supported)
 - ODBC
 - If you selected Microsoft SQL Server, configure the following:



Use custom connection string

Select the checkbox if you want to use a custom connection string.

NOTE: If you use the Use custom connection string option, the Server and Database fields are removed.

Connection string

Enter the connection string.

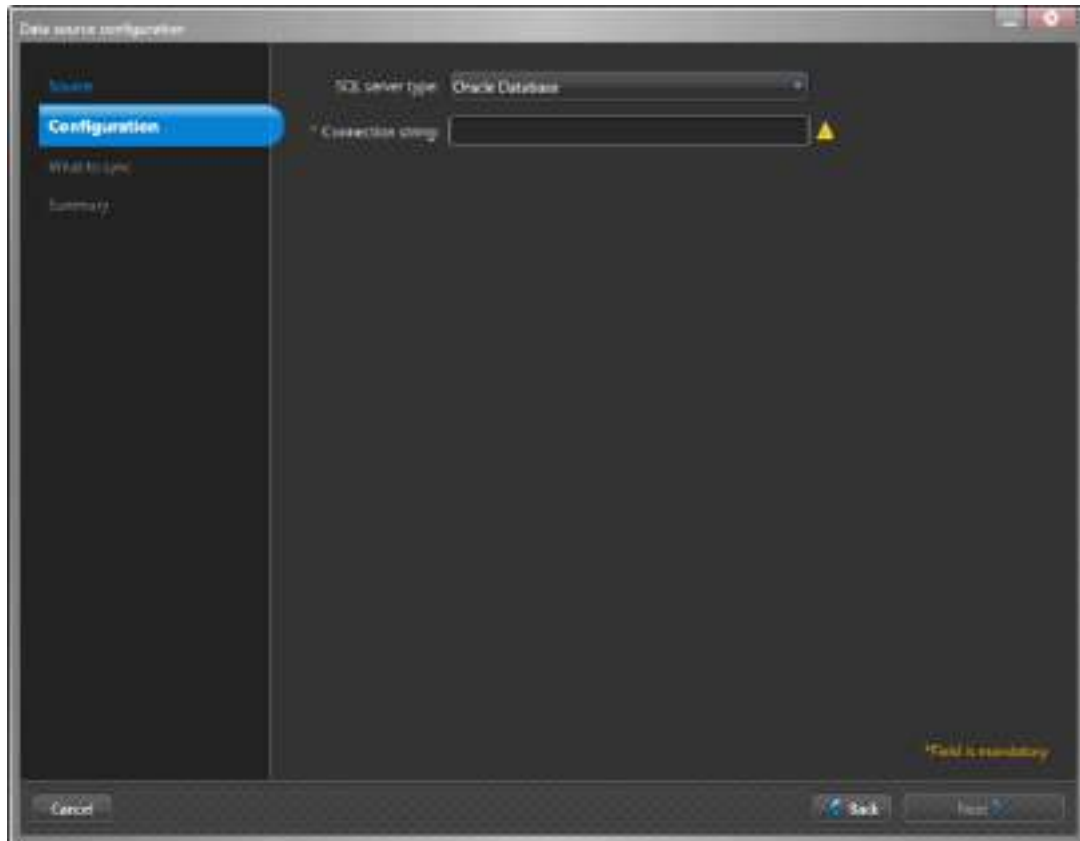
Server

Enter SQL server information or select a server from the list.

Database

Enter Database information or select a database from the list.

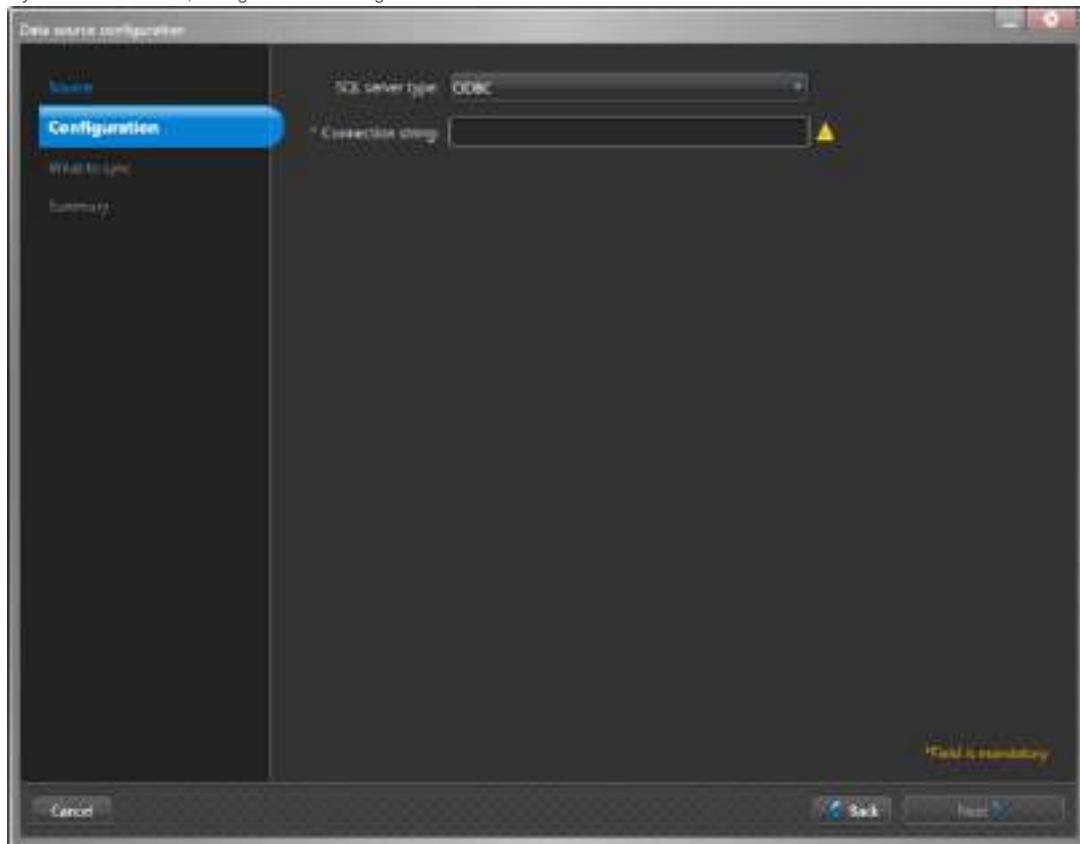
c. If you selected Oracle Database, configure the following:



Connection string

Enter the connection string.

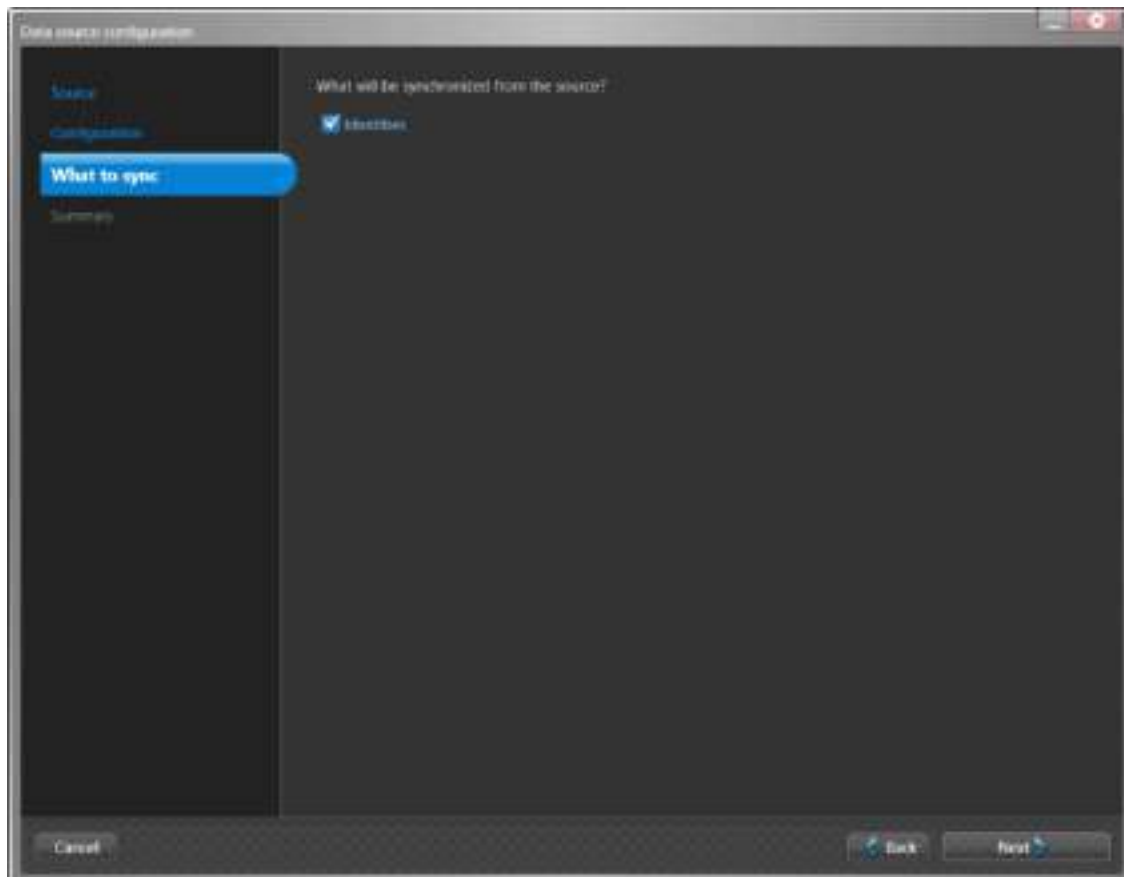
- d. If you selected ODBC, configure the following:



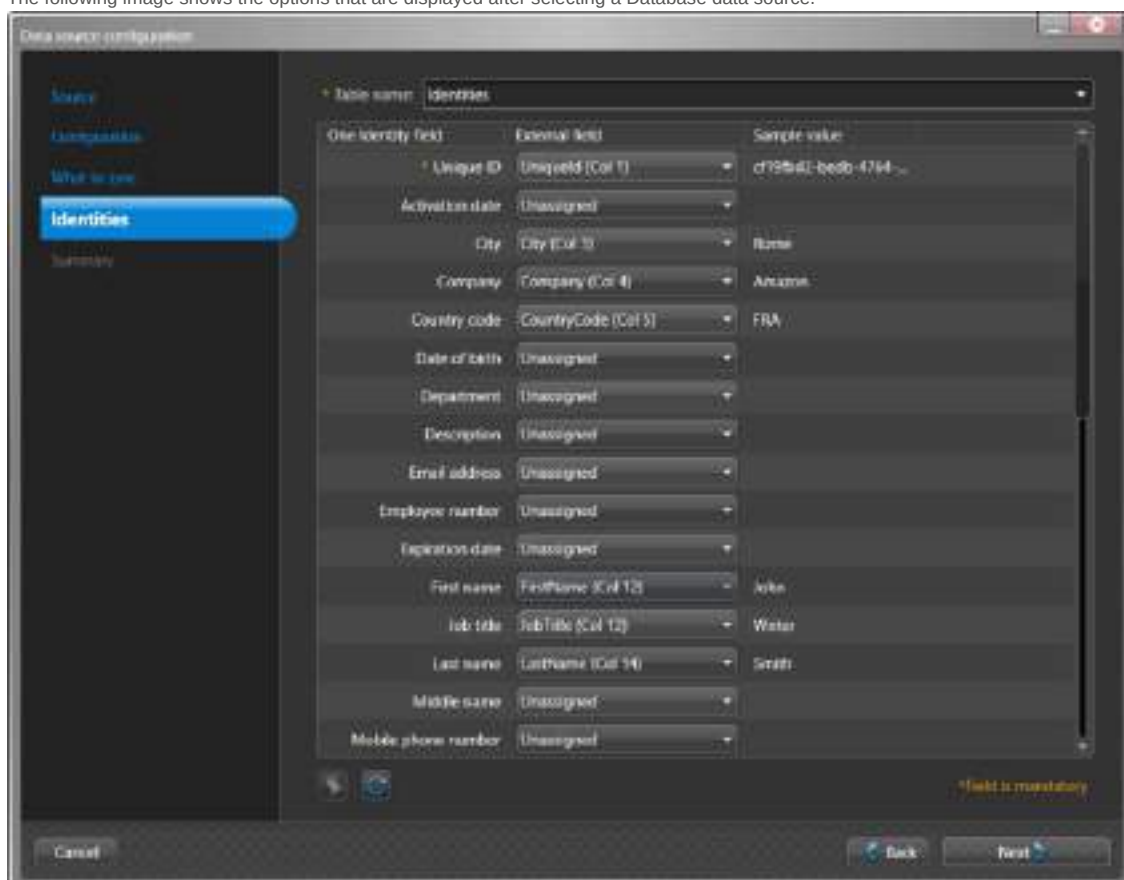
Connection string

Enter the connection string.

4. In the What to sync section of the Data source configuration dialog, select Identities to synchronize from the external system data source.



5. If you selected Identities as a data source, in the What to sync section, configure the identity attributes settings.
NOTE: The fields that are displayed vary depending on the data source you selected in the Source section.
The following image shows the options that are displayed after selecting a Database data source.



- a. Configure your External field attribute mappings.
One Identity field
Displays the ClearID identity attributes. Mandatory fields are highlighted using an asterisk (*).

Genetec ClearID®; User Guide

Displayed in the header

IMPORTANT: The Unique ID is used internally by One Identity as the primary key to identify what it is. For example, an employee number or email address could be used, as long as it is unique.

External Field

Select system attributes in the External field columns that you want to map from the external system to the ClearID identity attributes shown in the One Identity field column.

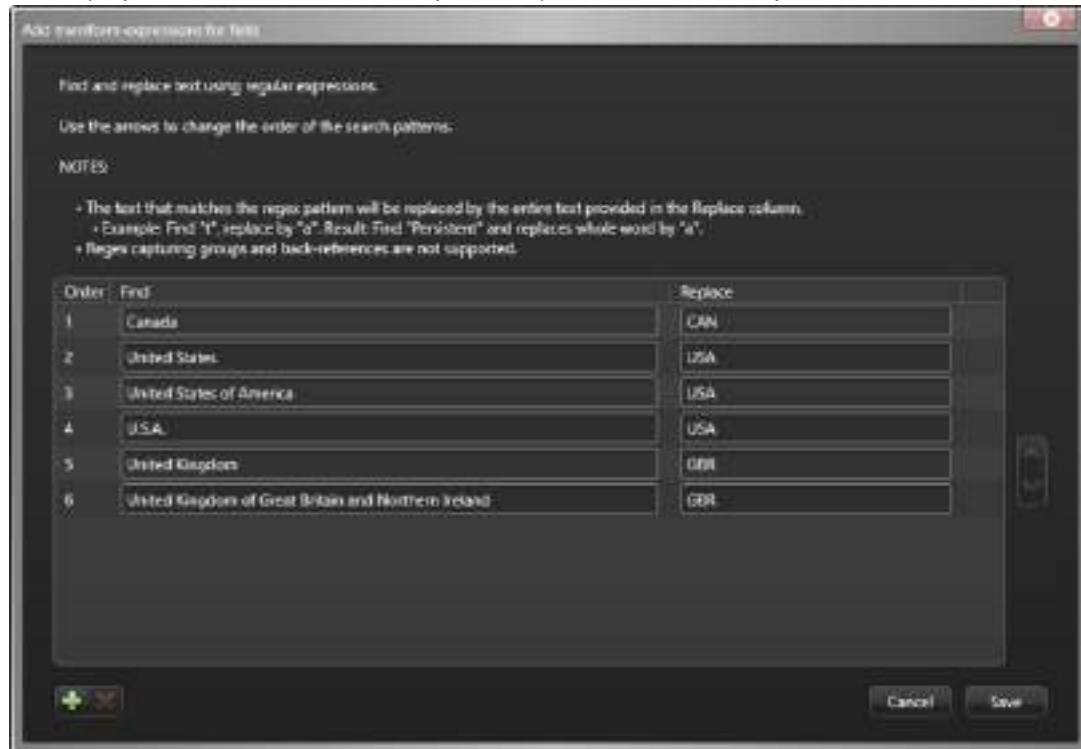
Sample value

If an External field is selected, an example of the selected external field data from your data source is displayed (if available) in the Sample value column next to the External field column.

Tip: Use the sample value column to check the format of the attributes data you are about to import from your external system fields into ClearID.

- b. (Optional) Click Script  to add a transform expression to find and replace external field text using regular expressions.

For example, you can look for variations of a country name to replace with the correct country code.



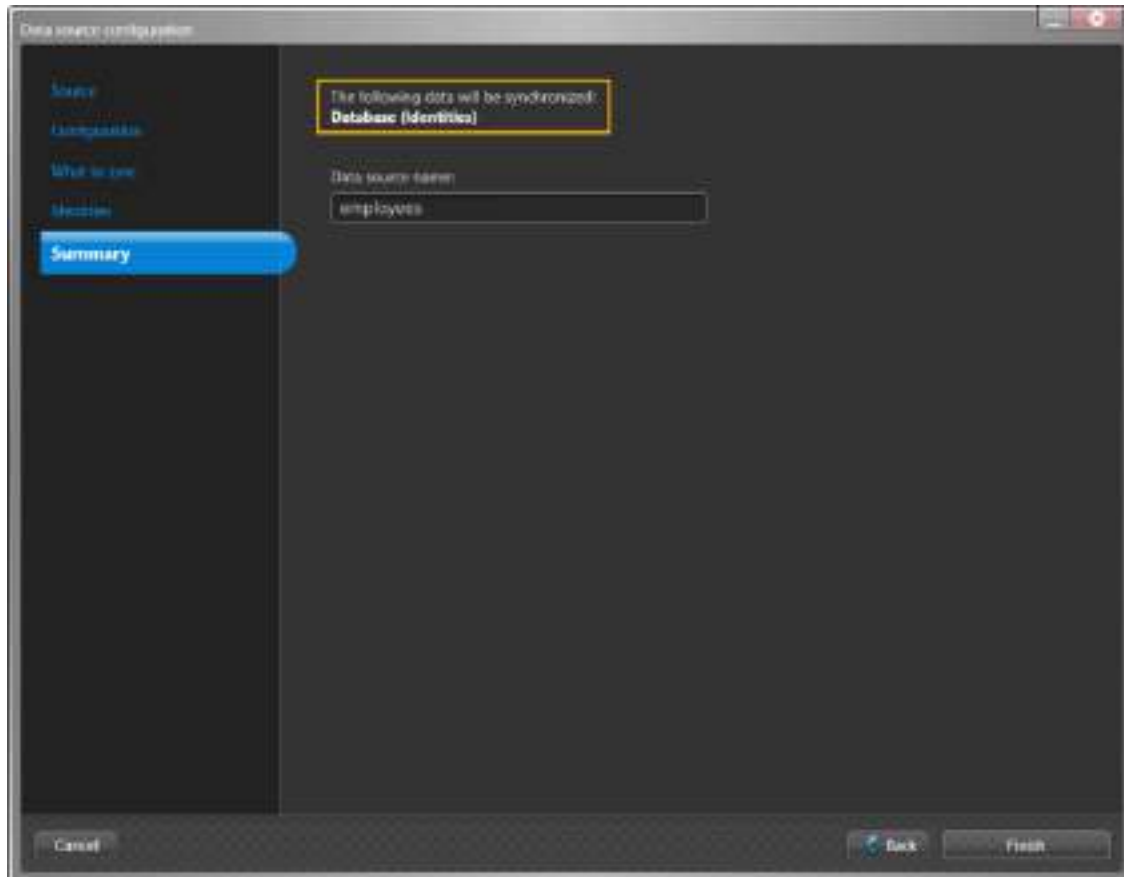
- A script icon  is shown in the Sample value column when the field text is being replaced with a regular expression.
- The transform expressions are processed in the order specified in the Add transform expressions for field dialog.

Tip: If required, you can select the row of any expressions that you no longer require, and click delete .

- c. (Optional) Click Refresh  to update the external fields data from your data source. This refresh option is used in situations where the existing data has been modified, new data rows have been added, or new attribute columns have been added.

- d. Click Next.

6. In the Summary section, review the data that will be synchronized.



NOTE: If multiple data sources are selected, only the first data source file is displayed in the Summary section Data source name field. If you want each of the data files listed in the Data sources section, you must add them individually.

- a. If the data synchronization details look correct, click Finish.

After you finish

Configure your synchronization settings.

Parent topic: [Configuring the ClearID One Identity Synchronization Tool](#)

Browse

- [About ClearID One Identity Synchronization Tool attribute fields](#)

12.5.5.4 | [Configuring the data source for File synchronization in the ClearID One Identity Synchronization Tool](#)

[Synchronizing identities using One Identity Synchronization Tool in ClearID](#) >

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool data sources for file (CSV) Synchronization.

Before you begin

- [Familiarize yourself with the One Identity attribute fields.](#)
- Prepare a CSV file containing the identities attributes that you want to import and synchronize.
- Check your license information: Part number CD-IDSYNC-SERVICE-1Y is required for One Identity Synchronization Tool import.

IMPORTANT: Make sure that your CSV files are not being edited and are closed, because the synchronization tool locks the files during the synchronization process.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

This procedure describes how to configure the data source for a File (CSV import).

- The data source order is important because the first data source always overrides common fields.
- One data source can include multiple CSV files containing identities.
- There is no limit to the number of data sources. However, the larger the data source (not only CSV files), the memory requirements increase.

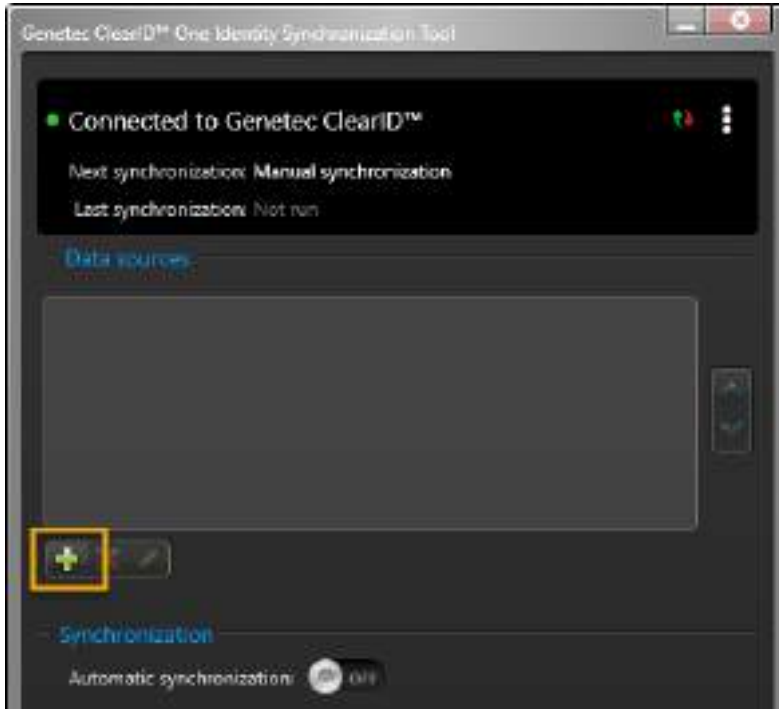
Genetec ClearID™ User Guide

Displayed in the header

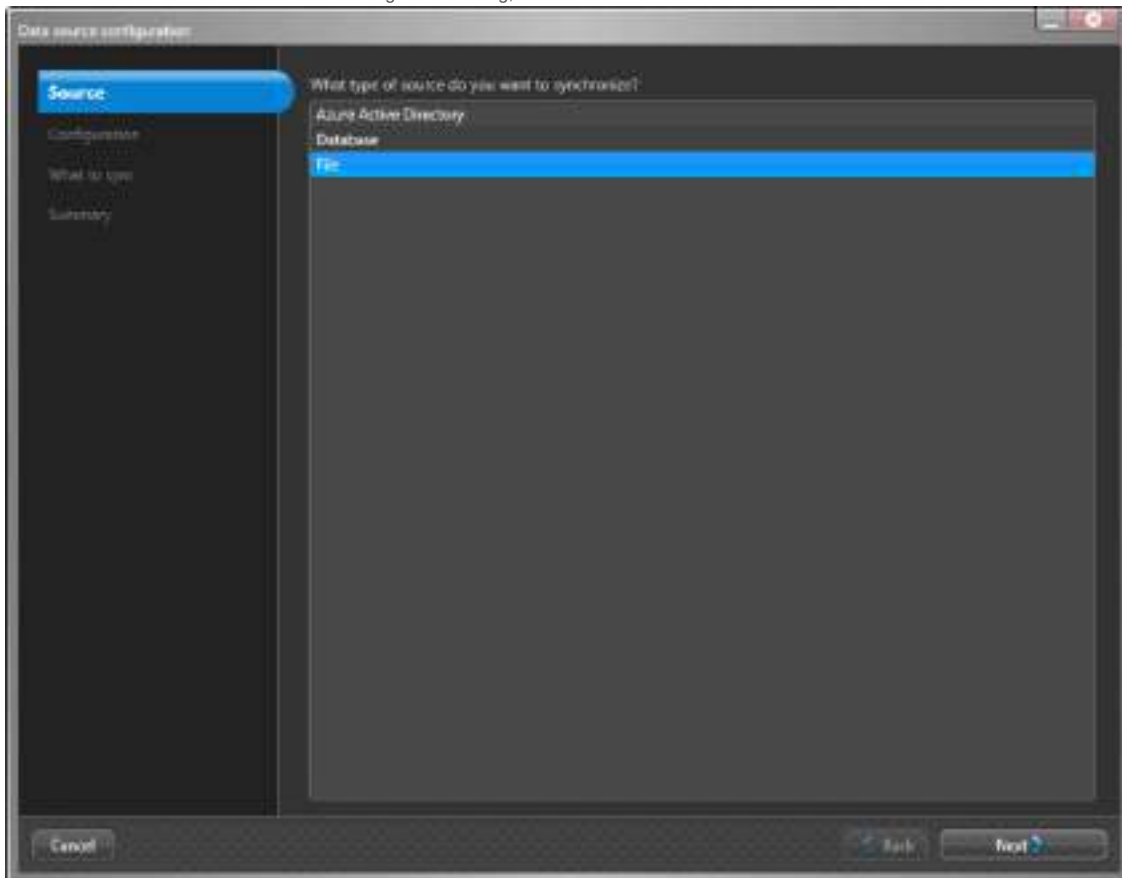
Best Practice: To avoid user permission issues when using CSV files with the ClearID One Identity Synchronization Tool, save them to a C: or C:\temp folder location. Do not save CSV files in a user-controlled file or folder locations (C:\Users folders or desktop folder location) or you might encounter File path is not valid user permissions issues.

Procedure

1. In the One Identity Synchronization Tool Data sources section, click Add data source .

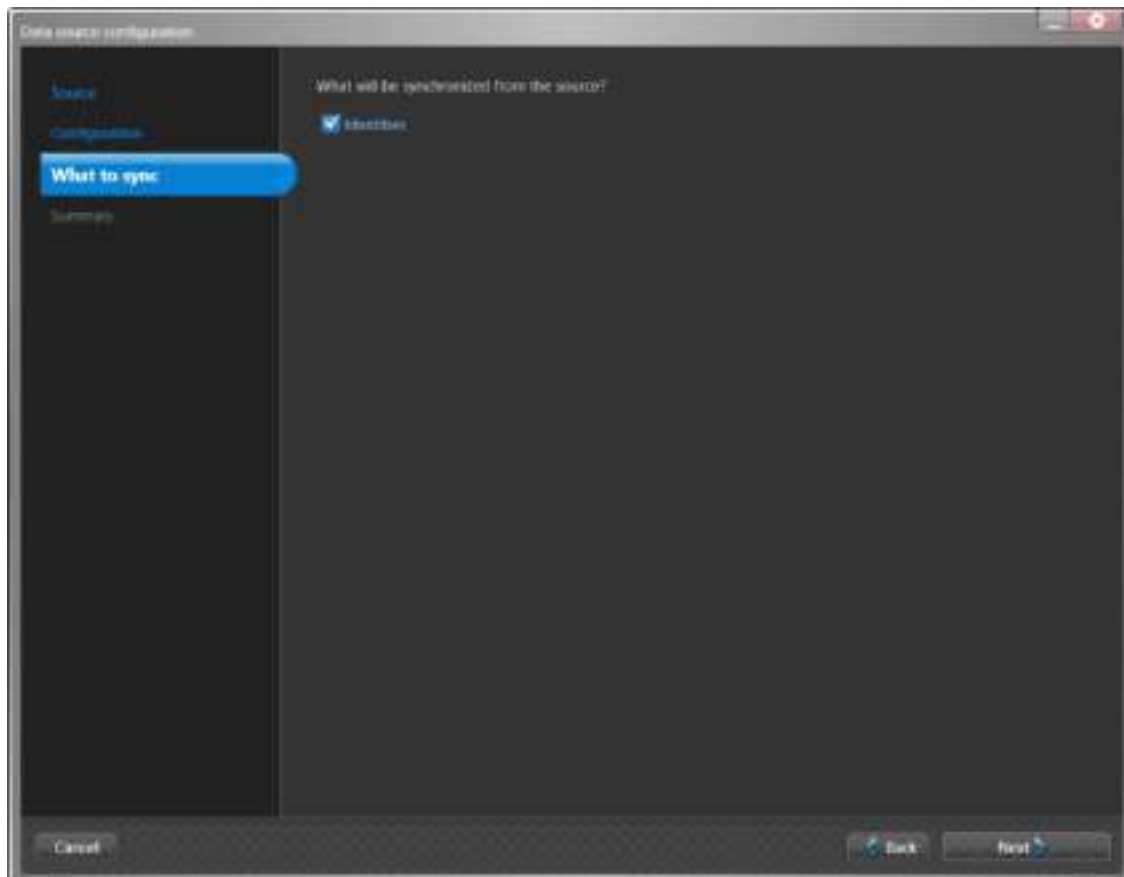


2. In the Source section of the Data source configuration dialog, select File and click Next.

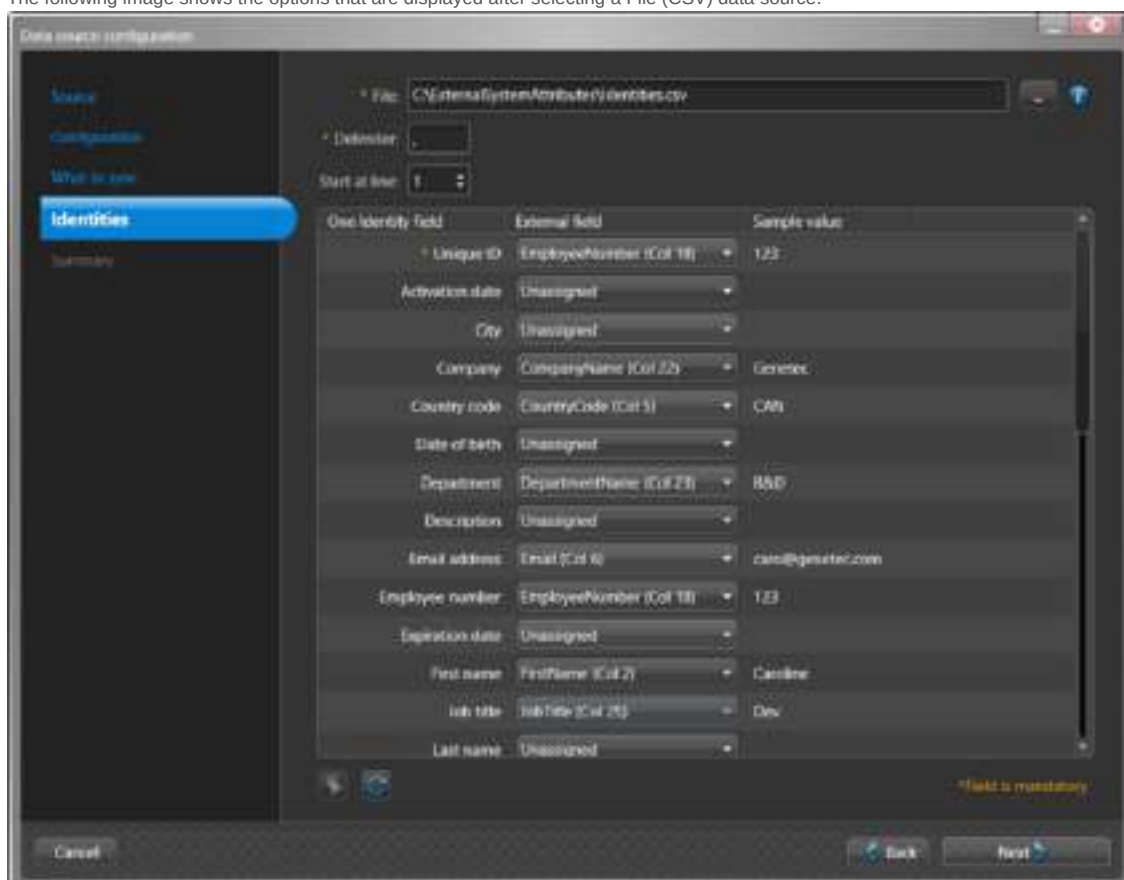


NOTE: If you selected File in the Source section, the Configuration section of the Data source configuration dialog is skipped because it is not required.

3. In the What to sync section of the Data source configuration dialog, select Identities to synchronize from the external system data source.



4. If you selected Identities as a data source, in the What to sync section, configure the identity attributes settings.
NOTE: The fields that are displayed vary depending on the data source selected in the Source section (step 2) earlier.
The following image shows the options that are displayed after selecting a File (CSV) data source.



- a. If you selected File as your data source, configure the file settings.

File

Click More (⋮) to select the CSV file containing your attributes.

NOTE: The file path must exist on the server where the One Identity Configuration Tool is installed.

Delimiter

Enter a Delimiter value.

For example, for a CSV file it is a comma-separated value (CSV).

Start at line

Select a Start at line.

For example, the data in a table with no headings might start at line 0, whereas the data in a table with headings might start at line 1.

b. Configure your External field attribute mappings.

One Identity field

Displays the ClearID identity attributes. Mandatory fields are highlighted using an asterisk (*).

IMPORTANT: The Unique ID is used internally by One Identity as the primary key to identify what it is. For example, an employee number or email address could be used, as long as it is unique.

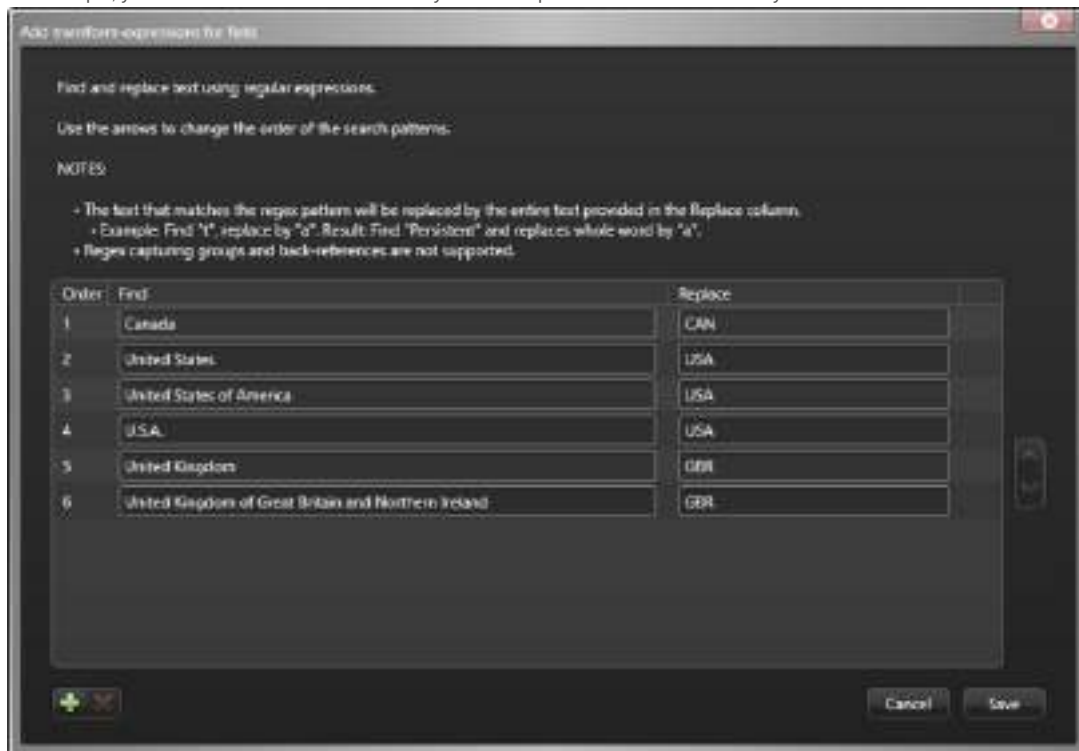
External Field

Select system attributes in the External field columns that you want to map from the external system to the ClearID identity attributes shown in the One Identity field column.

- If your CSV file contains column titles, the names are displayed.
- If your CSV file does not contain column titles, the column number is displayed.

c. (Optional) Click Script  to add a transform expression to find and replace external field text using regular expressions.

For example, you can look for variations of a country name to replace with the correct country code.



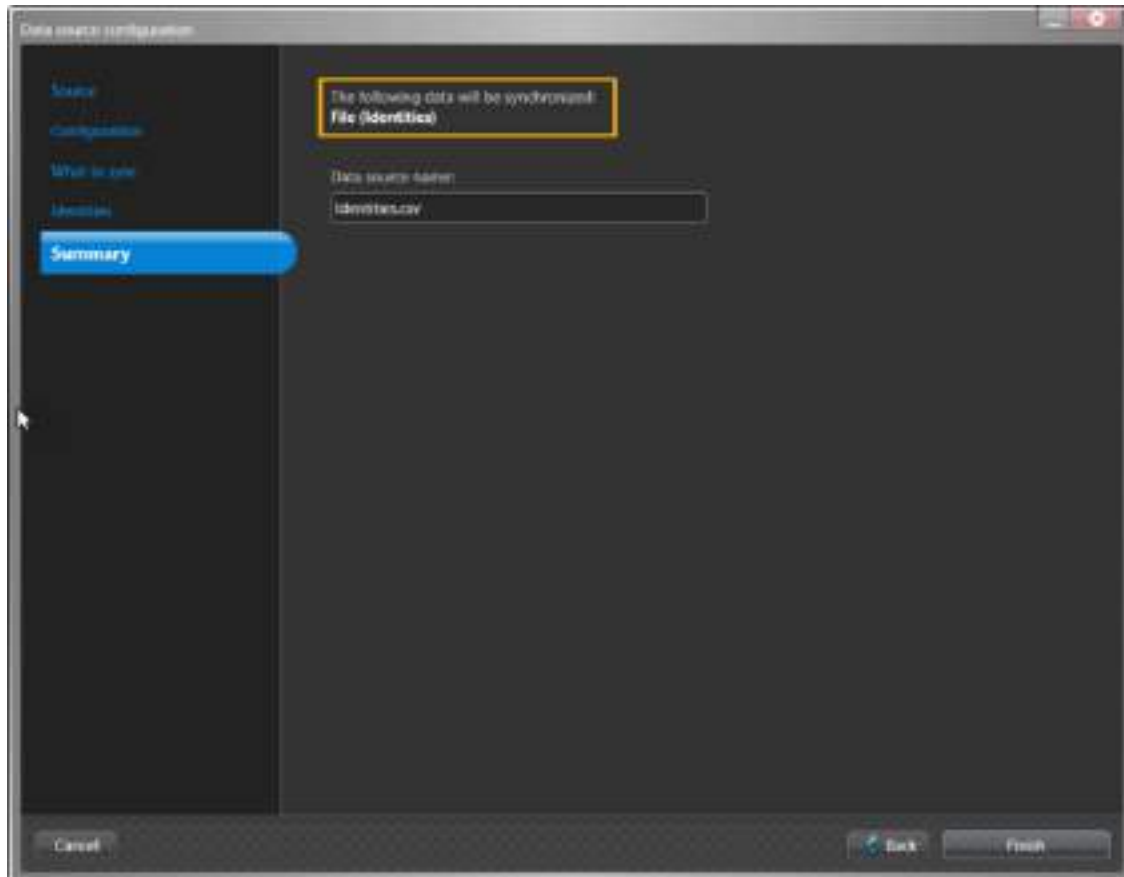
- A script icon  is shown in the Sample value column when the field text is being replaced with a regular expression.
- The transform expressions are processed in the order specified in the Add transform expressions for field dialog.

Tip: If required, you can select the row of any expressions that you no longer require, and click delete .

d. (Optional) Click Refresh  to update the external fields data from your data source. This refresh option is used in situations where the existing data has been modified, new data rows have been added, or new attribute columns have been added.

e. Click Next.

5. In the Summary section, review the data that will be synchronized.



NOTE: If multiple data sources are selected, only the first data source file is displayed in the Summary section Data source name field. If you want each of the data files listed in the Data sources section, you must add them individually.

- If the data synchronization details look correct, click Finish.

After you finish

Configure your synchronization settings.

Parent topic: [Configuring the ClearID One Identity Synchronization Tool](#)

Browse

- [About ClearID One Identity Synchronization Tool attribute fields](#)

12.5.5.5 | Configuring synchronization settings in the ClearID One Identity Synchronization Tool

[Synchronizing identities using One Identity Synchronization Tool in ClearID >](#)

Before you can synchronize an external system with Genetec ClearID™, you must first configure the Genetec ClearID™ One Identity Synchronization Tool synchronization settings.

Before you begin

- Check your license information: Part number CD-IDSYNC-SERVICE-1Y is required for One Identity Synchronization Tool import.

IMPORTANT: Make sure that your files are not being edited and are closed, because the synchronization tool locks the file during the synchronization process.

What you should know

This procedure is for IT or security personnel responsible for external system attributes administration.

Synchronization can be performed manually using the Synchronize now () option, or automatically at the Automatic synchronization intervals specified in the One Identity Synchronization Tool.

Synchronization of external system attributes into ClearID identity attributes is INBOUND only.

CAUTION:

Any changes only made to identities in ClearID can be overwritten during the next synchronization from the external system.

Procedure

1. In the One Identity Synchronization Tool Synchronization section, configure your synchronization settings.



Automatic synchronization

Enable automatic synchronization if you want attributes synchronized at a specified interval.

Interval

If automatic synchronization is enabled, choose a synchronization interval:

Fixed

Enter a Synchronization interval using the following format: 000d 01h 00m 00s.

For example, every 7 days would be 007d 00h 00m 00s, or every 12hrs 000d 12h 00m 00s.

Cron Schedule

Enter a synchronization interval using the Quartz Cron format. For example, 00***?*

For more information, see quartz-scheduler.org/documentation.

Tip: You can click Synchronize now () regardless of any scheduled settings to initiate an immediate synchronization.

Synchronize picture

Choose when to synchronize identity pictures from the external system.

Always

Identity pictures are synchronized every time a synchronization occurs.

Only if missing

Identity pictures are only synchronized when a synchronization occurs, if they are missing.

NOTE: Including pictures increases the amount of time that it takes to import attributes.

Stop Synchronization on error

Enable this option to stop synchronization if an error is encountered during the synchronization process.

Default web portal access

Specifies web portal access for synchronized users.

Grant access

ClearID web portal access for synchronized users is enabled by default.

NOTE: The username field must be mapped to give web portal access to a ClearID identity.

- There are only two possible values for the User type mapping: Admin and User. Any other value entered defaults to User.
- If the mapping for web portal access is not set, or the value is empty, the Default web portal access global setting is used.

No access

Web portal access for synchronized users is disabled by default.

Default country

Choose one of the following:

No default country

If a synchronized identity does not include a country attribute, the country attribute is ignored.

Default country

Select a default country. If a synchronized identity does not include a country attribute, the synchronized identity uses the default country specified here.

2. Click Save.

Results

The ClearID One Identity Synchronization Tool is now configured to synchronize attributes from the external system using the Data sources and Synchronization settings specified in the tool.

After you finish

After the synchronization has occurred, verify that the new attributes from the external system have been synchronized and contain the correct attributes.

Parent topic: [Configuring the ClearID One Identity Synchronization Tool](#)

12.5.6 | Reviewing synchronization status for the ClearID One Identity Synchronization Tool

To check that your identity attributes were synchronized into Genetec ClearID™ correctly, you can review the synchronization status in the Genetec ClearID™ One Identity Synchronization Tool or the ClearID web portal.

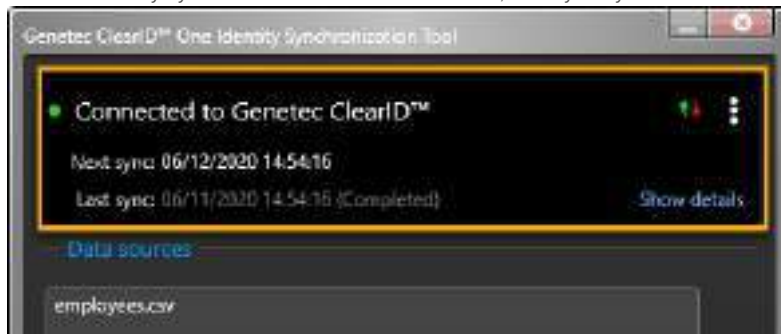
Before you begin

- [Configure the One Identity Synchronization Tool](#).
- Perform a manual or automatic synchronization using the One Identity Synchronization Tool.

Procedure

To review your attribute synchronization status in the One Identity Configuration Tool:

1. In the One Identity Synchronization Tool connection section, check your synchronization status.



Next sync

Displays information about the next synchronization.

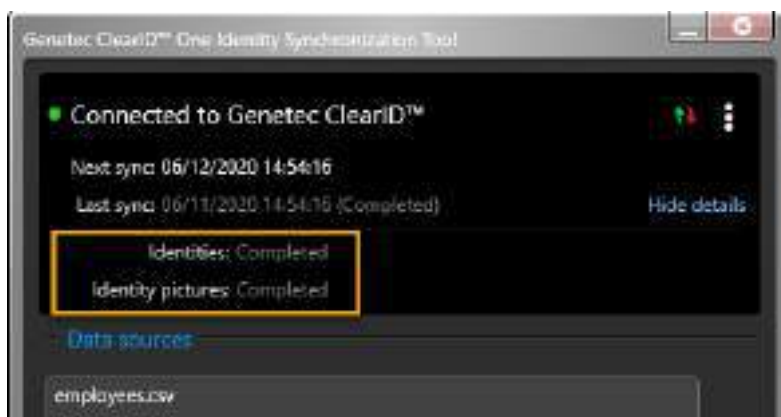
- If a date is displayed 06/16/2020 23:00:00, this date indicates the Fixed or Cron schedule interval when the next synchronization is scheduled to occur.
- If Manual synchronization is displayed, the synchronization must be performed manually.

Last sync

Displays information about the last synchronization.

Show details

Click Show details, to check the status of synchronization for Identities and Identity pictures.



NOTE: If there is an issue with any of the synchronizations, a Failed message is displayed next to the failing synchronization.

2. (Optional) Review summary logs.
 - a. Click  then click Open logs folder.
 - b. Review CSV-formatted Summary logs to identify any issues that might occur during synchronization.
 - c. Read the overview Recap.txt file for a quick synchronization overview.

NOTE: The summary log files are saved in C:\ProgramData\Genetec\OneIdentity\Logs\Summary.

To review your attributes synchronization status in the ClearID web portal:

1. In the ClearID web portal, check to verify that the new attributes from the external system have been synchronized and contain the correct attributes.

- a. Click Organization > Identities and verify that your synchronized identity data is correct.

Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.7 | About ClearID One Identity Synchronization Tool logs

The Genetec ClearID™ One Identity Synchronization Tool includes logs that can be used for troubleshooting. The logs can be used to check the status of the configuration tool, the windows service, or review synchronization activities.

The ClearID One Identity Synchronization Tool uses the industry-standard Apache log4net™ framework for logging.

The logging configuration can be changed for both the synchronization service and the synchronization tool.

- To change the Genetec.ClearID.OneIdentity.SynchronizationService (OneIdentityService.exe) logging configuration, you can modify the `log4net.service.config` file.
- To change the Genetec.ClearID.OneIdentity.SynchronizationTool (OneIdentityConfigurationTool.exe) logging configuration, you can modify the `log4net.ct.config` file.

These log configuration files are found in the installation folder `C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service .`

The default settings are as follows:

- Log level is WARN.
- File size before rolling is 10Mb.
- Max rolling backups is 10.

For more information about the supported values and how to change them, see the [Apache log4net](#) documentation.

Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.8 | Viewing the ClearID One Identity Synchronization Tool logs

You can use the Genetec ClearID™ One Identity Synchronization Tool logs to check the status of the configuration tool, the windows service, or review synchronization activities.

Before you begin

- [Configuring the ClearID One Identity Synchronization Tool](#)
- [Configuring synchronization settings in the ClearID One Identity Synchronization Tool](#)

What you should know

Logs are subdivided into three separate folders as follows:

Configuration

Logs related to the *Genetec ClearID™ One Identity Synchronization Tool (OneIdentityConfigurationTool.exe)*.

Service

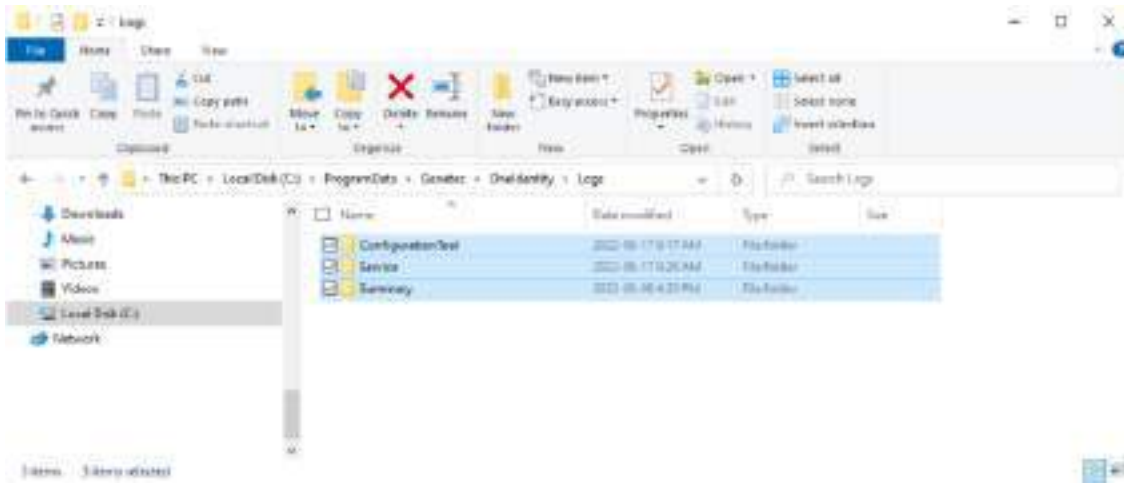
Logs related to the *Genetec.ClearID.OneIdentity.SynchronizationService (OneIdentityService.exe)*.

Summary

Logs related to synchronization summaries.

Procedure

1. Click  then click Open logs folder.



2. Review the ConfigurationTool logs if you are having connectivity issues. For example, if the synchronization tool is unable to connect to ClearID or unable to connect to Azure AD.
3. Review the Service logs if you are having data synchronization issues. For example, missing data fields, missing name fields, or missing email addresses.
4. Review the Summary logs to see a summary of synchronization activities. For example, when a synchronization started or ended and what occurred during the synchronization.
 - a. Read the Recap.txt file for a quick synchronization overview.

NOTE: The summary log files are CSV-formatted files to facilitate sorting information in Microsoft® Excel if required. They are automatically generated at the end of the synchronization.

- o If the synchronization completely fails, the summary log files are not generated.
- o If there is nothing to import, the summary log files are not created.

Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.5.9 | Updating existing identities from an external data source using ClearID One Identity Synchronization Tool

When users that have already been created have the same external ID as existing users, you can use Genetec ClearID™ One Identity Synchronization Tool to update the existing identities information from an external data source.

What you should know

This procedure is relevant for newly installed ClearID One Identity Synchronization Tool service when the Genetec ClearID™ environment already contains identities that are also present in the external system data source.

- When an external ID already exists in ClearID, that identity is updated with the values provided in the data sources.
- When an identity from the data source does not exist in One Identity (for example, on the first synchronization), the service tries to create the identity in ClearID.
- When the creation fails because the identity already exists, that identity is then fetched and updated.

Procedure

1. To reproduce a newly installed service, delete the file mappings under %ProgramData%\Genetec\OneIdentity\Configuration.
2. Configure a data source that already contains one or more identities that are present in ClearID.

The identities in the data source should have the same external ID and email as the identities in ClearID.
3. Start the synchronization and wait for completion.

Results

The identities in ClearID are updated with the mappings from the data source.

Parent topic: [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

12.6 | Synchronizing identities using LDAP in ClearID

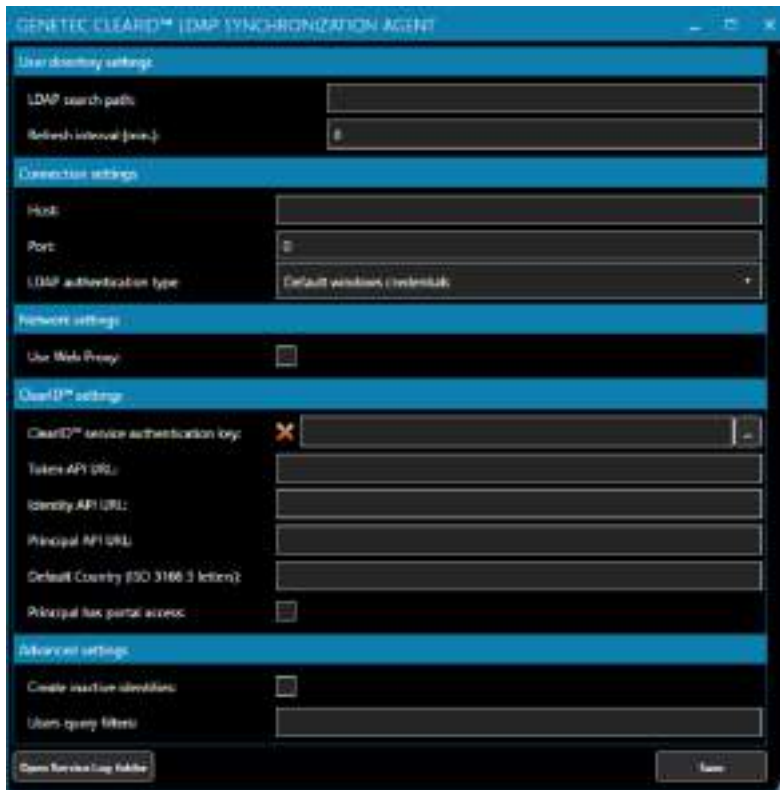
Use the Genetec ClearID™ LDAP Synchronization Agent to synchronize Active Directory (AD) Lightweight Directory Access Protocol (LDAP) attributes into Genetec ClearID™ identity attributes. These identity attributes in ClearID can then be used to assign people to roles and automate role-based access control.

Procedure

1. [Learn about the Genetec ClearID™ LDAP Synchronization Agent.](#)
2. [Learn about LDAP attributes to ClearID attribute mappings.](#)
3. [Configure the Genetec ClearID™ LDAP Synchronization Agent.](#)

12.6.1 | About ClearID LDAP Synchronization Agent

The Genetec ClearID™ LDAP Synchronization Agent is a Windows application that is used to synchronize Active Directory (AD) Lightweight Directory Access Protocol (LDAP) attributes into Genetec ClearID™ identity attributes.



The ClearID LDAP Synchronization Agent application includes the following components:

- Konfigurator (Genetec.ClearID.LdapSyncAgentConfiguration.exe) is the user interface component of the windows application that is used to configure the synchronization agent.
- Genetec ClearID LDAP Synchronizer (Genetec.ClearID.LdapSyncAgent.Service.exe) is the Windows service component of the application that performs Active Directory LDAP attributes to Genetec ClearID™ identity attributes synchronization automatically in the background at intervals specified in the Synchronization Agent.

The ClearID LDAP Synchronization Agent application is intended for use by IT or security personnel responsible for Active Directory (AD) administration.

Synchronization

Identities in ClearID can come from a variety of data sources (Databases, HR, External Sources) and can be synchronized using various tools (Genetec ClearID™ LDAP Synchronization Agent, Genetec ClearID™ API, or Genetec ClearID™ One Identity Synchronization Tool).

The following information describes Active Directory LDAP synchronization:

- Synchronization of LDAP attributes into ClearID identity attributes is INBOUND only.
CAUTION:
Any changes only made to identities in ClearID can be overwritten by the next synchronization from the Active Directory.
- Synchronization occurs automatically at the intervals specified in the ClearID LDAP Synchronization Agent.
 - The *whenChanged* attribute indicates the last time that a synchronization occurred. This attribute is then used to query Active Directory users that have changed since the last synchronization so that only changed users are updated when the next synchronization occurs.
 - The first time a synchronization occurs, all Active Directory user attributes are synchronized.
 - The next time a synchronization occurs, only Active Directory user attributes that have changed since the last time the agent ran are synchronized.

Parent topic: Synchronizing identities using LDAP in ClearID

12.6.2 | LDAP attributes to ClearID attribute mappings

When you synchronize an Active Directory (AD) with Genetec ClearID™ using the ClearID LDAP Agent Configurator, Lightweight Directory Access Protocol (LDAP) attributes are mapped to ClearID identity attributes.

LDAP attributes to ClearID attribute mappings

LDAP attributes	ClearID identity attributes
whenChanged IMPORTANT: The <i>whenChanged</i> attribute indicates the last time a synchronization with the ClearID LDAP Synchronization Agent occurred. This attribute is then used to query Active Directory users that have changed since the last synchronization so that only changed users are updated when the next synchronization occurs.	Not applicable
userAccountControl	Status NOTE: The ClearID <i>Status</i> attribute is set to inactive if the Active Directory attribute <i>userAccountControl</i> is set to disabled.
givenName	FirstName
sn	LastName
displayName	DisplayName
jpegPhoto	NOTE: <i>jpegPhoto</i> is used to upload a picture into the ClearID identity.
thumbnailPhoto (fallback if jpegPhoto is empty)	NOTE: <i>thumbnailPhoto</i> is used as a fallback (if jpegPhoto is empty) to upload a picture into the ClearID identity.
countryCode	CountryCode
employeeID	EmployeeNumber
employeeNumber (fallback if employeeID is empty)	EmployeeNumber
title	JobTitle
telephoneNumber	PhoneNumberPrimary
phone	PhoneNumberSecondary
Mobile (fallback if phone is empty)	PhoneNumberSecondary
department	DepartmentName
company	CompanyName
userPrincipalName NOTE: The <i>userPrincipalName</i> attribute is used as the link between the AD user and the ClearID identity.	Email, ExternalId
manager	SupervisorName
mail	Email

Parent topic: [Synchronizing identities using LDAP in ClearID](#)

12.6.3 | Configuring the ClearID LDAP Synchronization Agent

Before you can synchronize an Active Directory (AD) with Genetec ClearID™, you must first configure the Genetec ClearID™ LDAP Synchronization Agent.

Before you begin

- Download a service authentication key.
- Install the ClearID LDAP Synchronization Agent on its own dedicated server. It does not require a Security Center server.
NOTE: The ClearID LDAP Synchronization Agent is not generally available as a public download. The synchronizer download is supplied by your Deployment contact when needed.
- Part number: CD-IDSYNC-SERVICE-1Y is required for LDAP import.

What you should know

This procedure is for IT or security personnel responsible for Active Directory (AD) administration.
Synchronization of LDAP attributes into ClearID identity attributes is INBOUND only.

CAUTION:

Any changes only made to identities in ClearID can be overwritten by the next synchronization from the Active Directory.

Procedure

1. Open the ClearID LDAP Synchronization Agent (Genetec.ClearID.LdapSyncAgentConfiguration.exe) and configure your settings.

2. In the User directory settings section, enter your user directory details:

The User directory settings section is used to connect to the LDAP directory containing user attributes.

LDAP search path

Enter your organizational unit. For example, OU=Genetec. This search path specifies the location, root folder, or group containing Active Directory user attributes.

NOTE: The distinguishedName of the AD group is required for the LDAP search path field.

Refresh interval (min.)

Enter a refresh interval in minutes. For example, 60 to synchronize attributes every hour.

NOTE: Depending on the size of your organization and the number of attributes, *12hr.* or *24hr.* synchronizations (720 or 1440 mins) might be more appropriate.

3. In the Connection settings section, configure the host connection settings:

The Connection settings section is used to connect to the server where the User Directory settings are stored.

Host

Enter the address of your Active Directory. For example, Genetec.com.

Port

Enter the default port for your Active Directory. For example, 389.

LDAP authentication type

Select an authentication type from the following:

Genetec ClearID®; User Guide

Displayed in the header

Default windows credentials

For a client-side application, this option uses the Windows credentials (*username* and *password*) of the user running the application.

Simple bind

With the Simple bind option, the credentials (*username* and *password*) used to bind the LDAP client to the LDAP server are passed over the network unencrypted.

CAUTION:

Simple bind authentication type is not recommended in production LDAP servers.

Simple bind over SSL

Best Practice: With the Simple bind over SSL option, the credentials (*username* and *password*) used to bind the LDAP client to the LDAP server are passed over the network encrypted.

Username

If Simple bind or Simple bind over SSL was selected, enter the *username* supplied by your organization.

Password

If Simple bind or Simple bind over SSL was selected, click Set password and enter a password, then click OK.

NOTE: Use industry best practices for creating strong passwords. All passwords stored in the configuration file are encrypted.

4. (Optional) In the Network settings section, configure the Web proxy settings:

The Network settings section is used to configure proxy settings.

Use Web Proxy

Select the Use Web Proxy checkbox to specify that a proxy server is required to access the internet.

This option is typically used by customers behind a firewall or where network access to the internet is restricted.

A proxy server is a server that verifies and forwards incoming client requests to other servers for further communication. For example, when a client is unable to meet the security authentication requirements of the server but should be permitted access to some services.

Proxy URL

If Use Web Proxy is enabled, enter the proxy URL supplied by your organization.

For example, https://proxy:8080/outgoing. This information is typically supplied by the network administration team.

Proxy Authentication

Proxy authentication is the process of validating user credentials for access to a proxy server. This authentication typically includes a *username* and can also include a *password*.

Click to select either Default Credentials or Specific Credentials:

Default Credentials

Specifies that proxy authentication is not required.

Specific Credentials

Specifies that proxy authentication is required.

Proxy Username

If proxy authentication Specific Credentials was enabled, enter the proxy username supplied by your organization.

Proxy Password

Click Set password and enter a password, then click OK.

NOTE: Use industry best practices for creating strong passwords.

Proxy Domain

Enter the domain name supplied by your organization.

Proxy connection status

Status icons indicate a valid () or invalid () proxy connection. The status is only displayed after the Verify button has been clicked.

Verify

Click Verify to test that the connection settings for your proxy server are valid.

5. In the ClearID settings section, configure the settings:

The ClearID settings section is used to connect to ClearID services and synchronize data.

ClearID service authentication key

Click more () to navigate to and select the authentication key for your API integration. This key is used to authenticate the synchronization agent communications when making requests to your ClearID account.

-  Indicates that the synchronization agent is not connected to ClearID and a private key is needed.
-  Indicates that the synchronization agent is connected to ClearID and that the private key has been provided.

The following API URL settings are automatically completed after the ClearID service authentication key has been selected:

Token API URL (read-only)

The Token service provides the authentication token to contact the identity and principal service.

Identity API URL (read-only)

The Identity service is used to access all ClearID identity information.

Principal API URL (read-only)

The Principal service is used to give web portal access to users.

Default Country (ISO 3166 3 letters)

Enter your three-letter country code. For example, the USA or CAN.

NOTE: The three-letter country codes are based on the Alpha-3 codes in the ISO 3166-1 country codes standard.

Principal has portal access

Select the checkbox to enable ClearID web portal access for synchronized users.

6. (Optional) In the Advanced settings section, leave these fields blank.

The Advanced settings section is used to customize the synchronization agent behavior.

Create inactive identities

Select the checkbox to create inactive ClearID identities for any inactive users found in the Active Directory during synchronization.

Best Practice: This checkbox is typically cleared to prevent the creation of inactive users.

Users query filters

(Optional) Enter custom user query filters as specified by your deployment contact.

IMPORTANT: Only use this option when you are advised to by your deployment contact.

7. Click Save.

GENETEC CLEARID™ LDAP SYNCHRONIZATION AGENT

User directory settings

LDAP search path: OU=Genetec

Refresh interval (min.): 720

Connection settings

Host: Genetec.com

Port: 389

LDAP authentication type: Default windows credentials

Network settings

Use Web Proxy: ☒

Proxy URL: https://proxy:8080/outgoing

Proxy Authentication: ☒ Default Credentials ☐ Specific Credentials

Proxy connection status: Verify

ClearID™ settings

ClearID™ service authentication key: C:\Users\jdoe\Downloads\key-techdoc-johndoe_s_ldap_service_user.json

Token API URL: https://sts-demo.clearid.io

Identity API URL: https://identityservice-demo.clearid.io

Principal API URL: https://principalservice-demo.clearid.io

Default Country (ISO 3166 3 letters): CAN

Principal has portal access: ☒

Advanced settings

Create inactive identities: ☐

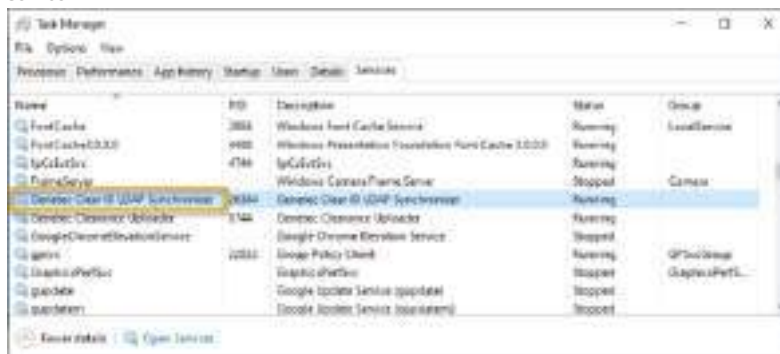
Users query filters:

Open Service Log Folder Save

The Synchronization Agent config file is saved to C:\ProgramData\Genetec ClearID LDAP Synchronizer\config.json

Tip: You can delete this file if you want to remove all your settings and configure the synchronization agent again.

8. Open the Windows Task Manager, and right-click the Genetec ClearID LDAP Synchronizer (Genetec.ClearID.LdapSyncAgent.Service.exe) windows service.



- a. If it is the first time you configure the agent, click Start to start your service so that your configuration settings are activated.
- b. If the agent is already running, click Restart to restart your service so that your configuration changes are activated.

Results

Your ClearID Synchronization Agent is now configured to automatically synchronize Active Directory LDAP attributes into ClearID identity attributes.

After you finish

1. Check the ClearID web portal to verify that the new identities for Active Directory users have been synchronized and contain the correct attributes.
2. (Optional) You can click Open Service Log folder to view the ErrorLog.txt or Eventlog.txt log files.
NOTE: The information in the *Service Log* folder is typically used when you raise a support call or if advised by your deployment contact to send Service logs to Genetec Inc..

Parent topic: [Synchronizing identities using LDAP in ClearID](#)

Browse

- [Authenticating your connection with ClearID](#)

13 | Visitor management devices

13.1 | About ClearID Self-Service Kiosk

Genetec ClearID™ Self-Service Kiosk is a mobile app that simplifies the management of visitors enrolled using the Genetec ClearID™ self-service portal. The self-service kiosk is intended for visitor centers or gated facilities where guests check-in by themselves.



Visitors can check in at the ClearID Self-Service Kiosk using several methods:

- Find a visitor associated with a visit by scanning their invitation QR code.
- Find a visitor associated with a visit by scanning their drivers license.
- Find a visitor associated with a visit by scanning their passport or citizen card (MRZ data).
- Find a visitor associated with a visit by scanning their Identity Document (various ID types from more than 200 countries).
- Find a visitor associated with a visit by their email.

NOTE: After visitors are checked-in from the ClearID Self-Service Kiosk, the host is notified by email and SMS message (if enabled).

With the ClearID Self-Service Kiosk, you can also do the following:

- Screen visitors during a self-service check-in or a self-registration.
- Take a photo of the visitor¹.
- Print a visitor badge using a wireless label printer (Bluetooth or Wi-Fi). The badge includes a photo and identifies the visitor and the event they are attending.
- Visitor self-registration.
- Company logos on the ClearID Self-Service Kiosk and visitor badges.
- Customer-specific welcome and assistance messages on the ClearID Self-Service Kiosk.

NOTE: ¹This photo is only used on the printed badge. The photo is not saved or stored for later use to ensure that visitor information is protected.

Visitor badges

The following examples show visitor badges in *portrait* and *landscape* orientation.



Badge dimensions: 10 x 6.1 cm's or 3.94 x 2.56 inches.

To download the Genetec ClearID™ Self-Service Kiosk mobile app, visit the App Store.

Browse

- Supported devices for ClearID
- Identity document types in ClearID

Browse

- ClearID Self-Service Kiosk Datasheet (2 pages)

13.1.1 | About ClearID Self-Service Kiosk check-in

Use this information to help you understand how visitors check in at a Genetec ClearID™ Self-Service Kiosk.



NOTE: Visitors can check in up to 1 hour before a visit event.

Scenario 1: Self-Service Kiosk check-in (paper badge)

Visitors can easily check in at a ClearID Self-Service Kiosk. Using their emailed QR code, visitors scan the code, take a picture, and print a visitor badge that identifies the visitor and the event they are attending.

Scenario 2: Self-Service Kiosk check-in (cardholder credential)

Using Security Center, a receptionist can assign a credential to Genetec ClearID™ visitors, the visitor can then use their card to access specified areas in the building when accompanied by their host.

Self-service check-in

The self-service check-in is intended for visitors who have been invited or pre-registered.



You can use the ClearID Self-Service Kiosk to check in yourself using QR code, ID, or email up to 1 hour before a visit event:

- If duplicate names are found, you select your unique email from list.
- If you scan a QR code that is not found, the Self-Service Kiosk switches to looking for visitor by email.
- If an ID or email is not found the Self-Service Kiosk switches to the self-registration process.

NOTE: The check-in choices displayed on the ClearID Self-Service Kiosk Welcome page can be customized to hide any options that are not relevant to your site or your visitor experience.

For more information, see the Kiosks tab section in Enabling visitor management for sites in ClearID.

Parent topic: [About ClearID Self-Service Kiosk](#)

Browse

- [Enabling visitor management for sites in ClearID](#)

13.1.2 | About ClearID Self-Service Kiosk Self registration

The Genetec ClearID™ Self-Service Kiosk self-registration process is designed to manage unplanned visits or visitors who have not been invited or pre-registered.

The self-registration workflow is triggered (if enabled for your account) when a visitor arrives on site with no invite and they are not found in the system during the self-service check-in process.

NOTE: Any pre-filled entries cannot be modified.



The self-registration process is linked to a site. Visitors are accepted automatically with default entry-level visitor access to the site. For example, Front door, reception, or check-in area to ensure a smooth check-in experience.

IMPORTANT: Any visitors on a block list will be denied access if the *watchlist* function is enabled for your account, and the *watchlist manager* is notified. In this situation, the visitor should talk to security or reception staff.

Parent topic: [About ClearID Self-Service Kiosk](#)

13.2 | Configuring the ClearID Self-Service Kiosk iPad

Before visitors can use the self-service kiosk to check in or check out, you must add the Genetec ClearID™ Self-Service Kiosk iPad device to Genetec ClearID™. Then you can register and activate the device in the ClearID Self-Service Kiosk mobile app.

Before you begin

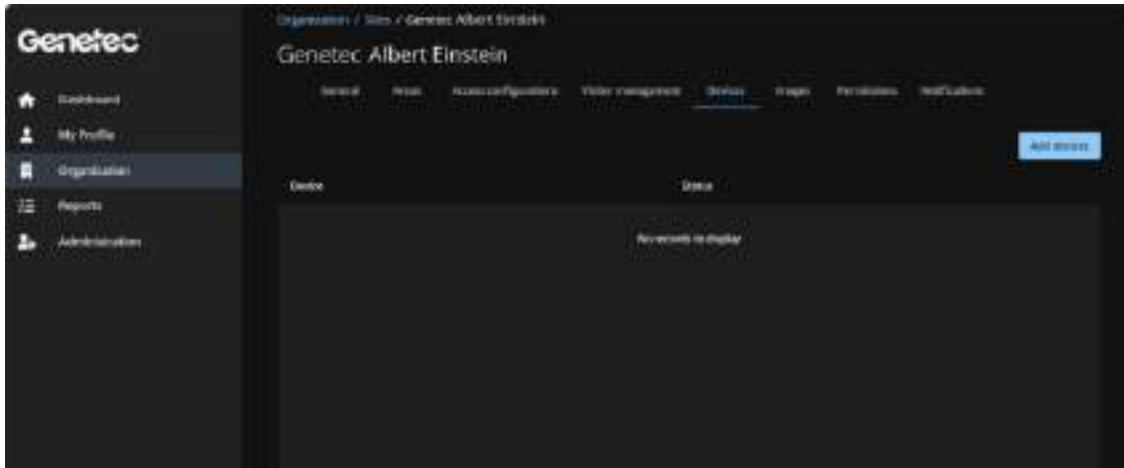
- Wi-Fi must be enabled on the self-service kiosk device before activating the device.
- Your device must be running iOS 16.6 or later.

What you should know

- Only an *administrator* or a *Site owner* can generate a device activation code in ClearID.
- You can only activate and associate a ClearID Self-Service Kiosk with one site at a time.
- The ClearID Self-Service Kiosk iPad must be on the same Wi-Fi network as the label printer.

Procedure

1. In ClearID, click Organization and select your site.
2. On the Site page, click Devices.



- a. Click Add devices to configure your ClearID Self-Service Kiosk in ClearID.
 - b. In the Add devices dialog, enter a name for the device.
Tip: Consider including the associated site or area in the name to help you easily identify your device in the future.
 - c. Enter the number of devices that you want to add, and click Add.
NOTE: You can configure up to 50 devices with a single activation code.
3. Download the ClearID Self Service Kiosk app on the iOS devices that you want to register,
 4. Activate your kiosk in ClearID:
 - a. Select your iPhone from the devices list.
 - b. In the Status field, click Generate activation code.



c. Make a note of the activation code for later use.

d. (Optional) Copy to clipboard.

Tip: Use Copy to clipboard when the person who registers the ClearID mobile operator check-in device in the ClearID portal is different to the person who activates the device. Once the code is in the clipboard, it can be emailed to the person who activates the device.

e. Click OK.

5. In the ClearID Self-Service Kiosk mobile app, enter your device activation code and tap Activate.



Results

Your self-service kiosk is now activated in ClearID and ready for use.



Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.



After you finish

- Configure your kiosk label printer
- (Optional) Customize your banner image for email notifications
- (Optional) Customize your Self-Service Kiosk configuration
- (Optional) Customize your Self-Service Kiosk badge logo

Browse

- Supported devices for ClearID
- Firewall ports used in ClearID

13.2.1 | Customizing the ClearID Self-Service Kiosk configuration

Configure your site images and kiosk options to customize the choices that are displayed to visitors using your Genetec ClearID™ Self-Service Kiosk during the check-in or check-out process. Customization can include company logos, kiosk themes, and customer-specific welcome and assistance messages.

Before you begin

Configuring the ClearID Self-Service Kiosk iPad

Tip: Ensure that your welcome screen images meet the requirements described in the  tooltip on the Visitor management > Kiosks page of the Genetec ClearID™ web portal.

What you should know

Only a site owner or account administrator can customize the kiosk configuration options.

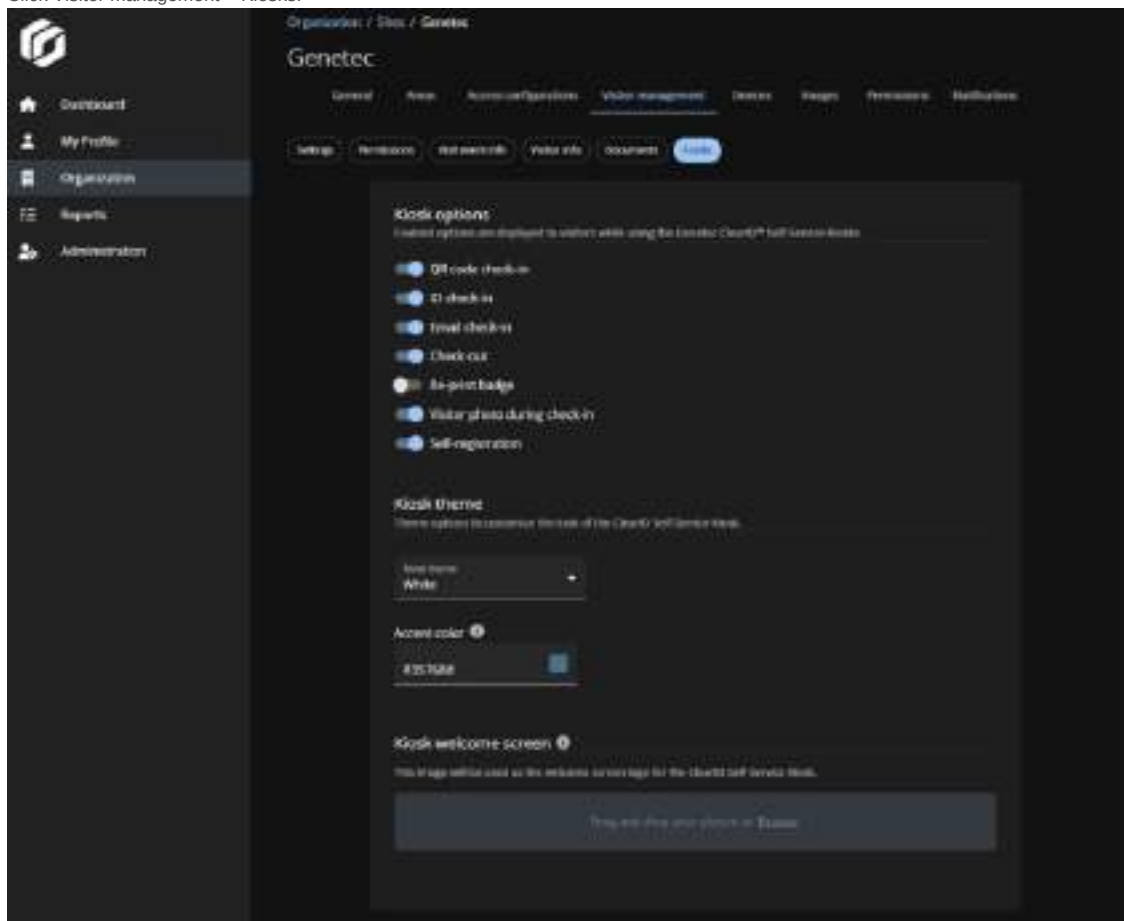
- Customized kiosk options changes are synchronized with your kiosk every 60 seconds.

Best Practice: For optimum results, use transparent .PNG images when customizing your welcome screen image.

Procedure

1. In the ClearID web portal, click Organization and select your site.

2. Click Visitor management > Kiosks.



3. In the Kiosk tab, customize your kiosk configuration options as required:

- (Optional) In the Kiosk theme section, choose a theme to customize the look of the kiosk.
For example, select the White theme and choose an Accent color that aligns with your corporate branding.
- (Optional) In the Kiosk welcome screen section, upload an image to use as the welcome screen logo.
For example, a *company name* or *logo* that aligns with your corporate branding.

For more detailed information and to see examples of these kiosk customizations, see [Enabling visitor management for sites in ClearID](#).

4. Click Save.

Example

Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages.

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com ou ative o JavaScript caso ele esteja desativado em seu navegador.

Parent topic: [Configuring the ClearID Self-Service Kiosk iPad](#)

13.2.2 | Customizing the ClearID Self-Service Kiosk visitor badge logo

You can customize the visitor badge logo image that is used on temporary badges or visitor badges printed by the kiosk.

Before you begin

Configuring the ClearID Self-Service Kiosk iPad

Tip: Ensure that your badge logo images meet the requirements described in the  tooltip on the Images page of the Genetec ClearID™ web portal.

What you should know

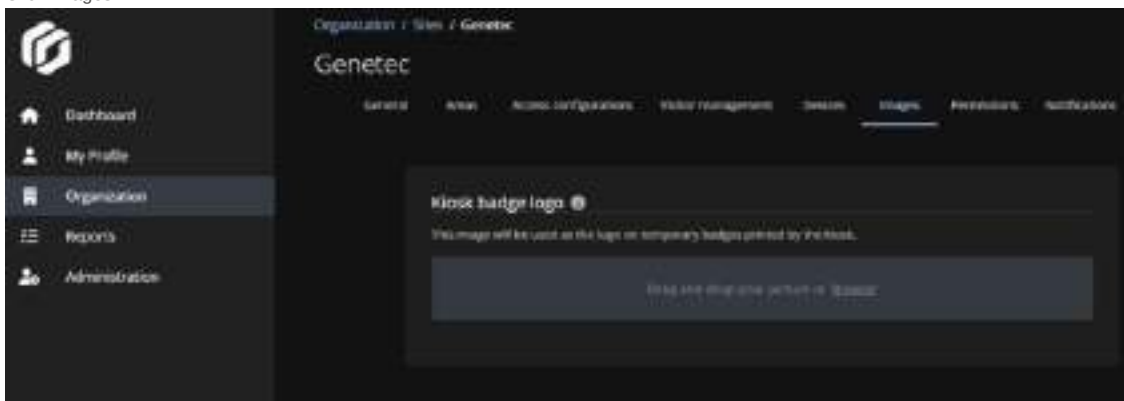
Only a site owner or account administrator can customize the visitor badge logo.

- Customized Kiosk options changes are synchronized with your kiosk every 60 seconds.

Best Practice: For optimum results, use transparent .PNG images when customizing your visitor badge logo.

Procedure

1. In the ClearID web portal, click Organization > Sites.
2. Search for and select a site.
3. Click Images.



- a. In the Kiosk badge logo section, drag and drop your picture or browse to select a Kiosk badge logo.
This image is used as the logo on temporary badges printed by the kiosk.
- b. Click Save.
The following example shows a custom badge logo for the kiosk.



Parent topic: Configuring the ClearID Self-Service Kiosk iPad

13.2.3 | Adding visitor compliance documents to the ClearID Self-Service Kiosk

For sites with special requirements, *Account administrators* and *Site owners* can upload documents like non-disclosure agreements, waivers, and more for visitors to sign when checking in using the Self-Service Kiosk.

Before you begin

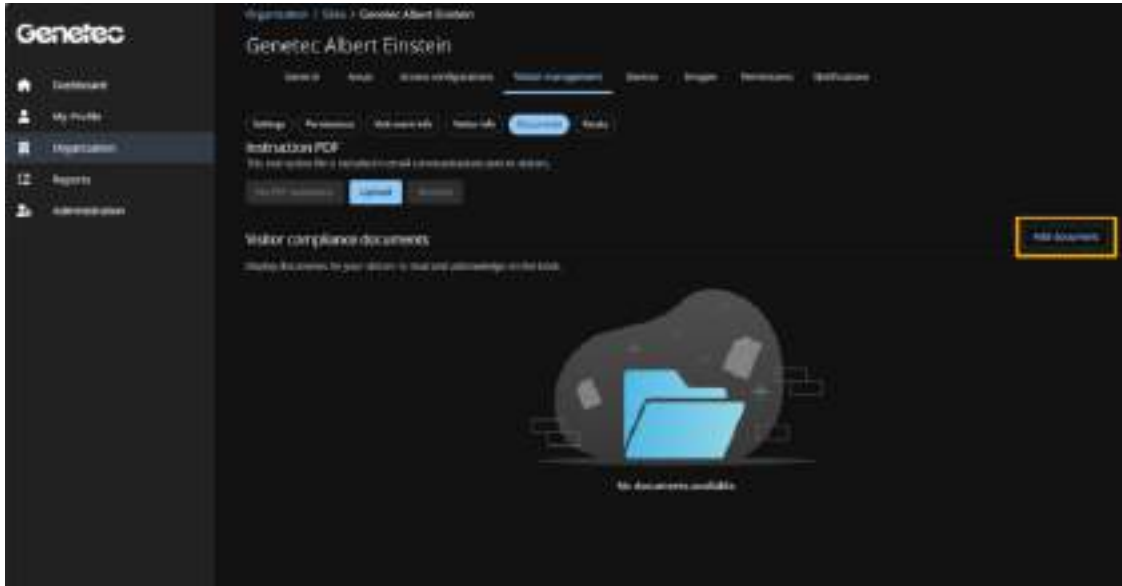
Enable visitor management for sites.

What you should know

- You must be an *Account administrator* or *Site owner* to add documents for visitors to acknowledge to the Self-Service Kiosk.
- You can display up to five documents on the kiosk during check-in.

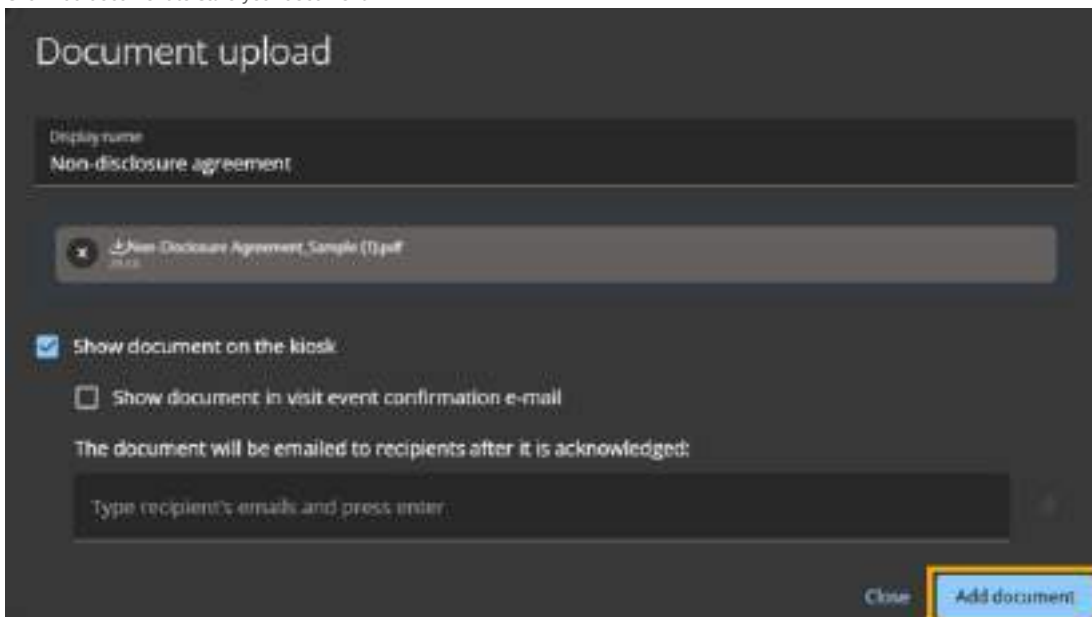
Procedure

1. In the Genetec ClearID™ web portal, click Organization > Site > Visitor management > Documents.
2. Click Add document.



IMPORTANT: These documents must be in PDF format.

- a. In the Display name field, enter a name for the document.
 - b. Drag and drop a file into the field, or click Browse to search for a file.
3. Configure your sharing preferences for the document as needed:
 - a. Select the Show document on the kiosk checkbox to show the document on the Kiosk during visitor check-in.
Tip: When the checkbox is not selected, the document remains available in draft mode.
 - b. Select the Show document in visit event confirmation e-mail checkbox to attach a copy of the document to visitor confirmation emails so that visitors can review the documents before they arrive.
 - c. Add a list of recipients who should receive a copy of the document once visitors acknowledge it.
NOTE: You can click  to copy the complete list of recipients, for example, to add the same recipients to other compliance documents.
 4. Click Add document to save your document.

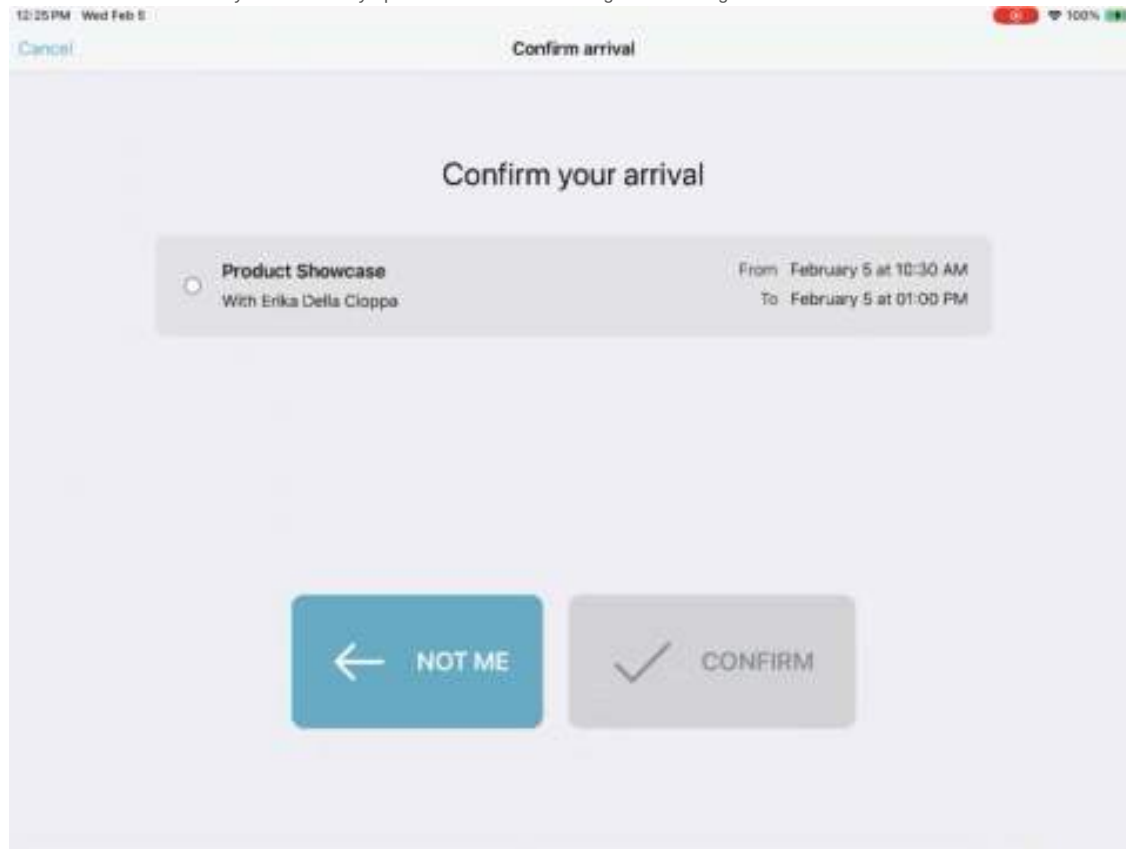


5. Use the icons to manage each uploaded document:
 - a. Click  to modify an existing document.

- b. Click  to download a local copy of the document.
- c. Click  to remove a document.

Results

Visitors have to confirm they have read any uploaded documents and sign them during check-in at the Self-Service Kiosk.



Parent topic: [Configuring the ClearID Self-Service Kiosk iPad](#)

13.2.4 | Activating badge reprinting for the ClearID Self-Service Kiosk

As a *Site owner*, you can activate badge reprinting so that visitors can reprint lost or damaged temporary badges from the ClearID Self-Service Kiosk.

Before you begin

[Configure the Self-Service Kiosk iPad.](#)

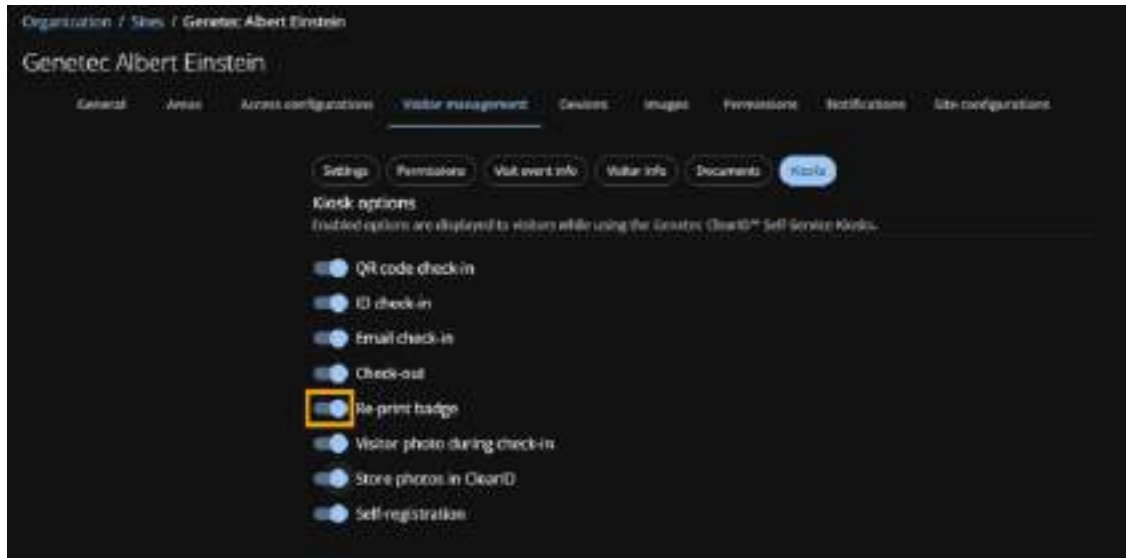
What you should know

You must be a *Site owner* to activate badge reprinting with the ClearID Self-Service Kiosk.

Best Practice: Visitor QR codes configured as credentials should only give access to non-secure areas.

Procedure

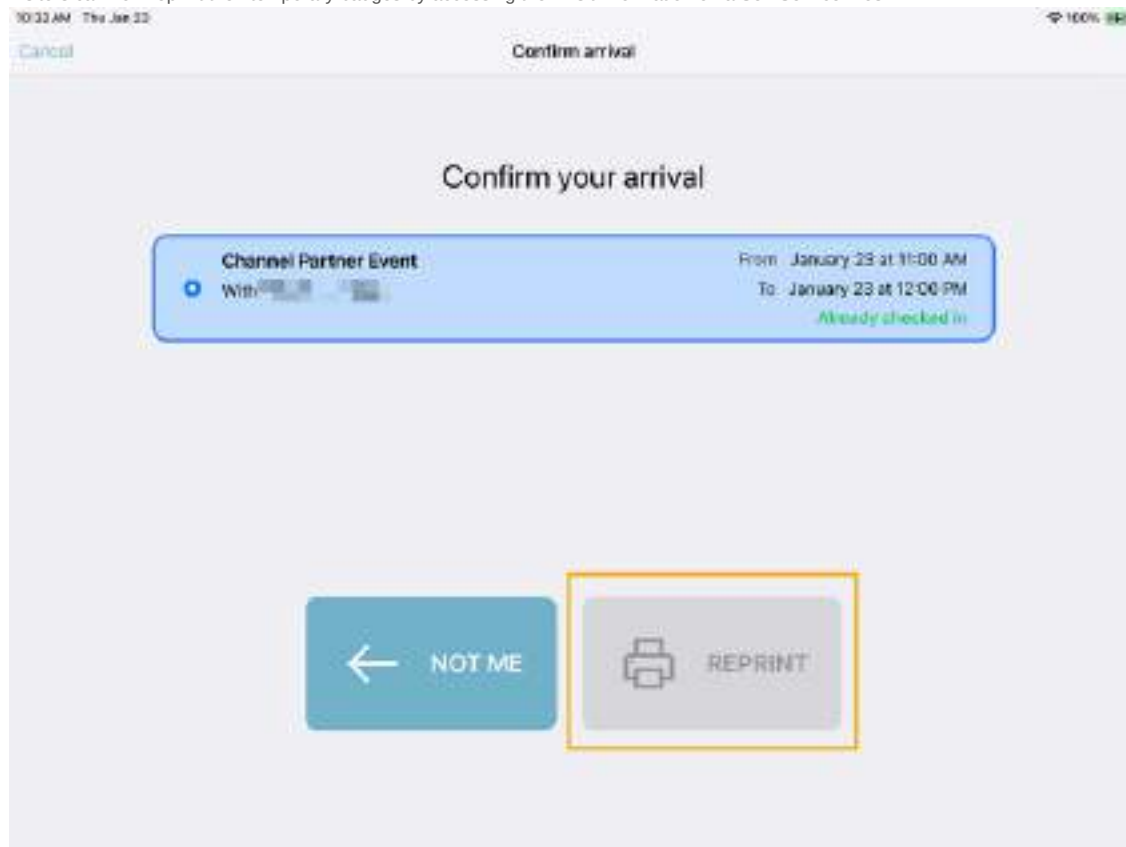
1. In the Genetec ClearID™ web portal, click Organization > Site > Visitor management > Kiosks.
2. In the Kiosk options section, turn on the Re-print badge option.



3. Click Save.

Results

Visitors can now reprint their temporary badges by accessing their visit information on a Self-Service Kiosk.



Parent topic: Configuring the ClearID Self-Service Kiosk iPad

13.2.5 | Disabling visitor photo during ClearID Self-Service Kiosk check-in

For sites where visitor privacy is crucial, *Site owners* can disable photo-taking during visitors check-in at the ClearID Self-Service Kiosk.

Before you begin

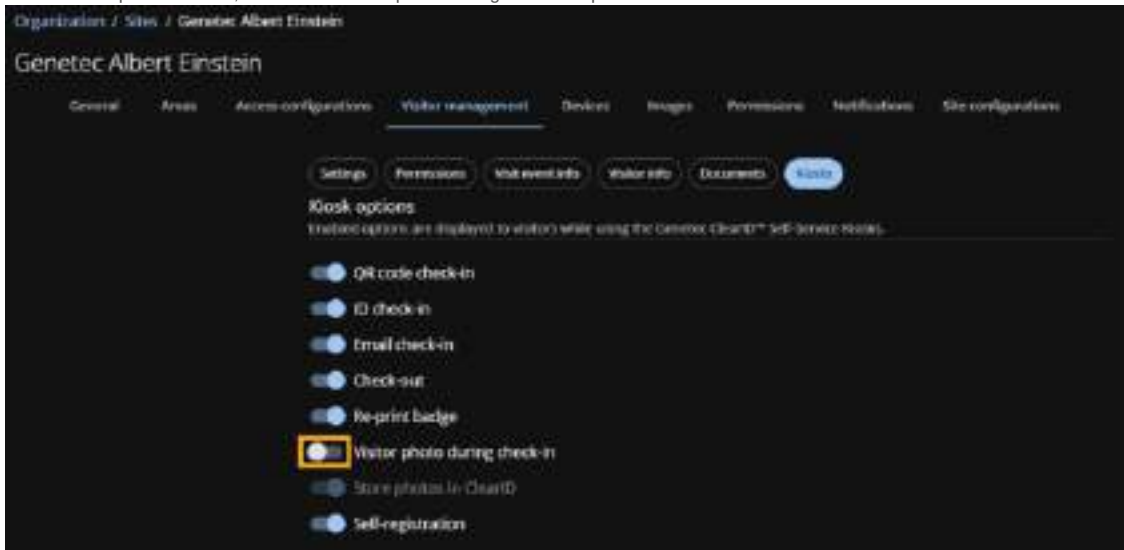
Configure the Self-Service Kiosk iPad.

What you should know

You must be a *Site owner* to disable visitor photos during check-in with the ClearID Self-Service Kiosk.

Procedure

1. In the Genetec ClearID™ web portal, click Organization > Site > Visitor management > Kiosks.
2. In the Kiosk options section, turn off the Visitor photo during check-in option.



NOTE: Visitor photo during check-in is turned on by default.

3. Click Save.

Results

Visitors can now check in at a Self-Service Kiosk without having to take a photo.

Parent topic: [Configuring the ClearID Self-Service Kiosk iPad](#)

13.2.6 | Activating visitor photo retention in ClearID

As a *Site owner* you can activate visitor photo retention to save photos of visitors taken during check-in to the Genetec ClearID™ web portal. You can access saved visitor photos for incident management and auditing purposes.

Before you begin

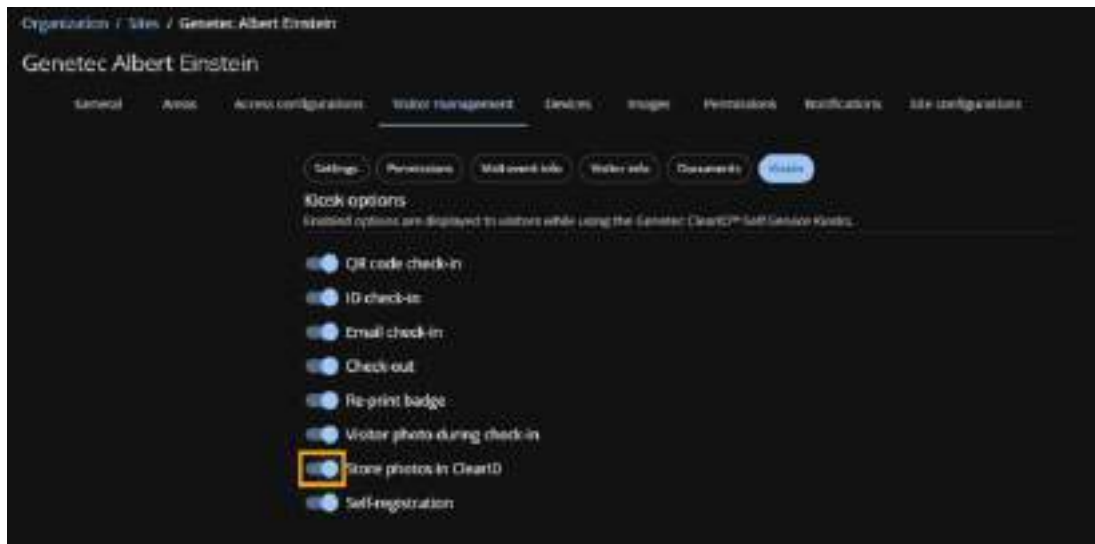
Configure the Self-Service Kiosk iPad and enable visitor photos during check-in.

What you should know

- You must be a *Site owner* to turn on visitor photo retention.
- Visitor photo during check-in must be turned on to store visitor photos in ClearID.

Procedure

1. In the ClearID web portal, click Organization > Site > Visitor management > Kiosks.
2. In the Kiosk options section, turn on the Store photos in ClearID option.



NOTE: Visitor photo during check-in is turned on by default.

3. Click Save.

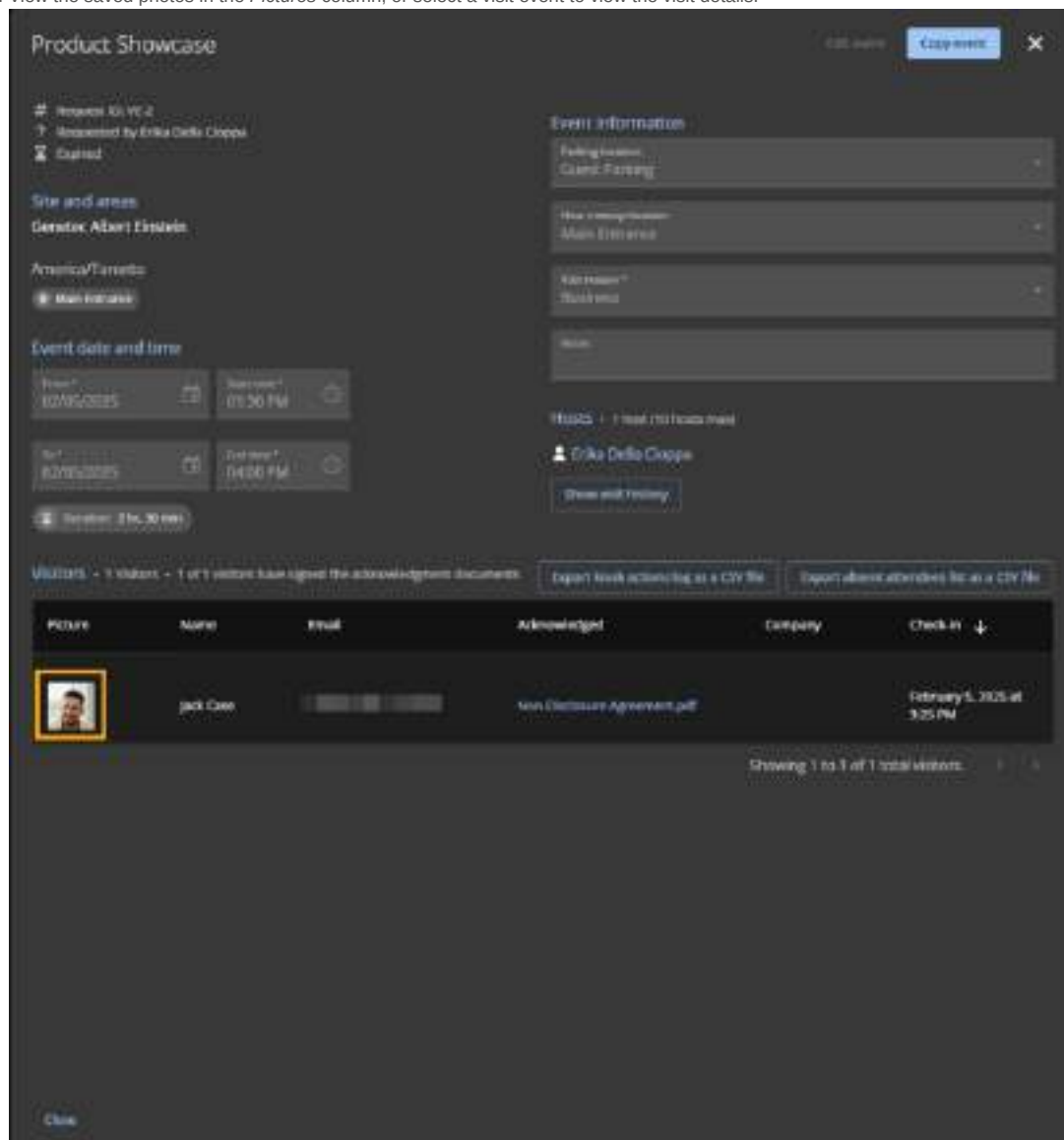
Visitor photos are stored in ClearID.

4. (Optional) View saved visitor photos.

a. In the ClearID web portal, click Reports > Visitors.

b. Filter the report as needed.

c. View the saved photos in the *Pictures* column, or select a visit event to view the visit details.



NOTE: Visitor photos are stored in ClearID for one year by default.

Parent topic: Configuring the ClearID Self-Service Kiosk iPad

13.3 | About ClearID mobile operator check-in

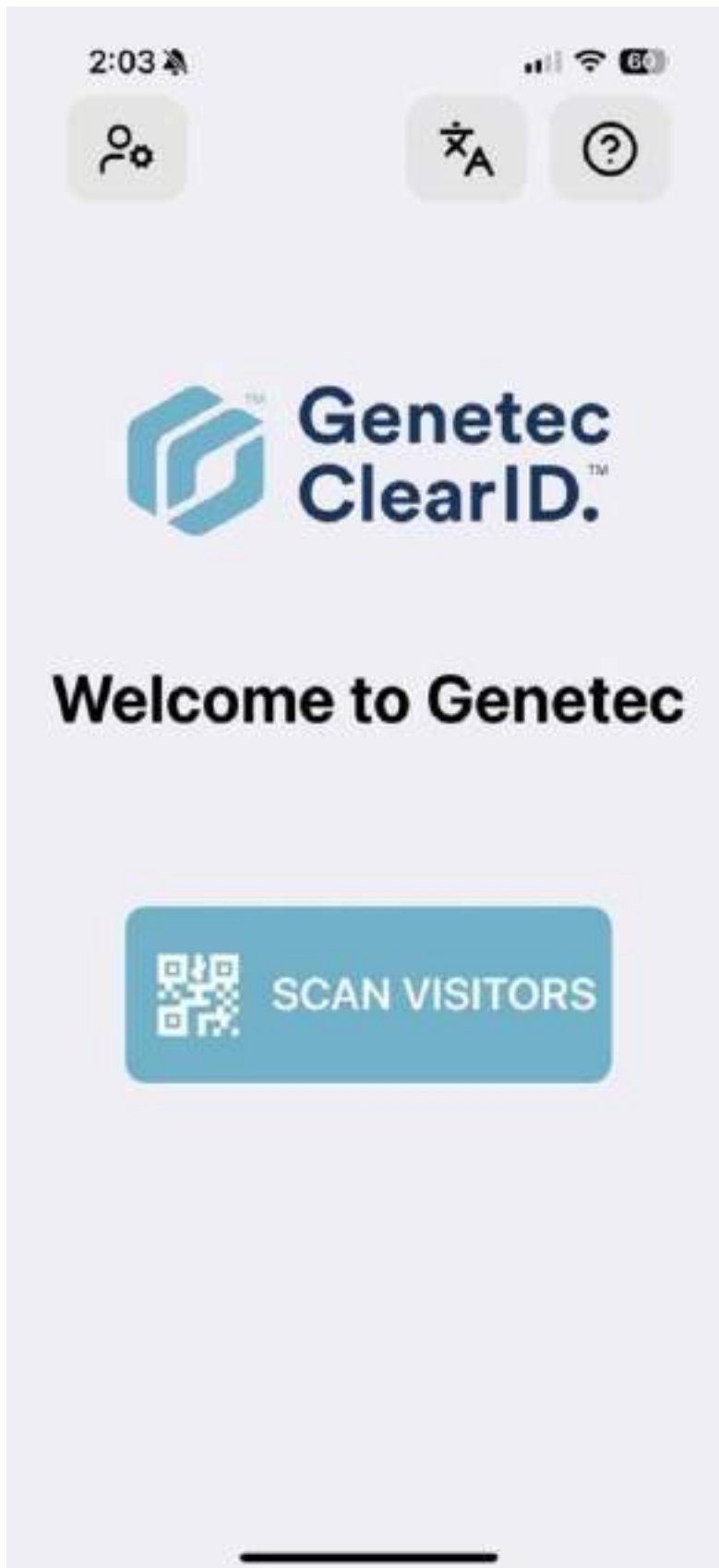
Use this information to help you understand how operators check visitors in and out of events using mobile operator check-in.



NOTE: Visitors can check in up to 1 hour before a visit event.

Mobile operator check-in

Mobile operator check-in is intended for operators in charge of checking in visitors who have been invited or pre-registered. Mobile operator check-in can be active on many iPhones at the same time, making checking into large events quicker by avoiding lineups at self-service kiosks.



Operators such as receptionists, security guards, and attendants can quickly check many visitors in at large events. Using the ClearID Self-Service Kiosk app on an iPhone, operators can scan QR codes or search for visitors by name or email.

- Visitors can't self-register when checked in by an operator.
- Mobile operator check-in doesn't scan IDs, take pictures, or print badges.

Check-in count

Once an operator scans a visitor's QR code, all visit information is displayed, including check-in and check-out options. Using these options, Genetec ClearID™ tracks the number of times visitors enter and leave your event.

13.4 | Configuring ClearID mobile operator check-in

Before you can use mobile operator check-in to check visitors into large events or look up visitor information, you must add an iPhone to Genetec ClearID™. Then you can register and activate the device in the ClearID Self-Service Kiosk mobile app.

Before you begin

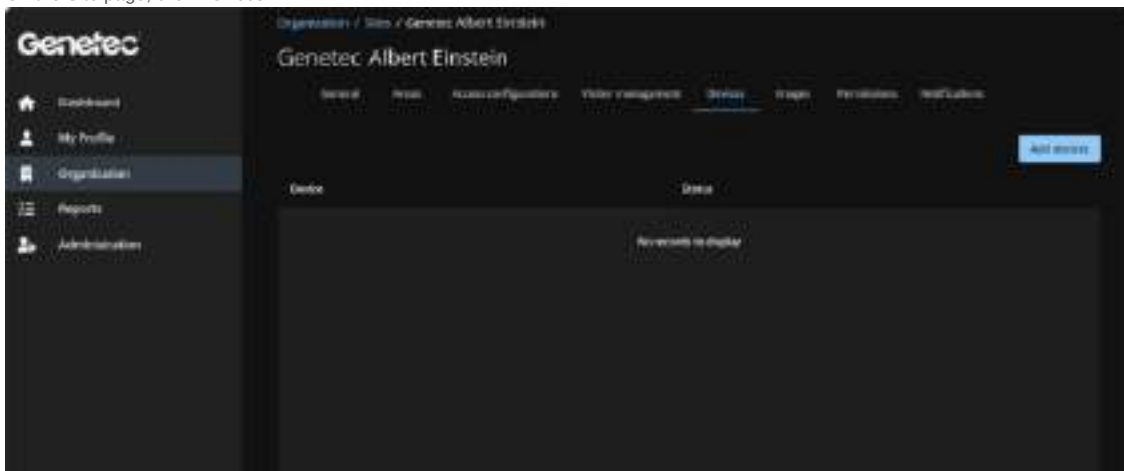
- Wi-Fi or cellular data must be enabled on the mobile operator check-in device before activating the device.
- Your device must be running iOS 16.6 or later.

What you should know

- Only an *administrator* or a *Site owner* can generate a device activation code in ClearID.
- You can only activate and associate a mobile operator check-in device with one site at a time.
- iPhones inherit the theme and settings of the self-service kiosk iPads associated with the same site.
- Check-ins using an iPhone don't require visitors to take a photo, print a badge, or acknowledge documents.

Procedure

1. In Genetec ClearID, click Organization and select your site.
2. On the Site page, click Devices.



- a. Click Add devices to configure your mobile operator check-in device in ClearID.
 - b. In the Add devices dialog, enter a name for the device.
Tip: Consider including the associated site or area in the name to help you easily identify your device in the future.
 - c. Enter the number of devices that you want to add, and click Add.
NOTE: You can configure up to 50 devices with a single activation code.
3. Download the ClearID Self Service Kiosk app on the iOS devices that you want to register.
 4. Activate your iPhone in ClearID:
 - a. Select your iPhone from the devices list.
 - b. In the Status field, click Generate activation code.



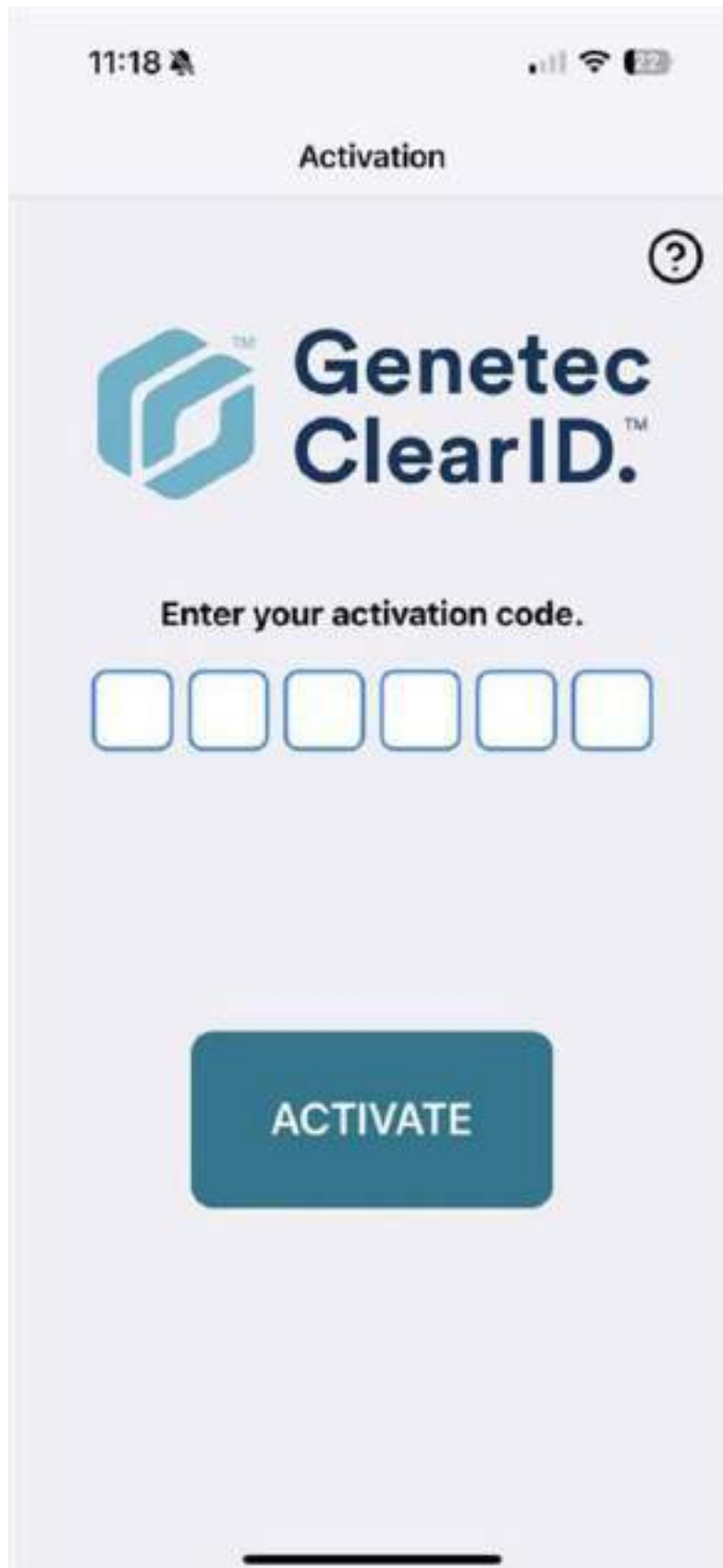
c. Make a note of the activation code for later use.

d. (Optional) Copy to clipboard.

Tip: Use Copy to clipboard when the person who registers the ClearID mobile operator check-in device in the ClearID portal is different to the person who activates the device. Once the code is in the clipboard, it can be emailed to the person who activates the device.

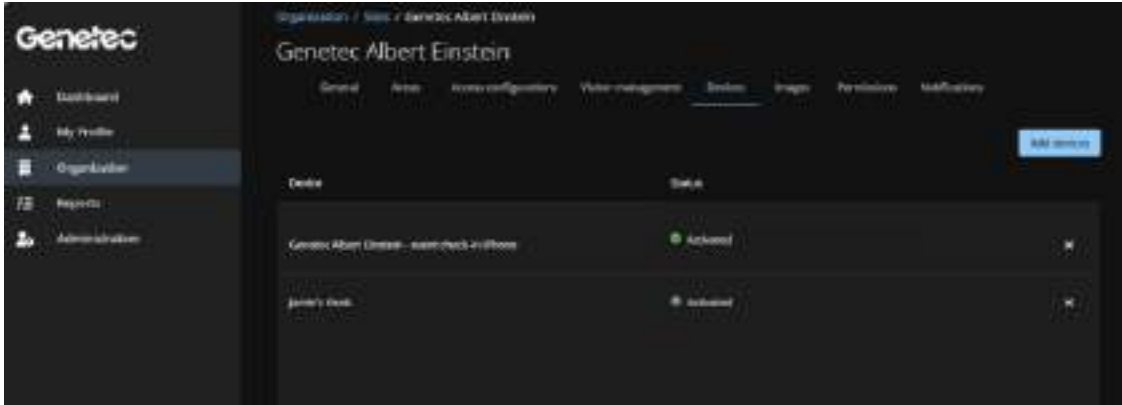
e. Click OK.

5. In the ClearID Self-Service Kiosk iPhone app, enter your device activation code and tap Activate.



Results

Your iPhone is now activated in ClearID and ready for use as a mobile operator check-in device.



13.5 | Configuring the ClearID Self-Service Kiosk label printer (Brother QL-820NWBc, QL-820NWB, or QL-810W)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother QL-810W/820NWB Quick Setup Guide \(English\)](#)
- [Brother QL-810W/QL-820NWB User Guide \(English\)](#)
- [Brother QL-820NWB LED Status indicators](#)

NOTE: The Brother QL-820NWBc replaced the Brother QL-820NWB printer (discontinued). For more information about the differences, see [Brother QL-820NWBc Specifications changes](#).

What you should know

Best Practice: Use only one label printer per kiosk and [pair the printer with the kiosk using Bluetooth](#).

If you require one label printer to be used with many kiosk devices, or you need the label printer far away from the kiosk devices use Wi-Fi or Ethernet. For example, two kiosks by the entrance and one label printer on the reception desk.

NOTE: A rechargeable Li-ion battery unit (power supply) can also be purchased and used in situations where mains power is unavailable.

Procedure

Choose one of the following:

- [Configuring Bluetooth mode \(Brother QL-820NWBc or QL-820NWB\)](#)
- [Configuring Wi-Fi mode \(Brother QL-820NWBc, QL-820NWB, or QL-810W\)](#)
- [Configuring Ethernet mode \(Brother QL-820NWBc or QL-820NWB\)](#)

After you finish

From time to time you might need to order supplies, replace the coin cell battery, recharge the optional battery unit (if used), or clean the label printer.

For more information, see *Brother QL-810W/QL-820NWB Quick Setup Guide* and *Brother QL810W/QL-820NWB User Guide*.

Browse

- [Brother QL-820NWB Label Printer FAQs](#)
- [Brother QL-820NWB printer supplies](#)

Browse

- [Supported devices for ClearID](#)
- [ClearID Self-Service Kiosk options](#)

13.5.1 | Configuring the ClearID Self-Service Kiosk label printer for Bluetooth mode (Brother QL-820NWBc or QL-820NWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother QL-810W/820NWB Quick Setup Guide \(English\)](#)
- [Brother QL-810W/QL-820NWB User Guide \(English\)](#)
- [Brother QL-820NWB LED Status indicators](#)

NOTE: The Brother QL-820NWBc replaced the Brother QL-820NWB printer (discontinued). For more information about the differences, see [Brother QL-820NWBc Specifications changes](#).

What you should know

When using the Brother QL-820NWBc or QL-820NWB label printer in Bluetooth printing mode, the following applies:

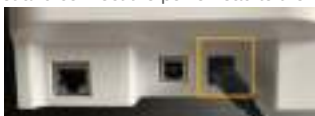
- One label printer can be paired with only one kiosk.
- The label printer must be within 30ft of the kiosk.

NOTE: A rechargeable Li-ion battery unit (power supply) can also be purchased and used in situations where mains power is unavailable.

Procedure

1. Plug printer AC adapter into a power outlet and connect the power lead to the label printer.

Brother QL-820NWBc label printer (rear)



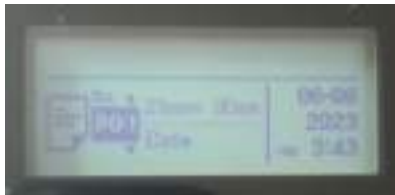
Brother QL-820NWB label printer (rear)



2. Press the Power button to turn the label printer on.

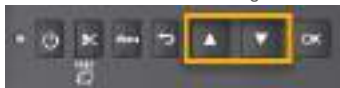


3. (Optional) If you see Template Mode menu and the incorrect label size displayed, disable it.



- a. Press Menu, navigate to Template Settings and turn off the Template Mode setting.

4. Use the arrow buttons to navigate the label printer menu.



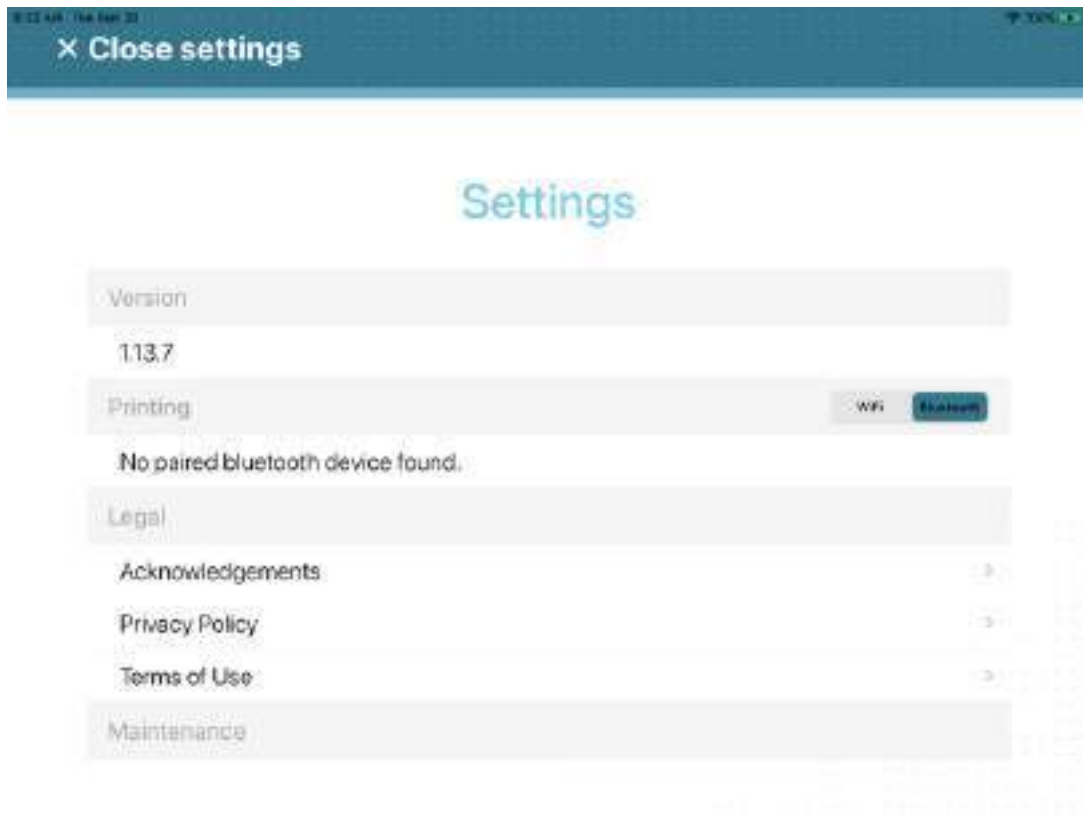
- a. Select Bluetooth > Bluetooth (On/Off) > On in the settings menu and press OK.

- b. Select Bluetooth > Automatic Reconnection (On/Off) > On in the settings menu and press OK.

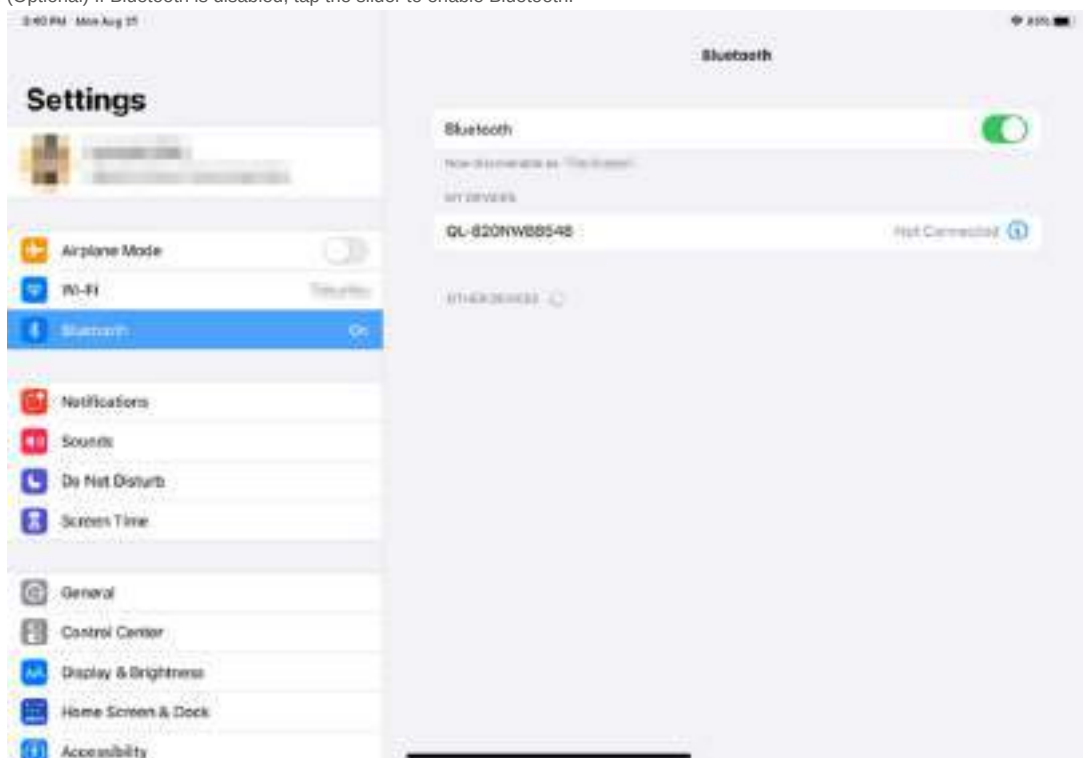
5. Pair your Bluetooth label printer with your ClearID Self-Service Kiosk iPad.

- a. In the Self-Service Kiosk mobile app, tap Settings (⚙️).

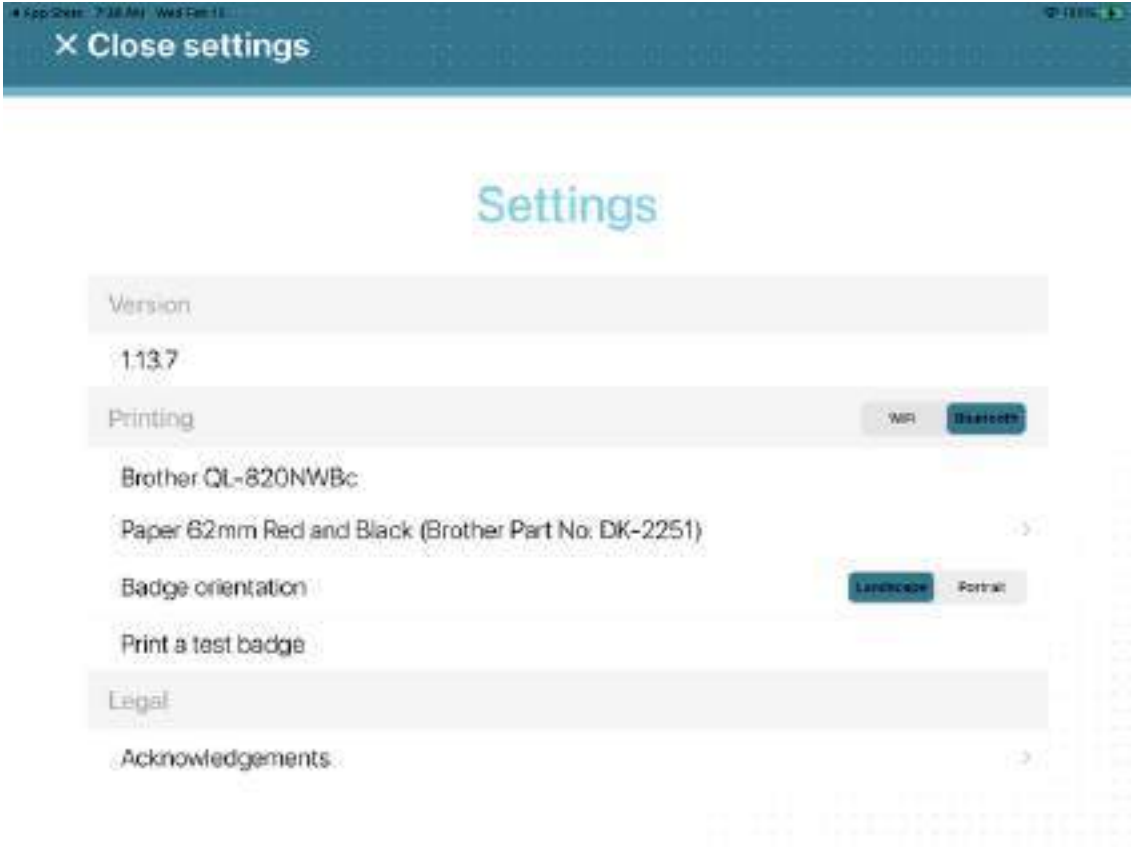
- b. In the Printing section, tap the slider control to select Bluetooth.



6. On your iPad, navigate to the Apple Settings icon, tap Settings > Bluetooth.
 - a. (Optional) If Bluetooth is disabled, tap the slider to enable Bluetooth.



- b. Click the correct printer to pair the ClearID Self-Service Kiosk iPad with your printer.
7. In the Self-Service Kiosk mobile app, tap Settings (👤).



- a. In the Printing section, check that your Brother QL-820NWBc or QL-820NWB printer is displayed.
Tip: If the printer is not displayed or bluetooth is not selected, tap WiFi then tap Bluetooth to trigger discovery again.

After you finish

(Optional) Print a test badge.
Parent topic: [Configuring the ClearID Self-Service Kiosk label printer \(Brother QL-820NWBc, QL-820NWB, or QL-810W\)](#)
[Browse](#)

- [Firewall ports used in ClearID](#)

13.5.2 | **Configuring the ClearID Self-Service Kiosk label printer for Wi-Fi mode (Brother QL-820NWBc, QL-820NWB, or QL-810W)**

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother QL-810W/820NWB Quick Setup Guide \(English\)](#)
- [Brother QL-810W/QL-820NWB User Guide \(English\)](#)
- [Brother QL-820NWB LED Status indicators](#)

NOTE: The Brother QL-820NWBc replaced the Brother QL-820NWB printer (discontinued). For more information about the differences, see [Brother QL-820NWBc Specifications changes](#).

What you should know

- One label printer can support up to five self-service kiosks
- The label printer must be on the same Wi-Fi network as the Genetec ClearID™ Self-Service Kiosk iPad.

The Wi-Fi network must be enabled for use and support the following:

- Bonjour - required for device search.
- SNMP - required to check printer status information.
- UDP or TCP Port 9100 - required to send print data.

NOTE: A rechargeable Li-ion battery unit (power supply) can also be purchased and used in situations where mains power is unavailable.

Procedure

1. Plug printer AC adapter into a power outlet and connect the power lead to the label printer.

Brother QL-820NWBc label printer (rear)



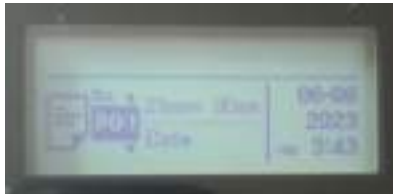
Brother QL-820NWB label printer (rear)



2. Press the Power button to turn the label printer on.

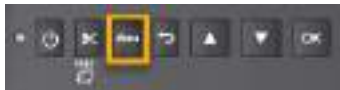


3. (Optional) If you see Template Mode menu and the incorrect label size displayed, disable it.

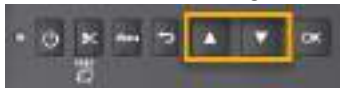


- a. Press Menu, navigate to Template Settings and turn off the Template Mode setting.

4. Press the Menu button.



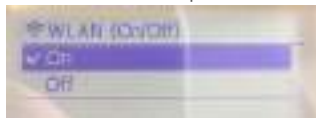
5. Use the arrow buttons to navigate the label printer menu.



6. Scroll down to the WLAN (5/7) settings and press OK.



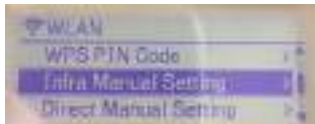
- a. Select WLAN On and press OK .



- b. In the Network Mode menu items, select Infrastructure Mode and press OK.



7. Scroll down to Infra Manual Setting and press OK.



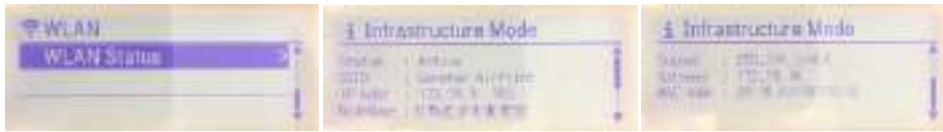
- a. After the search completes, scroll down and select your Wi-Fi network from the Service Set Identifier (SSID) list and press OK.



NOTE: Typically this network is a Wi-Fi network with AirPrint enabled.

b. When prompted enter the Wi-Fi password.

8. Navigate to WLAN Status and press OK to verify your Wi-Fi network status and IP address.



Tip: Make a note of the SSID (Wi-Fi network) and IP Addr (Label Printer IP) for later use.

- The SSID is used to verify that you are on the same Wi-Fi network as the ClearID Self-Service Kiosk iPad.
- The IP address is used later when selecting a label printer to verify you have the correct printer.

9. Select your Wi-Fi label printer.

After you finish

(Optional) Print a test badge.

Parent topic: Configuring the ClearID Self-Service Kiosk label printer (Brother QL-820NWBc, QL-820NWB, or QL-810W)

Browse

- Firewall ports used in ClearID

13.5.3 | Configuring the ClearID Self-Service Kiosk label printer for Ethernet mode (Brother QL-820NWBc or QL-820NWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- Brother QL-810W/820NWB Quick Setup Guide (English)
- Brother QL-810W/QL-820NWB User Guide (English)
- Brother QL-820NWB LED Status indicators

NOTE: The Brother QL-820NWBc replaced the Brother QL-820NWB printer (discontinued). For more information about the differences, see Brother QL-820NWBc Specifications changes.

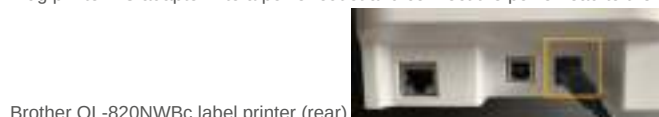
What you should know

- One label printer can support up to five self-service kiosks

NOTE: A rechargeable Li-ion battery unit (power supply) can also be purchased and used in situations where mains power is unavailable.

Procedure

1. Plug printer AC adapter into a power outlet and connect the power lead to the label printer.



Brother QL-820NWBc label printer (rear)



Brother QL-820NWB label printer (rear)

2. Make sure that the printer is turned OFF before connecting the LAN cable.

Brother QL-820NWBc label printer (rear)



Brother QL-820NWB label printer (rear)



- a. Connect a LAN cable to the LAN port on the back of the printer.

Tip: Use a straight-through Category 5 (or greater) twisted-pair cable for 10BASE-T or 100BASE-TX Fast Ethernet Network.

3. Press the Power button to turn the label printer on.



4. (Optional) If you see Template Mode menu and the incorrect label size displayed, disable it.



- a. Press Menu, navigate to Template Settings and turn off the Template Mode setting.

5. Select your label printer (Ethernet).

After you finish

(Optional) Print a test badge.

Parent topic: [Configuring the ClearID Self-Service Kiosk label printer \(Brother QL-820NWBc, QL-820NWB, or QL-810W\)](#)

Browse

- [Firewall ports used in ClearID](#)

13.6 | Configuring the ClearID Self-Service Kiosk label printer (Brother TD-4550DNWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the Brother TD-4550DNWB label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother TD-4550DNWB Quick Setup Guide](#)
- [Brother TD-4550DNWB User Guide](#)
- [Brother TD-4550DNWB online User Guide \(HTML\)](#)
- [Brother TD-4550DNWB LED status indicators](#)

What you should know

Best Practice: Use only one label printer per kiosk and [pair the printer with the kiosk using Bluetooth](#).

If you require one label printer to be used with many kiosk devices, or you need the label printer far away from the kiosk devices use Wi-Fi or Ethernet. For example, two kiosks by the entrance and one label printer on the reception desk.

Procedure

Choose one of the following:

- [Configuring Bluetooth mode \(Brother TD-4550DNWB\)](#)
- [Configuring Wi-Fi mode \(Brother TD-4550DNWB\)](#)
- [Configuring Ethernet mode \(Brother TD-4550DNWB\)](#)

After you finish

From time to time you might need to order supplies, replace the coin cell battery, or clean the label printer.

For more information, see *Brother TD-4550DNWB Quick Setup Guide* and *Brother TD-4550DNWB User Guide*.

Browse

- [Brother TD-4550DNWB Label Printer FAQs](#)
- [Brother TD-4550DNWB printer supplies](#)

Browse

- [Supported devices for ClearID](#)

13.6.1 | Configuring the ClearID Self-Service Kiosk label printer for Bluetooth mode (Brother TD-4550DNWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother TD-4550DNWB Quick Setup Guide](#)
- [Brother TD-4550DNWB User Guide](#)
- [Brother TD-4550DNWB online User Guide \(HTML\)](#)
- [Brother TD-4550DNWB LED status indicators](#)

What you should know

When using the Brother TD-4550DNWB label printer in Bluetooth printing mode, the following applies:

- One label printer can be paired with only one kiosk.
- The label printer must be within 30ft of the kiosk.

Procedure

1. Plug printer AC adapter into a power outlet and connect the power lead to the label printer.



2. Press the Power button to turn the label printer on.



3. Press the Menu button.



4. Use the arrow buttons to navigate the label printer menu.



- a. Select BLUETOOTH > BLUETOOTH (On/Off) > On in the settings menu and press OK.

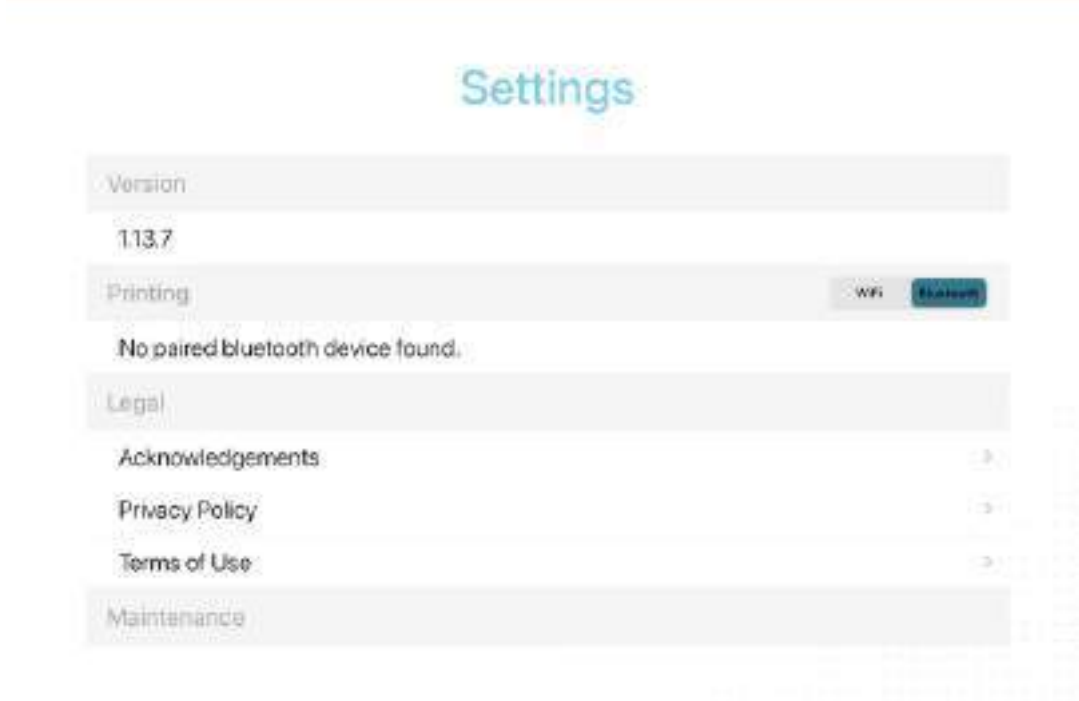


- b. Select BLUETOOTH > Automatic Reconnection (On/Off) > On in the settings menu and press OK.

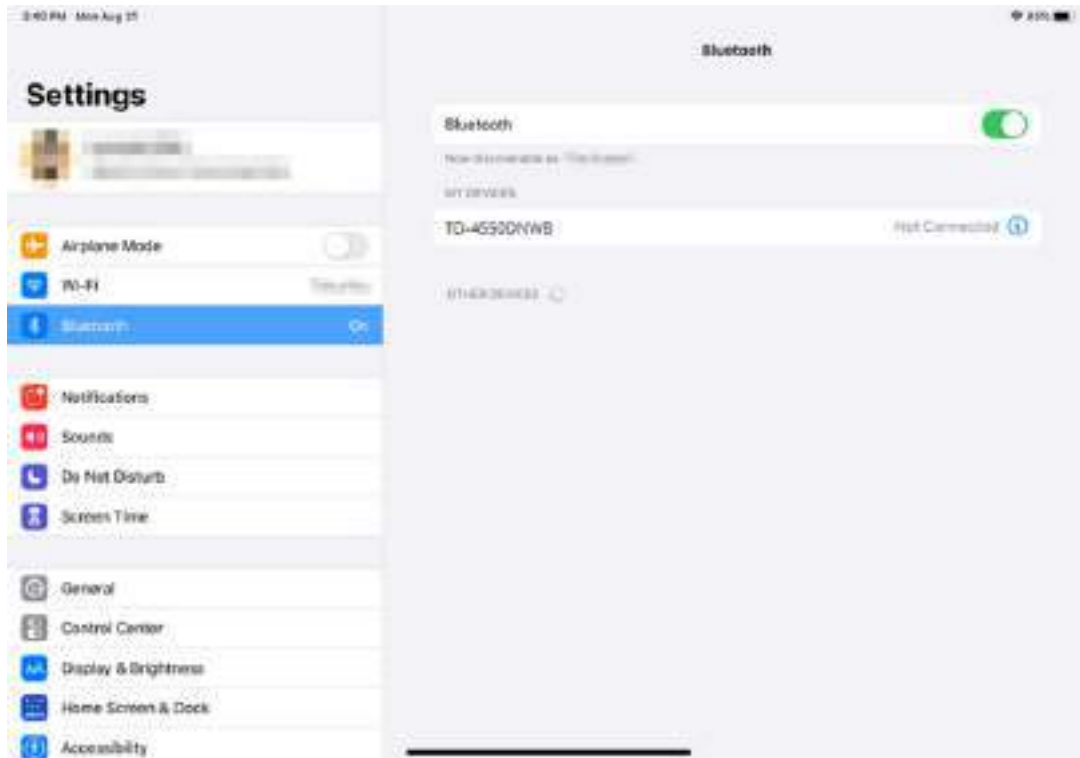


5. Pair your Bluetooth label printer with your ClearID Self-Service Kiosk iPad.

- a. In the Self-Service Kiosk mobile app, tap Settings (⚙️).
b. In the Printing section, tap the slider control to select Bluetooth.



6. On your iPad, navigate to the Apple Settings icon, tap Settings > Bluetooth.
a. (Optional) If Bluetooth is disabled, tap the slider to enable Bluetooth.



b. Click the correct printer to pair the ClearID Self-Service Kiosk iPad with your printer.

7. In the Self-Service Kiosk mobile app, tap Settings (⚙️).



a. In the Printing section, check that your Brother TD-4550DNWB printer is displayed.

Tip: If the printer is not displayed or bluetooth is not selected, tap WiFi then tap Bluetooth to trigger discovery again.

After you finish

(Optional) Print a test badge.

Parent topic: Configuring the ClearID Self-Service Kiosk label printer (Brother TD-4550DNWB)

Browse

- Firewall ports used in ClearID

13.6.2 | Configuring the ClearID Self-Service Kiosk label printer for Wi-Fi mode (Brother TD-4550DNWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- Brother TD-4550DNWB Quick Setup Guide
- Brother TD-4550DNWB User Guide
- Brother TD-4550DNWB online User Guide (HTML)
- Brother TD-4550DNWB LED status indicators

What you should know

- One label printer can support up to five self-service kiosks
- The label printer must be on the same Wi-Fi network as the Genetec ClearID™ Self-Service Kiosk iPad.
 - The Wi-Fi network must be enabled for use and support the following:
 - Bonjour - required for device search.
 - SNMP - required to check printer status information.
 - UDP or TCP Port 9100 - required to send print data.

Procedure

1. Plug printer AC adapter into a power outlet and connect the power lead to the label printer.



2. Press the Power button to turn the label printer on.



3. Press the Menu button.



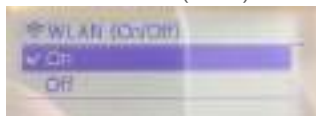
4. Use the arrow buttons to navigate the label printer menu.



5. Scroll down to the WLAN (6/8) settings and press OK.



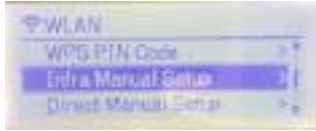
- a. Select WLAN WLAN (On/Off) > On and press OK .



- b. In the Network Mode menu items, select Infrastructure Mode and press OK.



6. Scroll down to Infra Manual Setup and press OK.



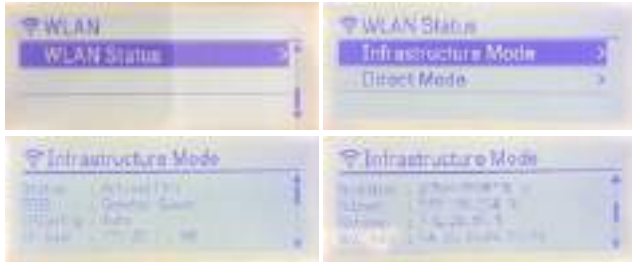
- a. After the search completes, scroll down and select your Wi-Fi network from the Service Set Identifier (SSID) list and press OK.



NOTE: Typically this network is a Wi-Fi network with AirPrint enabled.

- b. When prompted enter the Wi-Fi password.

7. Navigate to WLAN Status > Infrastructure Mode and press OK to verify your Wi-Fi network status and IP address.



Tip: Make a note of the SSID (Wi-Fi network) and IP Addr (Label Printer IP) for later use.

- The SSID is used to verify that you are on the same Wi-Fi network as the ClearID Self-Service Kiosk iPad.
- The IP address is used later when selecting a label printer to verify you have the correct printer.

8. Select your label printer (Wi-Fi).

After you finish

(Optional) Print a test badge.

Parent topic: [Configuring the ClearID Self-Service Kiosk label printer \(Brother TD-4550DNWB\)](#)

Browse

- [Firewall ports used in ClearID](#)

13.6.3 | Configuring the ClearID Self-Service Kiosk label printer for Ethernet mode (Brother TD-4550DNWB)

Before visitors can use the Genetec ClearID™ Self-Service Kiosk to check in, you must configure the label printer so that labels can be printed during the check-in process.

Before you begin

Familiarize yourself with the following:



- [Brother TD-4550DNWB Quick Setup Guide](#)
- [Brother TD-4550DNWB User Guide](#)
- [Brother TD-4550DNWB online User Guide \(HTML\)](#)
- [Brother TD-4550DNWB LED status indicators](#)

What you should know

- One label printer can support up to five self-service kiosks

IMPORTANT: Do not connect this product to any LAN connection that is subject to overvoltages.

Procedure

1. Plug printer AC adapter into a power outlet and connect the power lead to the label printer.



2. Make sure that the printer is turned OFF before connecting the LAN cable.



- a. Connect a LAN cable to the LAN port on the back of the printer.

Tip: Use a straight-through Category 5 (or greater) twisted-pair cable for 10BASE-T or 100BASE-TX Fast Ethernet Network.

3. Press the Power button to turn the label printer on.



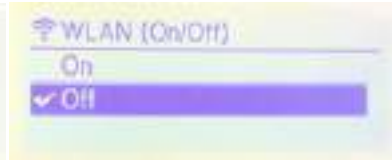
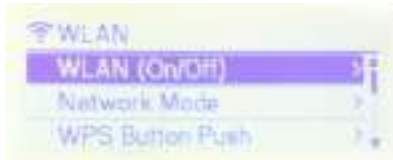
4. Press the Menu button.



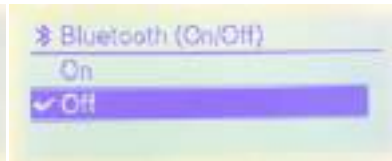
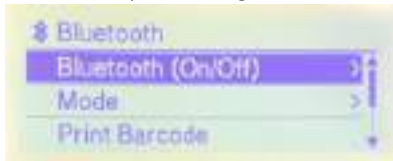
5. Use the arrow buttons to navigate the label printer menu.



6. From the label printer Settings menu, turn OFF WLAN (Wi-Fi).



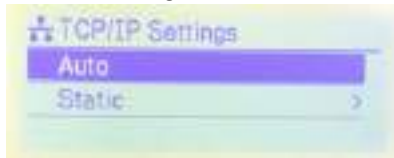
7. From the label printer Settings menu, turn OFF Bluetooth.



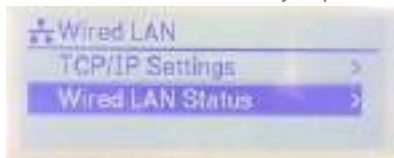
8. Scroll down to the Wired LAN (5/8) settings and press OK.



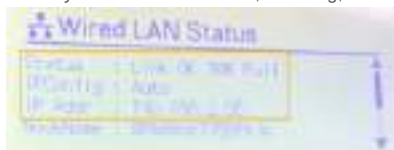
- a. Click TCP/IP Settings and select AUTO.



- b. Click Wired LAN Status to check your printer.



- c. Check your connection Status, IPConfig, and IP Addr.



Tip: Make a note of your IP address and other settings for later use when selecting your printer.

9. Select your label printer (Ethernet).

After you finish

(Optional) Print a test badge.

Parent topic: [Configuring the ClearID Self-Service Kiosk label printer \(Brother TD-4550DNWB\)](#)

Browse

- [Firewall ports used in ClearID](#)

13.7 | Selecting a ClearID Self-Service Kiosk label printer

Before you can print visitor badges from the Genetec ClearID™ Self-Service Kiosk, you must select a label printer.

Before you begin

Do one of the following:

- [Configure the Brother QL-820NWBc or QL-820NWB Self-Service Kiosk Label Printer](#)
- [Configure the Brother TD-4550DNWB Self-Service Kiosk Label Printer](#)

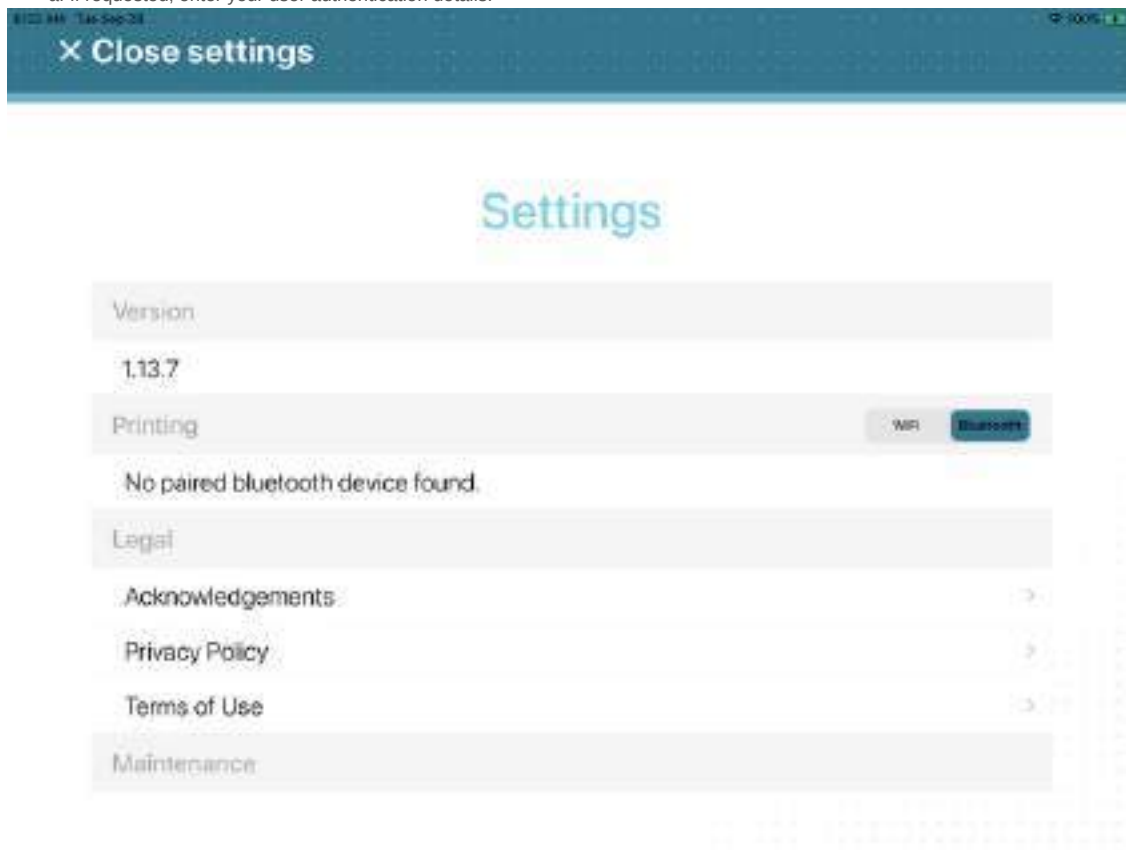
What you should know

Wi-Fi or Ethernet only: Make sure that you have the IP address of the label printer so that you can verify your selection.

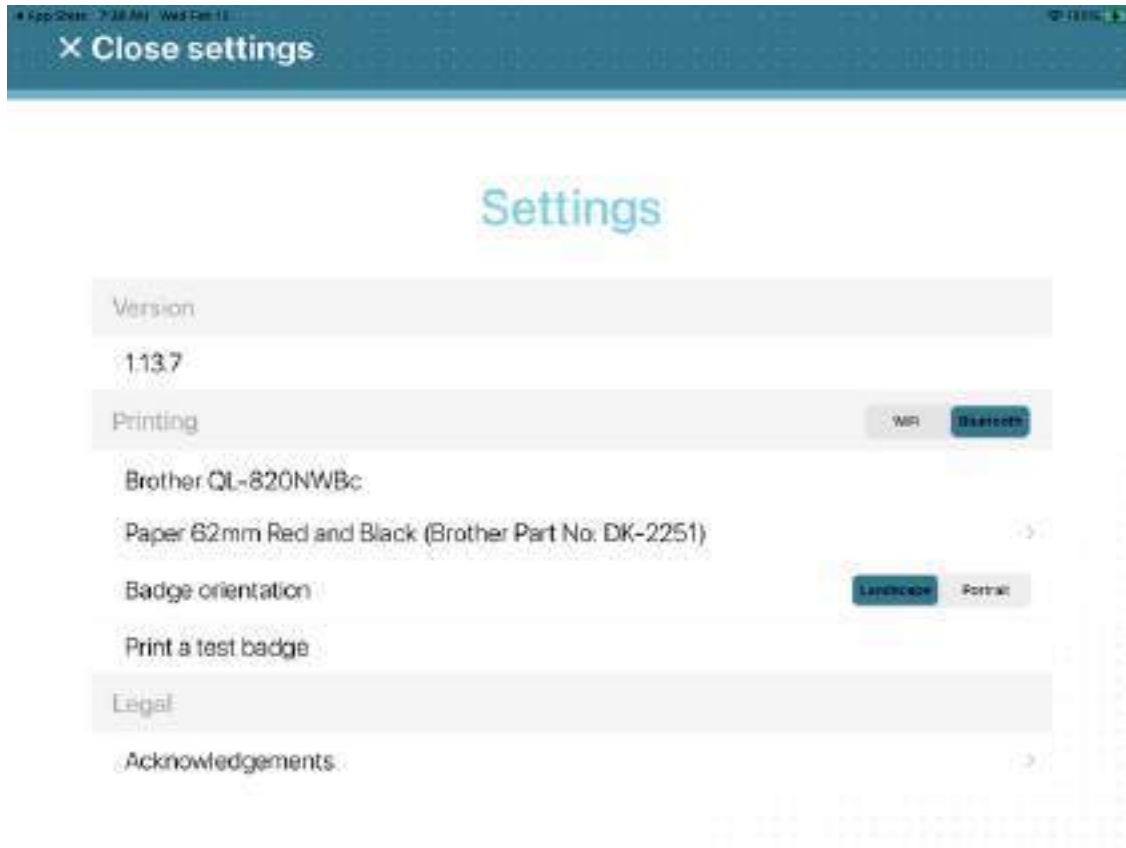
Procedure

To select a Bluetooth kiosk label printer:

1. In the Self-Service Kiosk mobile app, tap Settings (⚙️).
2. On the Settings page, tap Bluetooth to select the printing mode you require.
 - a. If requested, enter your user authentication details.



3. If you selected Bluetooth, in the Printing section, your selected printer should be displayed.

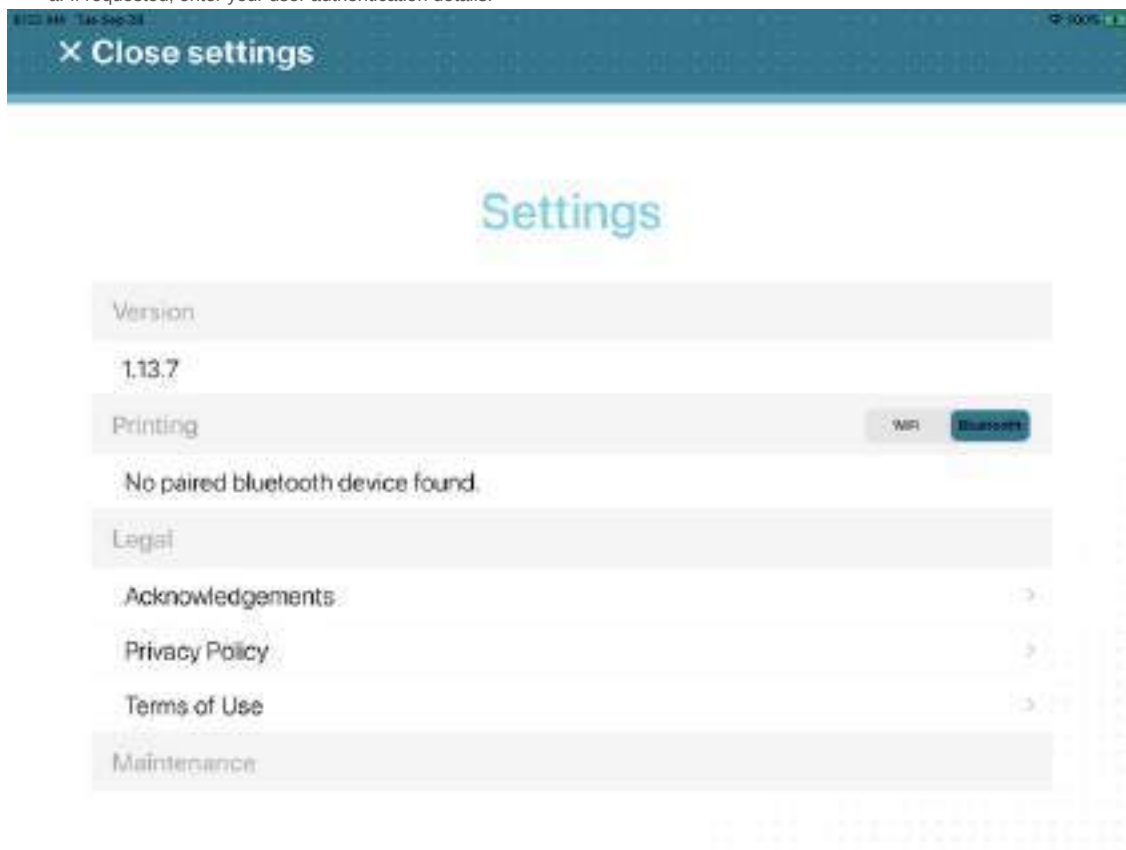


Tip: Bluetooth mode: If the printer is not displayed or bluetooth is not selected, tap WiFi then tap Bluetooth to trigger discovery again.

4. Tap Close settings to complete your printer selection setup.

To select a Wi-Fi kiosk label printer:

1. In the Self-Service Kiosk mobile app, tap Settings (👤).
2. On the Settings page, tap WiFi to select the printing mode you require.
 - a. If requested, enter your user authentication details.



3. Choose one of the following:
 - Discover WiFi printer
 - Set printer manually (IP address)

Genetec ClearID®; User Guide

Displayed in the header

- a. If you selected Discover WiFi printer, wait for the Printers list to be displayed then select your printer.
Verify that the IP address of the printer you are selecting matches the IP address seen during printer configuration.
Tip: Wi-Fi mode: If the printer is not displayed or Wi-Fi is not selected, tap Bluetooth then tap WiFi to trigger discovery again.
- b. If you selected Set printer manually (IP address), enter the IP address of the printer and tap Save.



4. Tap Close settings to complete your printer selection setup.

To select an Ethernet kiosk label printer:

1. In the Self-Service Kiosk mobile app, tap Settings (⚙️).
2. On the Settings page, tap WiFi to select the printing mode you require.
 - a. If requested, enter your user authentication details.



3. Choose one of the following:
 - Discover WiFi printer
 - Set printer manually (IP address)

- a. If you selected Discover WiFi printer, wait for the Printers list to be displayed then select your printer.
Verify that the IP address of the printer you are selecting matches the IP address seen during printer configuration.
Tip: Wi-Fi mode: If the printer is not displayed or Wi-Fi is not selected, tap Bluetooth then tap WiFi to trigger discovery again.
- b. If you selected Set printer manually (IP address), enter the IP address of the printer and tap Save.



4. Tap Close settings to complete your printer selection setup.

After you finish

Print a test badge.

13.8 | Printing a test badge from the ClearID Self-Service Kiosk

To help you understand if the printer is working as expected, you can print a test badge. This test print can be performed either after first initial setup or after replacing a label roll.

Before you begin

- Select a kiosk label printer.
- Make sure that labels are loaded in the printer.
- Make sure that labels are correctly aligned.

What you should know

The Brother QL-820NWBc, QL-820NWB, and QL-810W label printers can print either Black or Red and Black badges:

- 62mm Black (Brother Part No: DK-2205)
- 62mm Red and Black (Brother Part No: DK-2251)

The Brother TD-4550DNWB label printer can only print Black badges:

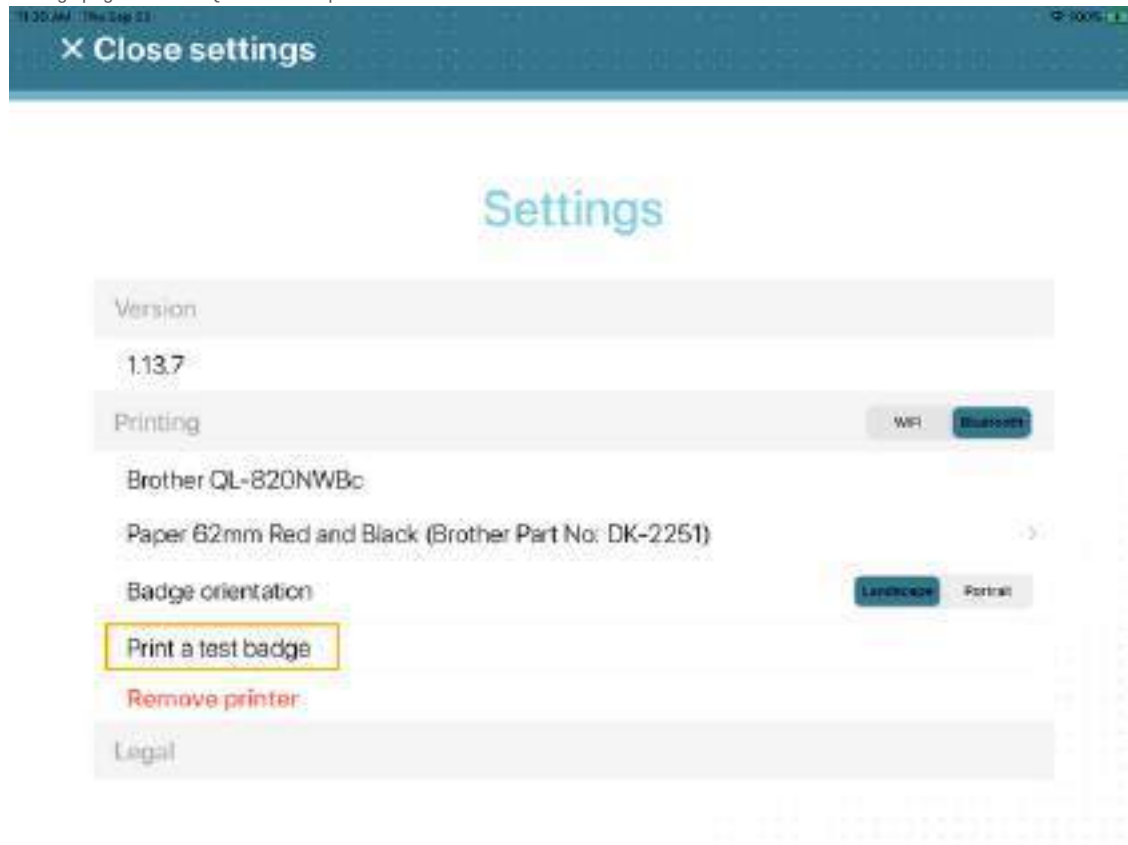
- 57mm Black (Brother Part No: RD001U1S)
IMPORTANT: The labels for the Brother TD-4550DNWB printer MUST be orientated correctly otherwise badge printing issues can occur.

Badges can be printed in either *Portrait* or *Landscape* format.

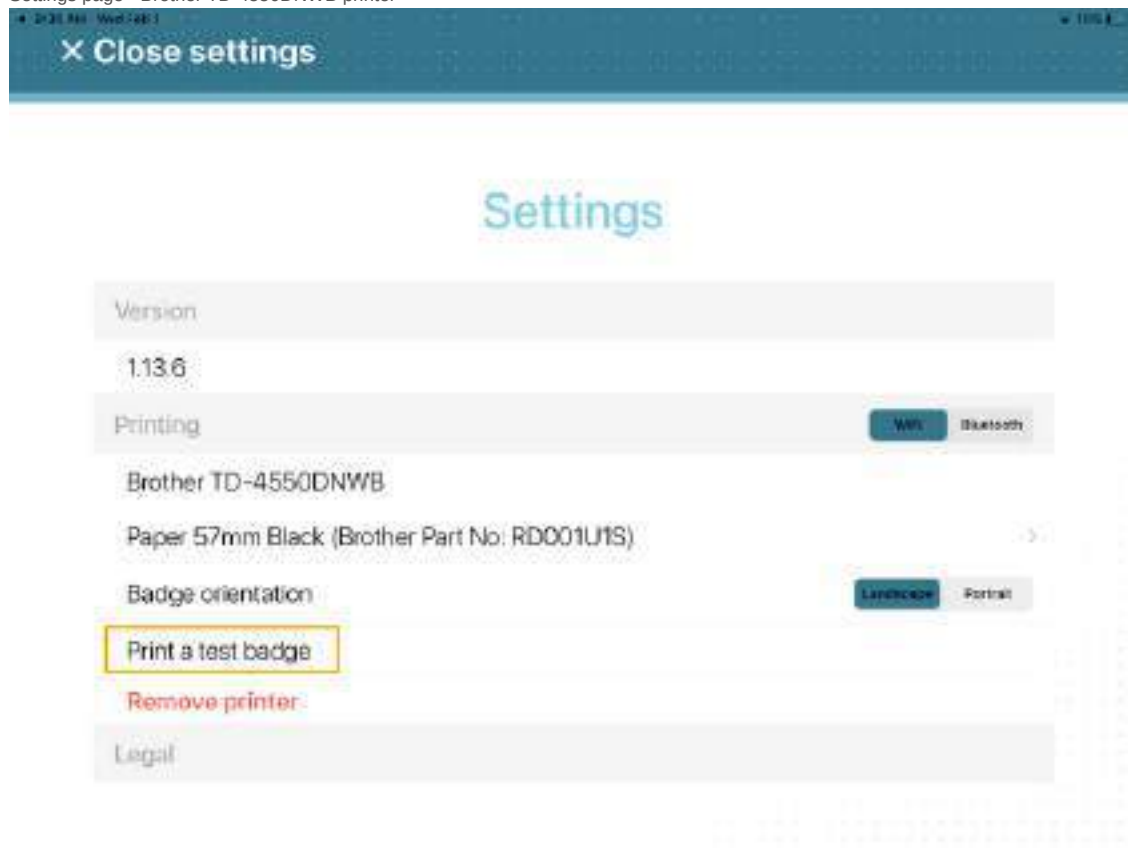
Procedure

1. In the Genetec ClearID™ Self-Service Kiosk mobile app, tap settings (⚙️).
2. In the Settings page, tap Print a test badge.

Settings page - Brother QL-820NWBc printer



Settings page - Brother TD-4550DNWB printer



3. Collect and examine your test badge.



Badge dimensions: 10 x 6.1 cm's or 3.94 x 2.56 inches.

NOTE: When printing to a Brother TD-4550DNWB label printer, your badges are printed in black and white.

Results

You are now ready for visitors to use the ClearID Self-Service Kiosk and print their own visitor badges during their check-in.

After you finish

From time to time you might need to order supplies, replace the coin cell battery, recharge the optional battery unit (Brother QL-820NWBc or QL-820NWB only), or clean the label printer.

For more information, see the third-party user guide documentation for your printer.

Browse

- [ClearID Self-Service Kiosk label printer issues](#)

13.9 | Resetting the ClearID Self-Service Kiosk mobile app

In some situations, you might need to perform a hard reset of the Genetec ClearID™ Self-Service Kiosk mobile app. For example, if you encounter issues with selecting the label printer, printing labels, listing people, or if you want to move the kiosk to another site.

Before you begin

- Make sure that you have your Apple ID information.
- Make sure that you have your Wi-Fi network information.

What you should know

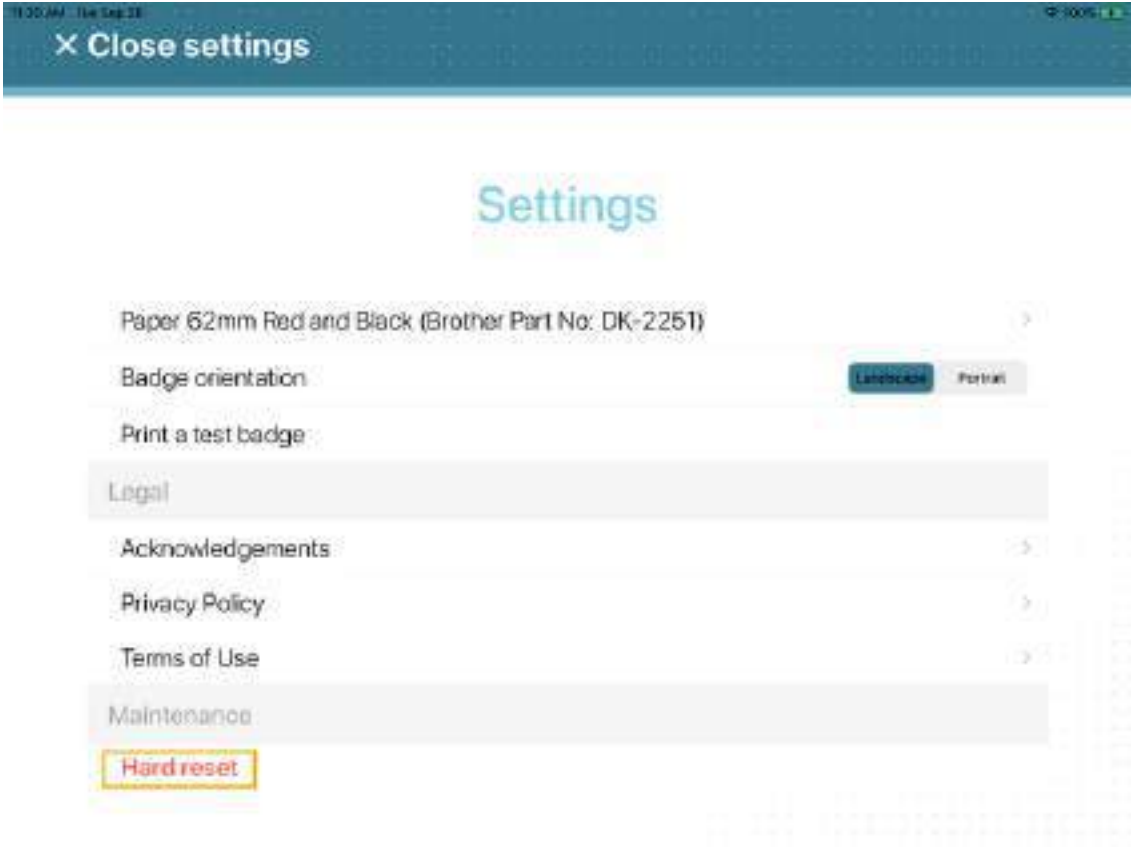
- Only an *administrator* or a *Site owner* can generate a device activation code in ClearID.

CAUTION:

The hard reset action erases all application data, user data, and visit, check-in, check-out information from the Kiosk device and performs a hard reset of the mobile app. If you proceed, you must register the kiosk device again.

Procedure

1. In the Self-Service Kiosk mobile app, tap Settings (👤).
2. In the Settings page, scroll to the bottom of the page and in the Maintenance section tap Hard reset.



3. Configure your Self-Service Kiosk iPad.
4. Configure your Self-Service Kiosk label printer.
5. Select your Self-Service Kiosk label printer.
6. Print a test badge.

Results

Your Self-Service Kiosk is now ready for use.
Browse

- ClearID Self-Service Kiosk label printer issues

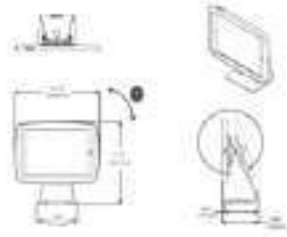
13.10 | ClearID Self-Service Kiosk options

Use the following information to help you understand the Genetec ClearID™ Self-Service Kiosk license, kiosk, and accessory options that are available.

ClearID Self-Service Kiosk license options

Item description	Part	Item
Kiosk license subscription One Genetec ClearID™ kiosk license for one, three, or five years NOTE: The ClearID Self-Service Kiosk app on an iPhone doesn't need to be licensed.	• CID-KIOSK-LIC-1Y • CID-KIOSK-LIC-3Y • CID-KIOSK-LIC-5Y	Kiosk subscription license

ClearID Self-Service Kiosk options

Item description	Part	Item
Kiosk tabletop stand Apple iPad (Wi-Fi) with one year of Apple Care Table top kiosk kit with iPad enclosure, tabletop stand, and one iPad charging cable. (Printer <u>not included</u>) NOTE: Depending on your check-in requirements, the kiosk iPad housing on this tabletop stand can be configured for use in either <i>Portrait</i> or <i>Landscape</i> mode.	VM-KIOSK-TABLETOP-KIT¹	
Tabletop kit Table top kiosk kit with iPad enclosure, tabletop stand, and one iPad charging cable. (iPad and Printer <u>not included</u>) NOTE: Depending on your check-in requirements, the kiosk iPad housing on this tabletop stand can be configured for use in either <i>Portrait</i> or <i>Landscape</i> mode.	VM-TABLETOP-KIT¹	
Kiosk floor stand kit Apple iPad (Wi-Fi) with one year of Apple Care Floor stand kit with iPad enclosure, floor stand, one iPad charging cable, and a printer shelf (Printer <u>not included</u>) NOTE: Depending on your check-in requirements, the kiosk iPad housing on this floor stand can be configured for use in either <i>Portrait</i> or <i>Landscape</i> mode.	VM-KIOSK-FLOORSTAND-KIT¹	
Floor stand kit Floor stand kit with iPad enclosure, floor stand, one iPad charging cable, and a printer shelf (iPad and Printer <u>not included</u>) NOTE: Depending on your check-in requirements, the kiosk iPad housing on this floor stand can be configured for use in either <i>Portrait</i> or <i>Landscape</i> mode.	VM-FLOORSTAND-KIT¹	

IMPORTANT: ¹ For EMEA, APAC, and some LATCAR regions, an adapter kit (VM-KIOSK-WORLD-ADAPTER-KIT) is added to your order once you've specified your region.

The VM-KIOSK-WORLD-ADAPTER-KIT part number includes a World Travel Adapter kit and power adapter plugs to fit different electrical outlets around the world. These include North America, Japan, China, United Kingdom, Continental Europe, Korea, Australia, Hong Kong, and Brazil. Without this kit, the plug isn't compatible with the electrical outlets in your region.

ClearID Self-Service Kiosk accessories

Item description	Part	Item
World travel adapter kit Adapter plug kit that includes plugs with prongs that fit different electrical outlets around the world	VM-KIOSK-WORLD-ADAPTER-KIT	International adapter plug kit for the kiosk iPad
Visitor label printer Brother QL-820NWBc thermal printer - Network (Ethernet), Wi-Fi, and Bluetooth - Prints black and red labels NOTE: Only the Brother DK Roll - 62mm Black (Brother Part No: DK-2205) or 62mm Red and Black (Brother Part No: DK-2251) labels are supported.	Brother QL-820NWBc Kit part numbers: - VM-KIOSK-PRINTER-NA-KIT - VM-KIOSK-PRINTER-AU-KIT - VM-KIOSK-PRINTER-BRA-KIT - VM-KIOSK-PRINTER-EU-KIT - VM-KIOSK-PRINTER-IN-KIT - VM-KIOSK-PRINTER-UK-KIT	

For more information or to order kiosk parts, see [Genetec Parts Manager](#).
Browse

- License options for ClearID system integration
- Supported devices for ClearID

Browse

- [ClearID Self-Service Kiosk Datasheet \(2 pages\)](#)

13.10.1 | ClearID Self-Service Kiosk floor stand

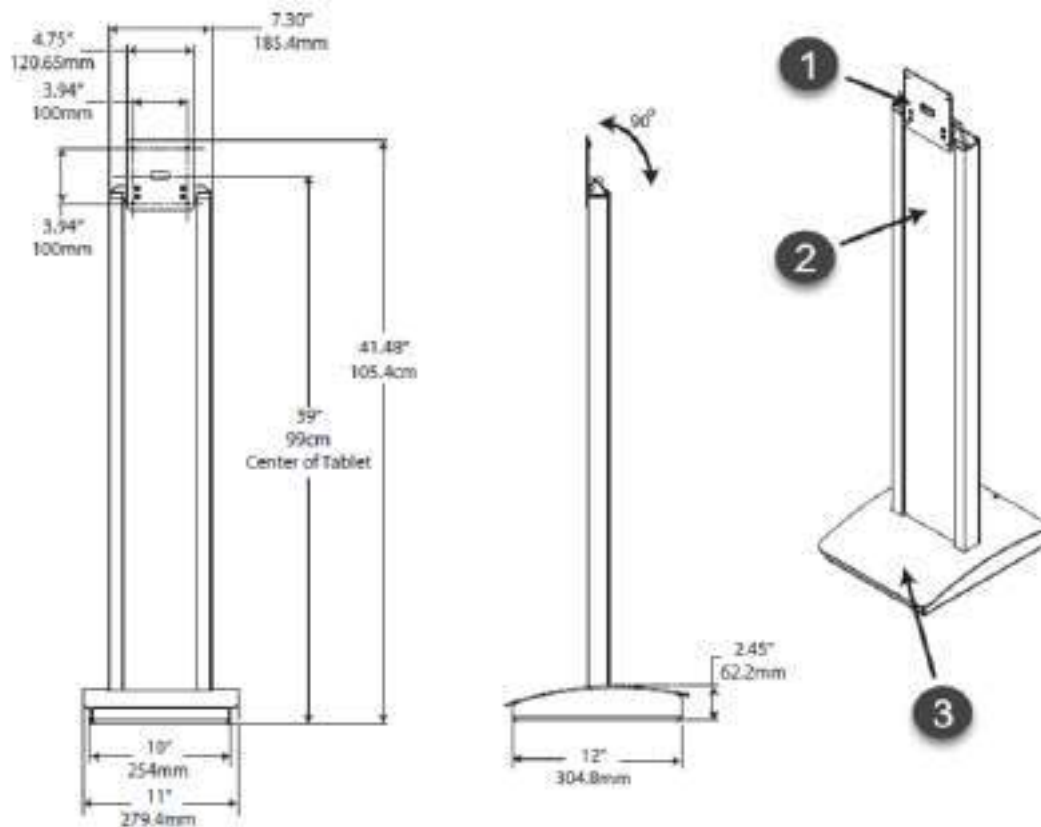
Use the following information to help you understand the Genetec ClearID™ Self-Service Kiosk floor stand dimensions, mounting, and features.



NOTE: Depending on your check-in requirements, the ClearID Self-Service Kiosk iPad housing can be configured on this floor stand for use in either *Portrait* or *Landscape* mode.

Floor stand dimensions

The following diagram illustrates the floor stand dimensions including the height and footprint of the stand.



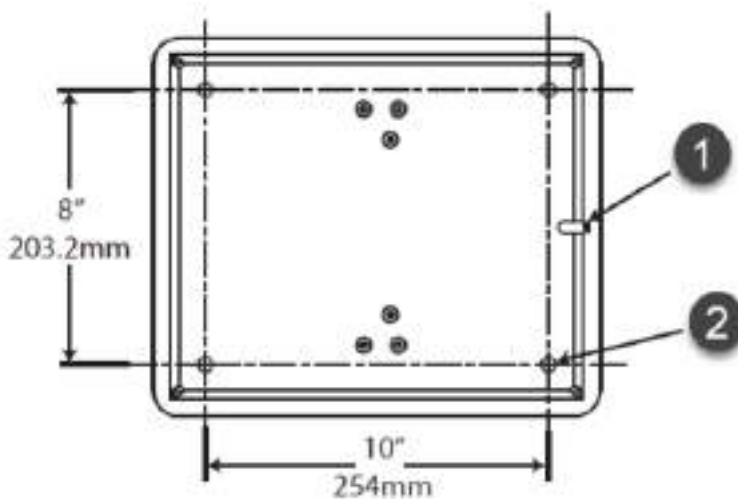
¹ Mount supports any tablet enclosure with a standard VESA mount (100mm x 100mm) or a 90° degree rotation adapter.

² Removable signage panel (included).

³ Removable cover provides access to the storage area for the power supply.

Floor mount

The following diagram illustrates the floor mount dimensions and underside view of the kiosk floor stand.



¹ Opening for power supply cable.

² 4x floor mounting holes for 0.25inch or 6mm screw hardware (not included) used to secure the floor stand to the floor surface.

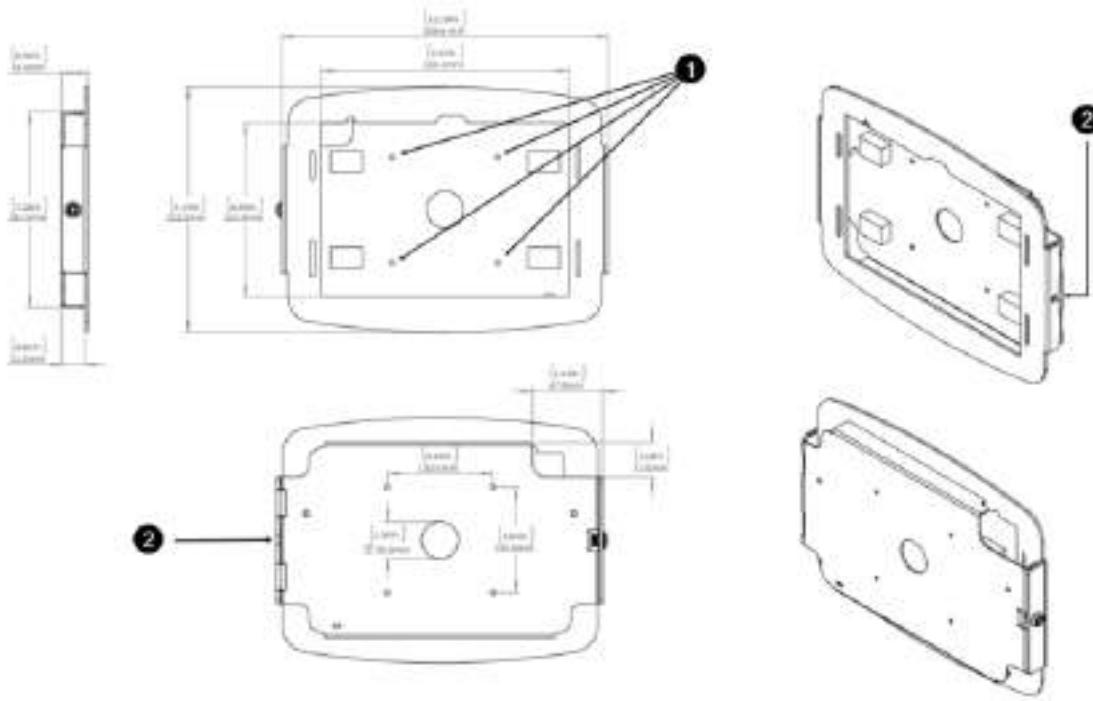
Floor stand features

The floor stand includes the following features:

- Free standing or floor mount option.
- The mount supports any tablet enclosure with a standard VESA mount (100mm x 100mm).
- Tablet power supply can be stored in the base.
- Tablet power cable can be concealed in the legs.
- The enclosure mounting surface can be rotated 90° degrees. This rotation function means that the iPad housing can be orientated on this floor stand for use in either *Portrait* or *Landscape* mode.

iPad enclosure

The following diagram illustrates the floor stand iPad enclosure dimensions.



¹ 4x holes for mounting iPad enclosure to floor stand.

² Opening for power supply cable.

Parent topic: [ClearID Self-Service Kiosk options](#)

Browse

- [ClearID Self-Service Kiosk options](#)
- [About ClearID Self-Service Kiosk](#)

Browse

- [ClearID Self-Service Kiosk Datasheet \(2 pages\)](#)

13.10.2 | ClearID Self-Service Kiosk floor stand printer shelf

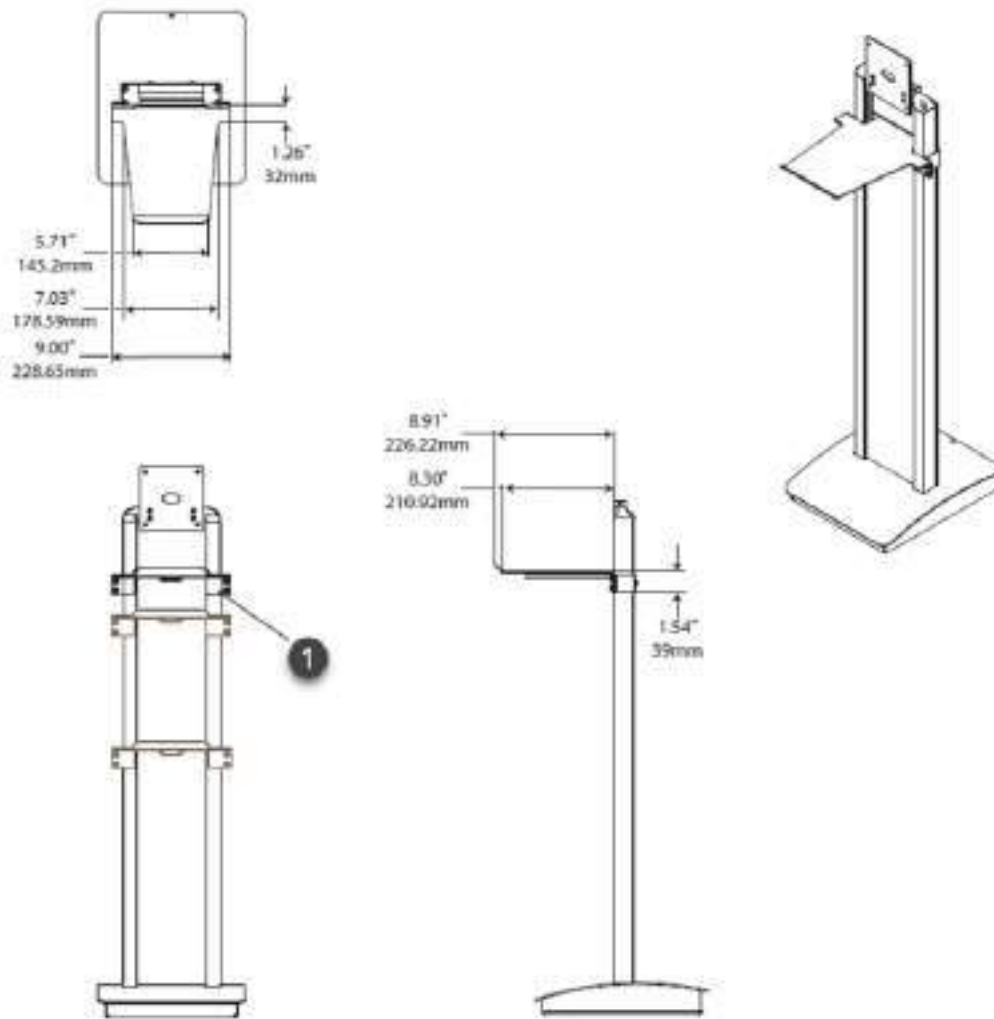
Use the following information to help you understand the dimensions and features of the printer shelf for the Genetec ClearID™ Self-Service Kiosk floor stand.



NOTE: Depending on the size and model of printer that you choose, you might need to trim or modify the center panel (graphic panel) of the floor stand to allow for cable access.

Printer shelf dimensions

The following diagram illustrates the printer shelf dimensions.



¹ Height adjustable printer shelf.

Printer shelf features

The printer shelf includes the following features:

- Mounts to floor stand
- Height adjustable
- Fits various printers

Parent topic: [ClearID Self-Service Kiosk options](#)

Browse

- [ClearID Self-Service Kiosk options](#)
- [About ClearID Self-Service Kiosk](#)

Browse

- [ClearID Self-Service Kiosk Datasheet \(2 pages\)](#)

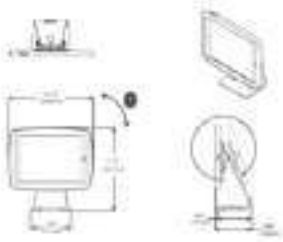
13.10.3 | ClearID Self-Service Kiosk tabletop stand

Use the following information to help you understand the Genetec ClearID™ Self-Service Kiosk tabletop stand dimensions, mounting, and features.



Tabletop stand dimensions

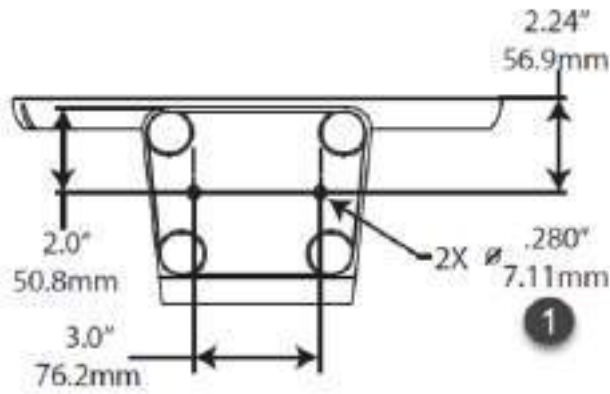
The following diagram illustrates the tabletop stand dimensions including the height and footprint of the stand.



¹ 90° rotation (portrait or landscape orientation).

Tabletop stand mounting

The following diagram illustrates the tabletop mount dimensions.



¹ 2x Tabletop mounting holes for 0.25inch or 6mm screw hardware (not included).

Tabletop stand features

The tabletop stand includes the following features:

- 90° degree rotation (portrait or landscape orientation).
- Flip tablet function.
- Counter mounting option.

Parent topic: [ClearID Self-Service Kiosk options](#)

Browse

- [ClearID Self-Service Kiosk options](#)
- [About ClearID Self-Service Kiosk](#)

Browse

- [ClearID Self-Service Kiosk Datasheet \(2 pages\)](#)

13.11 | Identity document types in ClearID

Use the following information to help you understand all the different identity document types that are supported in Genetec ClearID™ Self-Service Kiosk.

An extensive list of ID types can be used when using the ClearID Self-Service Kiosk during check-in.

NOTE: All identity document processing is performed locally on the ClearID Self-Service Kiosk iPad. This local processing during check-in ensures that ID data or pictures are never sent to the cloud for maximum security and compliance.

Supported identity documents (Asia)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Afghanistan	ID Card	تذکره الکترونیک	Front, back	Latin
Afghanistan	Paper Passport ^{BETA}	پاسپورٹ	Bio-data page	Latin
Armenia	ID Card	Նույնականացման քարտը	Front, back	Latin
Azerbaijan	ID Card	Şəxsiyyət vəsiqəsi	Front, back	Latin
Azerbaijan	Polycarbonate Passport ^{BETA}	Pasport	Bio-data page	Latin
Bangladesh	Driving License ^{BETA}	মোটর ড্রাইভিং লাইসেন্স	Front, back	Latin
Bangladesh	ID Card	জাতীয় পরিচয় পত্র	Front, back	Latin
Bangladesh	Paper Passport	পাসপোর্ট	Bio-data page	Latin
Brunei	ID Card	Kad Pengenalan (Kuning)	Front, back	Latin
Brunei	Military ID ^{BETA}	Kad Pengenalan Tentera (ABDB)	Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Brunei	Residence Permit ^{BETA}	Kad Pengenalan (Ungu)	Front, back	Latin
Brunei	Temporary Residence Permit ^{BETA}	Kad Pengenalan (Hijau)	Front, back	Latin
Cambodia	Driving License ^{BETA}	ប័ណ្ណបើកបរ	Front	Latin
Cambodia	ID Card	អត្តសញ្ញាណប័ណ្ណសញ្ជាតិខ្មែរ	Front	Latin
Cambodia	Polycarbonate Passport	លិខិតឆ្លងដែន	Bio-data page	Latin
China	ID Card	中华人民共和国居民身份证	Front, back	Latin
China	Paper Passport	中华人民共和国护照	Bio-data page	Latin
Hong Kong	ID Card	香港身份證	Front	Latin
Hong Kong	Polycarbonate Passport ^{BETA}	護照	Bio-data page	Latin
India	ID Card ^{BETA}	Aadhaar card, आधार कार्ड	Front, back	Latin
India	PAN Card	स्थायी खाता संख्या कार्ड	Front	Latin
India	Paper Passport		Bio-data page	Latin
India	Voter ID	भारतीय मतदाता पहचान पत्र	Front, vertical	Latin
India, Gujarat	Driving License ^{BETA}	ડ્રાઇવિંગ લાઇસેન્સ	Front	Latin
India, Karnataka	Driving License	ડ્રાઇવિંગ લાઇસેન્સ	Front	Latin
India, Kerala	Driving License ^{BETA}	ਡ્રાઇવિંગ લાઇસેન્સ	Front, back	Latin
India, Madhya Pradesh	Driving License ^{BETA}	ਡ્રાઇવિંગ લાઇસેન્સ	Front	Latin
India, Maharashtra	Driving License	ડ્રાઇવિંગ લાઇસેન્સ	Front	Latin
India, Punjab	Driving License ^{BETA}	ਡ્રਾઇવિંગ ਲਾਇਸੈਂਸ	Front	Latin
India, Tamil Nadu	Driving License ^{BETA}	ਡ્રਾઇવિંગ લાઇસેન્સ	Front, back	Latin
Indonesia	Driving License	Surat Izin Mengemudi (SIM)	Front	Latin
Indonesia	ID Card	Kartu Tanda Penduduk (KTP)	Front	Latin
Indonesia	Paper Passport	Paspor	Bio-data page	Latin
Japan	Driving License ^{BETA}	運転免許	Front	Latin
Japan	My Number Card	マイナンバーカード	Front	Latin
Japan	Paper Passport	旅券	Bio-data page	Latin
Japan	Residence Permit ^{BETA}	在留カード	Front	Latin
Kazakhstan	ID Card	Жеке куәлік, Удостоверение личности	Front, back	Latin
Kyrgyzstan	ID Card	идентификациялык карта, идентификационная карта	Front, back	Latin
Malaysia	Driving License	Lesen Memandu	Front	Latin
Malaysia	MyKAS		Front, back	Latin
Malaysia	MyKad		Front, back	Latin
Malaysia	MyKid		Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Malaysia	MyPR		Front, back	Latin
Malaysia	MyPolis ^{BETA}		Front, back	Latin
Malaysia	MyTentera		Front, back	Latin
Malaysia	Refugee ID	UNHCR Card	Front	Latin
Malaysia	Polycarbonate Passport	Pasport	Bio-data page	Latin
Malaysia	i-Kad		Front	Latin
Maldives	ID Card	ދިވެހިރާއްޖޭގެ ޖުމްހޫރިއްޔާގެ ރައްކާތެރިކަން	Front, back	Latin
Myanmar	Driving License	ယာဉ်မောင်းလိုင်စင်	Front, back	Latin
Nepal	Paper Passport	राहदानी	Bio-data page	Latin
Pakistan	Consular ID	National Identity Card for Overseas Pakistanis (NICOP)	Front, back	Latin
Pakistan	ID Card	Computerized National Identity Card (CNIC), Smart National Identity Card (SNIC)	Front, back	Latin
Pakistan	Paper Passport		Bio-data page	Latin
Pakistan, Punjab	Driving License		Front	Latin
Philippines	Driving License		Front	Latin
Philippines	ID Card	PhilSys ID, PhilID	Front, back	Latin
Philippines	Multipurpose ID	Unified Multi-Purpose ID	Front	Latin
Philippines	Paper Passport		Bio-data page	Latin
Philippines	Professional ID	PRC License	Front	Latin
Philippines	Social Security Card	SSS ID	Front	Latin
Philippines	Tax ID ^{BETA}	TIN ID card	Front	Latin
Philippines	Voter ID ^{BETA}		Front	Latin
Singapore	Driving License		Front, back	Latin
Singapore	Employment Pass		Front	Latin
Singapore	Fin Card		Front	Latin
Singapore	ID Card	NRIC (Pink)	Front, back	Latin
Singapore	Resident ID	NRIC (Blue)	Front, back	Latin
Singapore	Polycarbonate Passport		Bio-data page	Latin
Singapore	S Pass		Front, back	Latin
Singapore	Work Permit		Front, back	Latin
South Korea	Driving License	자동차운전면허증	Front	Latin
South Korea	ID Card ^{BETA}	주민등록증	Front	Latin
South Korea	Paper Passport ^{BETA}	여권	Bio-data page	Latin
Sri Lanka	Driving License	රියද්දිරු බලපත්‍රය	Front	Latin

Genetec ClearID®; User Guide

Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Sri Lanka	ID Card	ජාතික හැඳුනුම්පත, தேசிய அடையாள அட்டை	Front, back, vertical	Latin
Sri Lanka	Paper Passport	ගමන් බලපත්‍රය, கடவுச்சீட்டு	Bio-data page	Latin
Taiwan	ID Card ^{BETA}	中華民國國民身分證	Front	Latin
Taiwan	Temporary Residence Permit ^{BETA}	中華民國居留證 (ARC)	Front	Latin
Latin	Latin	Latin	Latin	Latin
Thailand	Alien ID	บัตรประจำตัวคนซึ่งไม่มีสัญชาติไทย (บัตรสีชมพู)	Front	Latin
Thailand	Driving License ^{BETA}	ใบอนุญาตขับรถ	Front, back	Latin
Thailand	ID Card	บัตรประจำตัวประชาชน	Front, back	Latin
Thailand	Polycarbonate Passport	หนังสือเดินทาง	Bio-data page	Latin
Vietnam	Driving License ^{BETA}	Giấy phép lái xe	Front	Latin
Vietnam	ID Card ^{BETA}	Căn cước công dân, Giấy chứng minh nhân dân	Front, back	Latin

Supported identity documents (Europe)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Albania	Driving License	Leje drejtimi	Front	Latin
Albania	Driver Card	Karta e drejtuesit të mjetit	Front	Latin
Albania	ID Card	Letërnjoftim	Front, back	Latin
Albania	Professional DL	Certifikatë aftësimi profesionale	Front	Latin
Albania	Polycarbonate Passport	Pasaportë	Bio-data page	Latin
Austria	Driving License	Führerschein	Front	Latin
Austria	ID Card	Personalausweis	Front, back	Latin
Austria	Paper Passport	Reisepass	Bio-data page	Latin
Austria	Residence Permit ^{BETA}	Aufenthaltstitel	Front, back	Latin
Belarus	Driving License	ВАДЗІЦЕЛЬСКАЕ ПАСВЕДЧАННЕ, ВОДИТЕЛЬСКОЕ УДОСТОВЕРЕНИЕ	Front	Latin
Belarus	Paper Passport	Пашпарт, Паспорт	Bio-data page	Latin
Belgium	Driving License	Rijbewijs, Permis de conduire, Führerschein	Front	Latin
Belgium	ID Card	Identiteitskaart, Carte d'identité, Personalausweis	Front, back	Latin
Belgium	Minors ID	Kids-ID	Front, back	Latin
Belgium	Paper Passport	Paspoort, Passeport, Reisepass	Bio-data page	Latin
Belgium	Residence Permit	Verblijfstitel, Titre de Séjour	Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Belgium	Resident ID	Document de Sejour, Verblijfsdocument, Aufenthaltsdokument, E Kaart, Carte E, E Karte; E+ Kaart, Carte E+, E+ Karte; F Kaart, Carte F, F Karte; F+ Kaart, Carte F+, F+ Karte	Front, back	Latin
Belgium	Polycarbonate Passport ^{BETA}	Paspoort, Passeport, Reisepass	Bio-data page	Latin
Bosnia and Herzegovina	Driving License	Vozačka dozvola	Front	Latin
Bosnia and Herzegovina	ID Card	Lična karta, Osobna iskaznica	Front, back	Cyrillic, Latin
Bosnia and Herzegovina	Polycarbonate Passport	Pasoš, Пасош, Putovnica	Bio-data page	Latin
Bulgaria	Driving License	Свидетелство за управление на МПС	Front	Cyrillic, Latin
Bulgaria	ID Card	Лична карта	Front, back	Cyrillic, Latin
Bulgaria	Paper Passport	Паспорт	Bio-data page	Latin
Croatia	Driving License	Vozačka dozvola	Front	Latin
Croatia	ID Card	Osobna iskaznica	Front, back	Latin
Croatia	Residence Permit ^{BETA}	Boravišna iskaznica, Dozvola boravka	Front, back	Latin
Croatia	Polycarbonate Passport	Putovnica	Bio-data page	Latin
Cyprus	Driving License	Sürüş ruhsatı, Αάδεια οδήγησης	Front	Latin
Cyprus	ID Card	Kimlik kartı, Δελτίο Ταυτότητας	Front, back	Latin
Cyprus	Paper Passport	Pasaport, Διαβατήριο	Bio-data page	Latin
Cyprus	Residence Permit	ΑΔΕΙΑ ΔΙΑΜΟΝΗΣ	Front, back	Latin
Czechia	Driving License	Řidičský průkaz	Front	Latin
Czechia	ID Card	Občanský průkaz	Front, back	Latin
Czechia	Residence Permit	Povolení k pobytu	Front, back	Latin
Czechia	Polycarbonate Passport	Cestovní pas	Bio-data page	Latin
Denmark	Driving License	Kørekort	Front	Latin
Denmark	Residence Permit ^{beta}	Opholdstilladelse, Opholdskort	Front, back	Latin
Denmark	Polycarbonate Passport	Pas	Bio-data page	Latin
Estonia	Driving License	Juhiluba	Front	Latin
Estonia	ID Card	Isikutunnistus	Front, back	Latin
Estonia	Paper Passport	Pass	Bio-data page	Latin
Estonia	Residence Permit ^{BETA}	Elamisluba	Front, back	Latin
Finland	Alien ID	Ulkomaalaisen henkilökortti, Identitetskort för utlänning	Front, back	Latin
Finland	Driving License	Ajokortti, Körkort	Front	Latin
Finland	ID Card	Henkilökortti, Identitetskort	Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Finland	Residence Permit	Oleskelulupa, Uppehållstillstånd	Front, back	Latin
Finland	Polycarbonate Passport	Passi, Pass	Bio-data page	Latin
France	Driving License	Permis de conduire	Front	Latin
France	ID Card	Carte d'identité	Front, back	Latin
France	Paper Passport ^{BETA}	Passeport	Bio-data page	Latin
France	Residence Permit ^{BETA}	Titre de séjour	Front, back	Latin
Georgia	Driving License	მართვის მოწმობა	Front	Latin
Georgia	ID Card	მოქალაქის პირადობის მოწმობა	Front, back	Latin
Georgia	Paper Passport ^{BETA}	პასპორტი	Bio-data page	Latin
Germany	Driving License	Führerschein	Front	Latin
Germany	ID Card	Personalausweis	Front, back	Latin
Germany	Minors Passport	Kinderreisepass	Bio-data page	Latin
Germany	Paper Passport	Reisepass	Bio-data page	Latin
Germany	Residence Permit	Aufenthaltstitel	Front, back	Latin
Germany	Polycarbonate Passport	Reisepass	Bio-data page	Latin
Greece	Driving License	Αάδεια οδήγησης	Front	Latin
Greece	ID Card	ΔΕΛΤΙΟ ΤΑΥΤΟΤΗΤΑΣ	Front, back	Latin
Greece	Paper Passport	Διαβατήριο	Bio-data page	Latin
Greece	Residence Permit	ΑΔΕΙΑ ΔΙΑΜΟΝΗΣ	Front, back	Latin
Hungary	Address Card ^{BETA}	Lakcímkártya, Lakcímgazolvány	Front, back	Latin
Hungary	Driving License	Vezetői engedély	Front	Latin
Hungary	ID Card	Személyazonosító igazolvány	Front, back	Latin
Hungary	Paper Passport	Útleve	Bio-data page	Latin
Hungary	Residence Permit ^{BETA}	Tartózkodási engedély	Front, back	Latin
Iceland	Driving License ^{BETA}	Ökuskrteini	Front	Latin
Iceland	Paper Passport ^{BETA}	Vegabréf	Bio-data page	Latin
Ireland	Driving License	Ceadúnas tiomána	Front	Latin
Ireland	Passport Card	Cárta Pas	Front, back	Latin
Ireland	Public Services Card	Cárta Seirbhísi Poiblí	Front, back	Latin
Ireland	Residence Permit ^{BETA}		Front, back	Latin
Ireland	Polycarbonate Passport	Pas	Bio-data page	Latin
Italy	Driving License	Patente di guida	Front	Latin
Italy	ID Card	Carta d'identità	Front, back	Latin
Italy	Paper Passport ^{BETA}	Passaporto	Bio-data page	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Italy	Residence Permit	Permesso di soggiorno	Front, back	Latin
Kosovo	Driving License	Patentë shoferi, возачка дозвола	Front	Latin
Kosovo	ID Card	Letërnjoftim, Лична карта	Front, back	Latin
Kosovo	Paper Passport	Pasaportë, Пасош	Bio-data page	Latin
Latvia	Alien ID	Nepilsoņa personas apliecība	Front, back	Latin
Latvia	Driving License	Vadītāja apliecība	Front	Latin
Latvia	ID Card	Personas apliecība	Front, back	Latin
Latvia	Residence Permit ^{BETA}	Uzturēšanās atļauja	Front, back	Latin
Latvia	Polycarbonate Alien Passport	Nepilsoņa pase	Bio-data page	Latin
Latvia	Polycarbonate Passport	Pase	Bio-data page	Latin
Liechtenstein	ID Card	Identitätskarte	Front, back	Latin
Lithuania	Driving License	Vairuotojo pažymėjimai	Front	Latin
Lithuania	ID Card	Asmens tapatybės kortelė	Front, back	Latin
Lithuania	Residence Permit ^{BETA}	Leidimas gyventi	Front, back	Latin
Lithuania	Polycarbonate Passport	Pasas	Bio-data page	Latin
Luxembourg	Driving License	Permis de conduire	Front	Latin
Luxembourg	ID Card	Carte d'Identité, Personalausweis	Front, back	Latin
Luxembourg	Residence Permit	Titre de séjour	Front, back	Latin
Luxembourg	Polycarbonate Passport	Pass, Passeport	Bio-data page	Latin
Malta	Driving License	Liċenzja tas-Sewqan	Front	Latin
Malta	ID Card	Karta tal-Identità	Front, back	Latin
Malta	Residence Permit	Permess ta' residenza, Residence documentation	Front, back	Latin
Moldova	ID Card ^{BETA}	Buletin de identitate	Front, back	Latin
Moldova	Paper Passport ^{BETA}	Pașaport	Bio-data page	Latin
Montenegro	Driving License	Vozačka dozvola, Возачка дозвола	Front	Latin
Montenegro	ID Card	Lična karta, Лична карта	Front, back	Latin
Montenegro	Polycarbonate Passport	Pasoš, Пасош	Bio-data page	Latin
Netherlands	Driving License	Rijbewijs	Front, back	Latin
Netherlands	ID Card	Identiteitskaart (ID-kaart)	Front, back	Latin
Netherlands	Residence Permit	Verblijfstitel, Verblijfskaart	Front, back	Latin
Netherlands	Polycarbonate Passport	Paspoort	Bio-data page	Latin
North Macedonia	Driving License	возачка дозвола, Patentë shoferi	Front	Cyrillic, Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
North Macedonia	ID Card	лична карта, Letërnjoftim	Front, back	Cyrillic, Latin
North Macedonia	Polycarbonate Passport	Пасош, Pasaportë	Bio-data page	Latin
Norway	Driving License	Førerkort, Førarkort	Front	Latin
Norway	ID Card		Front, back	Latin
Norway	Residence Permit	Oppholdstillatelse, Oppholdsløyve	Front, back	Latin
Norway	Polycarbonate Passport	Pass	Bio-data page	Latin
Poland	Driving License	Prawo jazdy	Front	Latin
Poland	ID Card	Dowód osobisty	Front, back	Latin
Poland	Paper Passport	Paszport	Bio-data page	Latin
Poland	Residence Permit ^{BETA}	Karta pobytu	Front, back	Latin
Poland	Polycarbonate Passport	Paszport	Bio-data page	Latin
Portugal	Driving License	Carta de Condução	Front	Latin
Portugal	ID Card	Cartão de Cidadão (CC)	Front, back	Latin
Portugal	Paper Passport	Passaporte	Bio-data page	Latin
Portugal	Residence Permit ^{BETA}	Título de Residência, Cartão de Residência	Front, back	Latin
Romania	Driving License	Permis de conducere	Front	Latin
Romania	ID Card	Carte de identitate	Front	Latin
Romania	Polycarbonate Passport	Pasaport, Pașaport	Bio-data page	Latin
Russia	Driving License	Водительское удостоверение	Front	Latin
Russia	Polycarbonate Passport	(Заграничный) Паспорт	Bio-data page	Latin
Serbia	Driving License	Возачка дозвола, Vozačka dozvola	Front	Latin
Serbia	ID Card	Лична карта, Lična karta	Front, back	Cyrillic, Latin
Serbia	Polycarbonate Passport	Пасош, Pasoš	Bio-data page	Latin
Slovakia	Driving License	Vodičský preukaz	Front	Latin
Slovakia	ID Card	Občiansky preukaz	Front, back	Latin
Slovakia	Residence Permit	Povolenie na pobyt, Pobytový preukaz občana EÚ, Pobytový preukaz rodinného príslušníka občana EÚ	Front, back	Latin
Slovakia	Polycarbonate Passport	Cestovný pas	Bio-data page	Latin
Slovenia	Driving License	Vozniško dovoljenje	Front	Latin
Slovenia	ID Card	Osebná izkaznica	Front, back	Latin
Slovenia	Residence Permit	Dovoljenje za prebivanje	Front, back	Latin

Genetec ClearID®; User Guide

Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Slovenia	Polycarbonate Passport	Potni list	Bio-data page	Latin
Spain	Alien ID	Tarjeta de Identidad de Extranjero (TIE)	Front, back	Latin
Spain	Driving License	Permiso de Conducción	Front	Latin
Spain	ID Card	Documento Nacional de Identidad (DNI)	Front, back	Latin
Spain	Paper Passport	Pasaporte	Bio-data page	Latin
Spain	Residence Permit	Permiso de residencia	Front, back	Latin
Sweden	Driving License	Körkort	Front	Latin
Sweden	ID Card	Nationellt identitetskort	Front, back	Latin
Sweden	Residence Permit	Uppehållstillstånd, Uppehållskort	Front, back	Latin
Sweden	Polycarbonate Passport	Pass	Bio-data page	Latin
Sweden	Social Security Card	Identitetskort, Skatteverkets id-kort	Front	Latin
Switzerland	Driving License	Führerausweis, Permis de conduire, Licenza di condurre, Permiss da manischar	Front	Latin
Switzerland	ID Card	Identitätskarte, Carte d'identité, Carta d'identità, Carta d'identitad	Front, back	Latin
Switzerland	Paper Passport	Pass, Passeport, Passaporto, Passaport	Bio-data page	Latin
Switzerland	Residence Permit	Aufenthaltstitel, Titre de séjour, Permesso di soggiorno, Permissiun da dimora	Front, back	Latin
UK	Driving License	Trwydded yrru	Front	Latin
UK	Paper Passport		Bio-data page	Latin
UK	Proof Of Age Card	CitizenCard	Front	Latin
UK	Residence Permit		Front, back	Latin
UK	Polycarbonate Passport		Bio-data page	Latin
Ukraine	Driving License	Посвідчення водія, Водительское удостоверение	Front	Cyrillic, Latin
Ukraine	ID Card	Паспорт громадянина України	Front, back	Cyrillic, Latin
Ukraine	Residence Permit	Посвідка на постійне проживання (ППП)	Front, back	Cyrillic, Latin
Ukraine	Polycarbonate Passport	Паспорт	Bio-data page	Latin
Ukraine	Temporary Residence Permit	Посвідка на тимчасове проживання	Front, back	Cyrillic, Latin

Supported identity documents (Latin America and the Caribbean)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Antigua and Barbuda	Driving License ^{BETA}		Front	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Argentina	Alien ID	DNI para extranjeros	Front, back	Latin
Argentina	Driving License ^{BETA}	Licencia de Conducir	Front	Latin
Argentina	ID Card	Documento Nacional de Identidad (DNI)	Front, back	Latin
Argentina	Paper Passport	Pasaporte	Bio-data page	Latin
Bahamas	Driving License		Front	Latin
Bahamas	ID Card ^{BETA}	NIB Smart Card	Front	Latin
Barbados	ID Card ^{BETA}		Front, back	Latin
Bolivia	Driving License	Licencia para conducir	Front	Latin
Bolivia	ID Card	Cédula de identidad	Front, back	Latin
Bolivia	Minors ID	Cédula de identidad para menores	Front, back	Latin
Brazil	Consular Passport ^{BETA}	Passaporte	Bio-data page	Latin
Brazil	Driving License	Carteira Nacional de Habilitação (CNH)	Front, back	Latin
Brazil	ID Card ^{BETA}	Cédula de identidade	Front, back	Latin
Brazil	Paper Passport ^{BETA}	Passaporte	Bio-data page	Latin
Brazil, Rio De Janeiro	ID Card	Cédula de identidade	Front, back	Latin
Brazi, Rio Grande do Sul	ID Card ^{BETA}	Cédula de identidade	Front, back	Latin
Brazi, Sao Paulo	ID Card	Cédula de identidade	Front, back	Latin
Cayman Islands	Driving License ^{BETA}	Driver's license	Front	Latin
Chile	Alien ID	Cédula de identidad para extranjeros	Front, back	Latin
Chile	Driving License	Licencia de conducir	Front	Latin
Chile	ID Card	Cédula de Identidad	Front, back	Latin
Chile	Polycarbonate Passport	Pasaporte	Bio-data page	Latin
Columbia	Alien ID	Cédula de Extranjería (CE)	Front, back	Latin
Columbia	Driving License	Licencia de Conducción	Front, back	Latin
Columbia	ID Card	Cédula Digital Colombiana, Cédula de Ciudadanía (CC)	Front, back	Latin
Columbia	Minors ID	Tarjeta de identidad Biométrica (Azul)	Front, back	Latin
Columbia	Polycarbonate Passport	Pasaporte	Bio-data page	Latin
Costa Rica	Driving License ^{BETA}	Licencia de conducir	Front	Latin
Costa Rica	ID Card	Cédula de identidad	Front, back	Latin
Cuba	ID Card ^{BETA}	Carné de Identidad	Front, back	Latin
Cuba	Paper Passport	Pasaporte	Bio-data page	Latin
Dominican Republic	Driving License ^{BETA}	Licencia de conducir	Front, back	Latin
Dominican Republic	ID Card	Cédula de Identidad y Electoral (CIE)	Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Dominican Republic	Paper Passport	Pasaporte	Bio-data page	Latin
Ecuador	Driving License	Licencia de conducir	Front	Latin
Ecuador	ID Card	Cédula de Identidad, Cédula de Identidad Electrónica	Front, back	Latin
El Salvador	Driving License ^{BETA}	Licencia de conducir	Front, back	Latin
El Salvador	ID Card	Documento Único de Identidad (DUI)	Front, back	Latin
Guatemala	Consular ID	Tarjeta de Identificación Consular (TICG)	Front, back	Latin
Guatemala	Driving License	Licencia de conducir	Front, back	Latin
Guatemala	ID Card	Documento Personal de Identificación (DPI)	Front, back	Latin
Guatemala	Paper Passport	Pasaporte	Bio-data page	Latin
Haiti	Driving License	Permis de conduire	Front	Latin
Haiti	ID Card	Carte d'identification nationale (CIN), Kat Idantifikasyon Nasyonal	Front, back	Latin
Haiti	Paper Passport	Passeport, Paspò	Bio-data page	Latin
Honduras	Driving License ^{BETA}	Licencia de conducir	Front, back	Latin
Honduras	ID Card ^{BETA}	Tarjeta de identidad	Front, back	Latin
Honduras	Paper Passport ^{BETA}	Pasaporte	Bio-data page	Latin
Jamaica	Driving License	Motor vehicle license, MV license	Front, back	Latin
Mexico	Consular ID ^{BETA}	Matrícula consular	Front, back	Latin
Mexico	Paper Passport ^{BETA}	Pasaporte	Bio-data page	Latin
Mexico	Professional DL ^{BETA}	Licencia Federal de Conductor	Front	Latin
Mexico	Professional ID ^{BETA}	Cédula Profesional	Front, back, vertical	Latin
Mexico	Residence Permit ^{beta}	Tarjeta de Residencia Temporal y Residencia Permanente	Front, back	Latin
Mexico	Polycarbonate Passport	Pasaporte	Bio-data page	Latin
Mexico	Voter ID	Credencial para votar	Front, back	Latin
Mexico, Aguascalientes	Driving License	Licencia de Conducir	Front, back, vertical	Latin
Mexico, Baja California	Driving License	Licencia de Conducir	Front, back, vertical	Latin
Mexico, Baja California Sur	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Campeche	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Chiapas	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Chihuahua	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Ciudad de Mexico	Driving License	Licencia de Conducir	Front, vertical	Latin
Mexico, Coahuila	Driving License	Licencia de Conducir	Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Mexico, Colima	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Durango	Driving License	Licencia de Conducir	Front	Latin
Mexico, Guanajuato	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Guerrero Cocula	Driving License ^{BETA}	Licencia de Conducir	Front, back	
Mexico, Guerrero Juchitan	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Hidalgo	Driving License	Licencia de Conducir	Front, back, vertical	Latin
Mexico, Jalisco	Driving License	Licencia de Conducir	Front	Latin
Mexico, Mexico	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Michoacan	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Morelos	Driving License	Licencia de Conducir	Front	Latin
Mexico, Nayarit	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Nuevo Leon	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Oaxaca	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Puebla	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Quintana Roo Cozumel	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Quintana Roo Solidaridad	Driving License	Licencia de Conducir	Front, back, vertical,	Latin
Mexico, San Luis Potosi	Driving License	Licencia de Conducir	Front	Latin
Mexico, Sinaloa	Driving License ^{BETA}	Licencia de Conducir	Front	Latin
Mexico, Sonora	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Tabasco	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Tamaulipas	Driving License	Licencia de Conducir	Front, back, vertical,	Latin
Mexico, Tlaxcala	Driving License	Licencia de Conducir	Front, back	Latin
Mexico, Veracruz	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Yucatan	Driving License ^{BETA}	Licencia de Conducir	Front, back	Latin
Mexico, Zacatecas	Driving License	Licencia de Conducir	Front, back	Latin
Nicaragua	ID Card	Cédula de Identidad Ciudadana	Front, back	Latin
Panama	Driving License	Licencia de Conducir	Front	Latin
Panama	ID Card	Cédula de Identidad	Front	Latin
Panama	Residence Permit	Carné de Residente Permanente	Front	Latin
Panama	Temporary Residence Permit	Carné de Residencia Provisional	Front, back	Latin
Paraguay	Driving License	Licencia de Conducir	Front, back	Latin
Paraguay	ID Card	Cédula de Identidad Civil	Front, back	Latin
Peru	Driving License	Licencia de conducir	Front, back	Latin

Genetec ClearID®; User Guide

Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Peru	ID Card	Documento Nacional de Identidad (DNI)	Front, back	Latin
Peru	Minors ID ^{BETA}	Documento Nacional de Identidad (DNI) para menores	Front, back	Latin
Peru	Paper Passport	Pasaporte	Bio-data page	Latin
Puerto Rico	Driving License	Licencia de Conducir	Front	Latin
Puerto Rico	Voter ID ^{BETA}	Tarjeta de Identificación Electoral (TIE), Electoral Identification Card	Front	Latin
Saint Lucia	ID Card ^{BETA}		Front, back	Latin
Trinidad and Tobago	Driving License		Front	Latin
Trinidad and Tobago	ID Card		Front, back	Latin
Uruguay	ID Card	Cédula de Identidad	Front, back	Latin
Venezuela	Driving License	Licencia para conducir	Front	Latin
Venezuela	ID Card	Cédula de Identidad	Front	Latin
Venezuela	Polycarbonate Passport	Pasaporte	Bio-data page	Latin

Supported identity documents (Middle East and Africa)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Algeria	Driving License	رخصة القيادة	Front, back	Latin
Algeria	ID Card	Carte nationale d'identité, بطاقة الهوية الوطني	Front, back	Latin
Algeria	Paper Passport	جواز السفر, Passeport	Bio-data page	Latin
Bahrain	ID Card	بطاقة الهوية, CPR Card	Front, back	Latin
Botswana	ID Card	Omang	Front, back	Latin
Burkina Faso	ID Card	Carte Nationale d'Identité Burkinabè (CNIB)	Front, back	Latin
Cameroon	ID Card	Carte Nationale d'Identité (CNI)	Front, back	Latin
Democratic Republic of the Congo	Driving License ^{BETA}	Permis de conduire (CONADEP)	Front, back	Latin
Egypt	Driving License ^{BETA}	رخصة القيادة	Front, back	Latin
Egypt	ID Card	بطاقة تحقيق الشخصية	Front, back	Arabic, Latin
Egypt	Paper Passport ^{BETA}	جواز سفر	Bio-data page	Latin
Eswatini	Paper Passport		Bio-data page	Latin
Ghana	Driving License		Front	Latin
Ghana	ID Card	Ghana Card	Front, back	Latin
Ghana	Paper Passport		Bio-data page	Latin
Iran	Paper Passport ^{BETA}	گذرنامه	Bio-data page	Latin
Iraq	ID Card	البطاقة الوطنية, كارتى نيشتمانى	Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Iraq	Paper Passport ^{BETA}	پاسپورت, جواز سفر	Bio-data page	Latin
Israel	Driving License	רשיון נהיגה	Front	Latin
Israel	ID Card	Tehudat Zehut, بطاقة هوية, תעודת זהות	Front, back	Latin
Israel	Paper Passport ^{BETA}	דרכון	Bio-data page	Latin
Ivory Coast	Driving License	Permis de conduire	Front	Latin
Ivory Coast	ID Card	Carte Nationale d'Identité (CNI)	Front, back	Latin
Jordan	Driving License ^{BETA}	رخصة القيادة	Front	Latin
Jordan	ID Card	بطاقة شخصية	Front, back	Arabic, Latin
Jordan	Paper Passport ^{BETA}	جواز سفر	Bio-data page	Latin
Kenya	ID Card	Kitambulisho	Front, back	Latin
Kenya	Polycarbonate Passport	Passport, Pasi	Bio-data page	Latin
Kuwait	Driving License	رخصة القيادة	Front, back	Latin
Kuwait	ID Card	بطاقة المدنية	Front, back	Latin
Kuwait	Resident ID	بطاقة المدنية	Front, back	Latin
Lebanon	ID Card	بطاقة الهوية	Front, back	Latin
Libya	Polycarbonate Passport	جواز سفر	Bio-data page	Latin
Mauritius	ID Card		Front, back	Latin
Morocco	Driving License	Permis de conduire, رخصة القيادة	Front, back	Latin
Morocco	ID Card	Carte nationale d'identité, بطاقة التعريف الوطنية	Front, back	Latin
Morocco	Paper Passport ^{BETA}	Passeport, جواز سفر	Bio-data page	Latin
Mozambique	Driving License ^{BETA}	Carta de Condução	Front	Latin
Mozambique	ID Card	Bilhete de Identidade (BI)	Front, back	Latin
Nigeria	Driving License		Front, back	Latin
Nigeria	ID Card	e-ID card	Front, back	Latin
Nigeria	Paper Passport		Bio-data page	Latin
Nigeria	Polycarbonate Passport ^{BETA}		Bio-data page	Latin
Nigeria	Voter ID	Permanent Voter Card (PVC)	Front, back	Latin
Oman	Driving License ^{BETA}	رخصة قيادة مركبة	Front, back	Latin
Oman	ID Card	بطاقة الهوية	Front, back	Latin
Oman	Resident ID	بطاقة مقيم	Front, back	Latin
Qatar	Driving License	رخصة القيادة	Front	Latin
Qatar	ID Card ^{BETA}	بطاقة إثبات شخصية	Front	Latin
Qatar	Paper Passport	جواز سفر	Bio-data page	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Qatar	Residence Permit	تصريح الإقامة	Front, back	Latin
Rwanda	ID Card	Indangamuntu	Front	Latin
Saudi Arabia	Driving License	رخصة قيادة	Front	Latin
Saudi Arabia	ID Card	بطاقة الأحوال المدنية	Front, back	Latin
Saudi Arabia	Paper Passport	جواز سفر	Bio-data page	Latin
Saudi Arabia	Resident ID	هوية المقيم, Iqama	Front	Latin
Senegal	ID Card	Carte d'identité biométrique CEDEAO, Carte nationale d'identité	Front, back	Latin
South Africa	Driving License	Bestuurslisensie	Front	Latin
South Africa	ID Card	Smart ID card	Front, back	Latin
South Africa	ID Card ^{BETA}	Green barcoded ID book	Front, vertical	Latin
South Africa	Polycarbonate Passport	Passeport	Bio-data page	Latin
Sudan	Polycarbonate Passport	جواز سفر	Bio-data page	Latin
Syria	Paper Passport	جواز سفر	Bio-data page	Latin
Tanzania	Driving License	Leseni ya udereva	Front	Latin
Tanzania	ID Card ^{BETA}	Kitambulisho cha Taifa, NIDA	Front, back	Latin
Tanzania	Voter ID ^{BETA}	Kadi ya mpiga kura, Voter Card	Front	Latin
Togo	ID Card	Permis de conduire	Front, back	Latin
Tunisia	Driving License	رخصة قيادة	Front	Latin
Tunisia	ID Card	بطاقة التعريف الوطنية	Front	Latin
Tunisia	Paper Passport	جواز سفر	Bio-data page	Latin
Turkey	Driving License	Sürücü belgesi	Front	Latin
Turkey	ID Card	Kimlik Kartı	Front, back	Latin
Turkey	Paper Passport	Pasaport	Bio-data page	Latin
Turkey	Residence Permit ^{BETA}	İkamet izni	Front, back	Latin
Turkey	Polycarbonate Passport	Pasaport	Bio-data page	Latin
UAE	Driving License	رخصة القيادة	Front, back	Latin
UAE	ID Card	بطاقة الهوية	Front, back	Arabic, Latin
UAE	Paper Passport	جواز سفر	Bio-data page	Arabic, Latin
UAE	Resident ID	بطاقة الهوية الوطنية	Front, back	Arabic, Latin
Uganda	Driving License		Front	Latin
Uganda	ID Card		Front, back	Latin
Zimbabwe	ID Card	National registration card (NRC)	Front, back	Latin
Zimbabwe	Paper Passport		Bio-data page	Latin

Supported identity documents (North America)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Bermuda	Driving License ^{BETA}		Front	Latin
Canada	Citizenship Certificate ^{BETA}	Canada citizenship card, Carte de citoyenneté canadienne	Front, back	Latin
Canada	Paper Passport	Passport, Passeport	Bio-data page	Latin
Canada	Residence Permit	Permanent residence (PR) card, Carte de résident permanent	Front, back	Latin
Canada	Social Security Card ^{BETA}	Social insurance card (SIN card), Carte d'assurance sociale (Carte de NAS)	Front	Latin
Canada	Tribal ID	Certificate of Indian Status, Certificat de statut Indien	Front, back	Latin
Canada	Weapon Permit	Possession and Aquisition License (PAL), Permis de possession et d'acquisition	Front	Latin
Canada, Alberta	Driving License		Front, back	Latin
Canada, Alberta	ID Card		Front, back	Latin
Canada, British Columbia	Driving License		Front, back	Latin
Canada, British Columbia	Driver License, Public Services Card (Combined)		Front, back	Latin
Canada, British Columbia	ID Card		Front, back	Latin
Canada, British Columbia	Minors Public Services Card		Front, back	Latin
Canada, British Columbia	Public Services Card		Front, back	Latin
Canada Manitoba	Driving License		Front, back	Latin
Canada Manitoba	ID Card		Front, back	Latin
Canada, New Brunswick	Driving License	Permis de conduire	Front, back	Latin
Canada, Newfoundland and Labrador	Driving License		Front, back	Latin
Canada, Nova Scotia	Driving License		Front, back	Latin
Canada, Nova Scotia	ID Card ^{BETA}		Front, back	Latin
Canada, Nova Scotia	Driving License		Front, back	Latin
Canada, Nova Scotia	ID Card ^{BETA}		Front, back	Latin
Canada, Ontario	Driving License		Front, back	Latin
Canada, Ontario	ID Card	Photo card	Front, back	Latin
Canada, Quebec	Driving License	Permis de conduire	Front, back	Latin
Canada, Saskatchewan	Driving License		Front, back	Latin
Canada, Saskatchewan	ID Card ^{BETA}		Front, back	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Canada, Yukon	Driving License	Permis de conduire	Front, back	Latin
USA	Border Crossing Card	BCC	Front, back	Latin
USA	Global Entry Card		Front, back	Latin
USA	Green Card	Permanent resident card	Front, back	Latin
USA	Military ID	Common Access Card (CAC)	Front, back, vertical	Latin
USA	Nexus Card ^{BETA}		Front, back	Latin
USA	Paper Passport		Bio-data page	Latin
USA	Passport Card		Front, back	Latin
USA	Polycarbonate Passport		Bio-data page	Latin
USA	Social Security Card ^{BETA}		Front	Latin
USA	Veteran ID	VIC	Front	Latin
USA	Work Permit	Employment authorization document, EAD Card	Front, back	Latin
USA, Alabama	Driving License		Front, back, vertical	Latin
USA, Alabama	ID Card		Front, back, vertical	Latin
USA, Alaska	Driving License		Front, back	Latin
USA, Alaska	ID Card		Front, back	Latin
USA, Arizona	Driving License		Front, back, vertical	Latin
USA, Arizona	ID Card		Front, back, vertical	Latin
USA, Arkansas	Driving License		Front, back, vertical	Latin
USA, Arkansas	ID Card		Front, back, vertical	Latin
USA, California	Driving License		Front, back, vertical	Latin
USA, California	ID Card		Front, back, vertical	Latin
USA, Colorado	Driving License		Front, back, vertical	Latin
USA, Colorado	ID Card		Front, back	Latin
USA, Connecticut	Driving License		Front, back, vertical	Latin
USA, Connecticut	ID Card		Front, back	Latin
USA, Delaware	Driving License		Front, back, vertical	Latin
USA, District of Columbia	Driving License		Front, back, vertical	Latin
USA, District of Columbia	ID Card		Front, back, vertical	Latin
USA, Florida	Driving License		Front, back, vertical	Latin
USA, Florida	ID Card		Front, back, vertical	Latin
USA, Georgia	Driving License		Front, back, vertical	Latin
USA, Georgia	ID Card		Front, back, vertical	Latin
USA, Hawaii	Driving License		Front, back, vertical	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
USA, Hawaii	ID Card		Front, back	Latin
USA, Idaho	Driving License		Front, back, vertical	Latin
USA, Idaho	ID Card		Front, back	Latin
USA, Illinois	Driving License		Front, back, vertical	Latin
USA, Illinois	ID Card		Front, back, vertical	Latin
USA, Indiana	Driving License		Front, back	Latin
USA, Indiana	ID Card		Front, back	Latin
USA, Iowa	Driving License		Front, back, vertical	Latin
USA, Iowa	ID Card		Front, back, vertical	Latin
USA, Kansas	Driving License		Front, back, vertical	Latin
USA, Kansas	ID Card		Front, back, vertical	Latin
USA, Kentucky	Driving License		Front, back, vertical	Latin
USA, Kentucky	ID Card		Front, back, vertical	Latin
USA, Louisiana	Driving License		Front, back	Latin
USA, Maine	Driving License		Front, back, vertical	Latin
USA, Maine	ID Card		Front, back	Latin
USA, Maryland	Driving License		Front, back, vertical	Latin
USA, Maryland	ID Card		Front, back, vertical	Latin
USA, Massachusetts	Driving License		Front, back, vertical	Latin
USA, Massachusetts	ID Card		Front, back, vertical	Latin
USA, Michigan	Driving License		Front, back, vertical	Latin
USA, Michigan	ID Card		Front, back, vertical	Latin
USA, Minnesota	Driving License		Front, back, vertical	Latin
USA, Minnesota	ID Card		Front, back, vertical	Latin
USA, Missouri	Driving License		Front, back, vertical	Latin
USA, Missouri	ID Card		Front, back, vertical	Latin
USA, Montana	Driving License		Front, back	Latin
USA, Montana	ID Card		Front, back	Latin
USA, Nebraska	Driving License		Front, back, vertical	Latin
USA, Nebraska	ID Card		Front, back	Latin
USA, Nevada	Driving License		Front, back, vertical	Latin
USA, Nevada	ID Card		Front, back, vertical	Latin
USA, New Hampshire	Driving License		Front, back, vertical	Latin
USA, New Hampshire	ID Card ^{BETA}		Front, back	Latin
USA, New Jersey	Driving License		Front, back, vertical	Latin
USA, New Jersey	ID Card		Front, back, vertical	Latin

Genetec ClearID®; User Guide
Displayed in the header

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
USA, New Mexico	Driving License		Front, back, vertical	Latin
USA, New Mexico	ID Card		Front, back	Latin
USA, New York	Driving License		Front, back, vertical	Latin
USA, New York	ID Card		Front, back, vertical	Latin
USA, New York City	ID Card		Front, back	Latin
USA, North Carolina	Driving License		Front, back, vertical	Latin
USA, North Carolina	ID Card		Front, back, vertical	Latin
USA, North Dakota	Driving License		Front, back, vertical	Latin
USA, North Dakota	ID Card ^{BETA}		Front, back	Latin
USA, Ohio	Driving License		Front, back, vertical	Latin
USA, Ohio	ID Card		Front, back, vertical	Latin
USA, Oklahoma	Driving License		Front, back, vertical	Latin
USA, Oklahoma	ID Card		Front, back, vertical	Latin
USA, Oregon	Driving License		Front, back, vertical	Latin
USA, Oregon	ID Card		Front, back	Latin
USA, Pennsylvania	Driving License		Front, back, vertical	Latin
USA, Pennsylvania	ID Card		Front, back, vertical	Latin
USA, Rhode Island	Driving License		Front, back, vertical	Latin
USA, Rhode Island	ID Card		Front, back	Latin
USA, South Carolina	Driving License		Front, back, vertical	Latin
USA, South Carolina	ID Card		Front, back, vertical	Latin
USA, South Dakota	Driving License		Front, back, vertical	Latin
USA, South Dakota	ID Card ^{BETA}		Front, back	Latin
USA Tennessee	Driving License		Front, back, vertical	Latin
USA Tennessee	ID Card		Front, back, vertical	Latin
USA, Texas	Driving License		Front, back, vertical	Latin
USA, Texas	ID Card		Front, back, vertical	Latin
USA, Texas	Weapon Permit	License to Carry a Handgun (LTC)	Front	Latin
USA, Utah	Driving License		Front, back, vertical	Latin
USA, Utah	ID Card		Front, back, vertical	Latin
USA, Vermont	Driving License		Front, back	Latin
USA, Virginia	Driving License		Front, back, vertical	Latin
USA, Virginia	ID Card		Front, back	Latin
USA, Washington	Driving License		Front, back, vertical	Latin
USA, Washington	ID Card		Front, back, vertical	Latin
USA, West Virginia	Driving License		Front, back	Latin

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
USA, Wisconsin	Driving License		Front, back, vertical	Latin
USA, Wisconsin	ID Card		Front, back	Latin
USA, Wyoming	Driving License		Front, back	Latin
USA, Wyoming	ID Card		Front, back	Latin

Supported identity documents (Oceania)

Country or Region	Document Type	Localized Document Name	Supported side and orientation	Supported scripts
Australia	Paper Passport		Bio-data page	Latin
Australia, Australian Capital Territory	Driving License		Front	Latin
Australia, New South Wales	Driving License		Front	Latin
Australia, New South Wales	ID Card		Front	Latin
Australia, Northern Territory	Driving License ^{BETA}		Front, back	Latin
Australia, Northern Territory	Proof Of Age Card	NT Evidence of age card	Front, back	Latin
Australia, Queensland	Driving License		Front, back	Latin
Australia, South Australia	Driving License		Front, back	Latin
Australia, South Australia	Proof Of Age Card		Front	Latin
Australia, Tasmania	Driving License		Front, back	Latin
Australia, Victoria	Driving License		Front, back	Latin
Australia, Victoria	Proof Of Age Card		Front	Latin
Australia, Western Australia	Driving License		Front, back	Latin
New Zealand	Driving License		Front	Latin
New Zealand	Polycarbonate Passport	Uruwhenua	Bio-data page	Latin

Browse

- [About ClearID Self-Service Kiosk](#)

14 | Troubleshooting

14.1 | Plugin installed, but missing from Security Desk and Config Tool

If the Properties tab for the plugin is missing, then the plugin is not installed on your local machine. The plugin must be installed on a Genetec™ Server (main or expansion).

To help you troubleshoot this issue, refer to the possible causes and their respective solutions below.

Possible symptoms:

- In Config Tool, you see the plugin in the Plugins task, and you can add a new plugin role, but the new role is missing the Properties tab.
- In Security Desk, the plugin does not appear on the Options page.

Genetec ClearID™ User Guide Displayed in the header

Description of cause: The plugin is not installed on the local computer, the license (certificate) is invalid, or you are missing required user privileges.

Solution 1: Install the plugin on your local computer.

Solution 2: Make sure that a Genetec™ Server has the plugin installed, the role created, and is configured correctly.

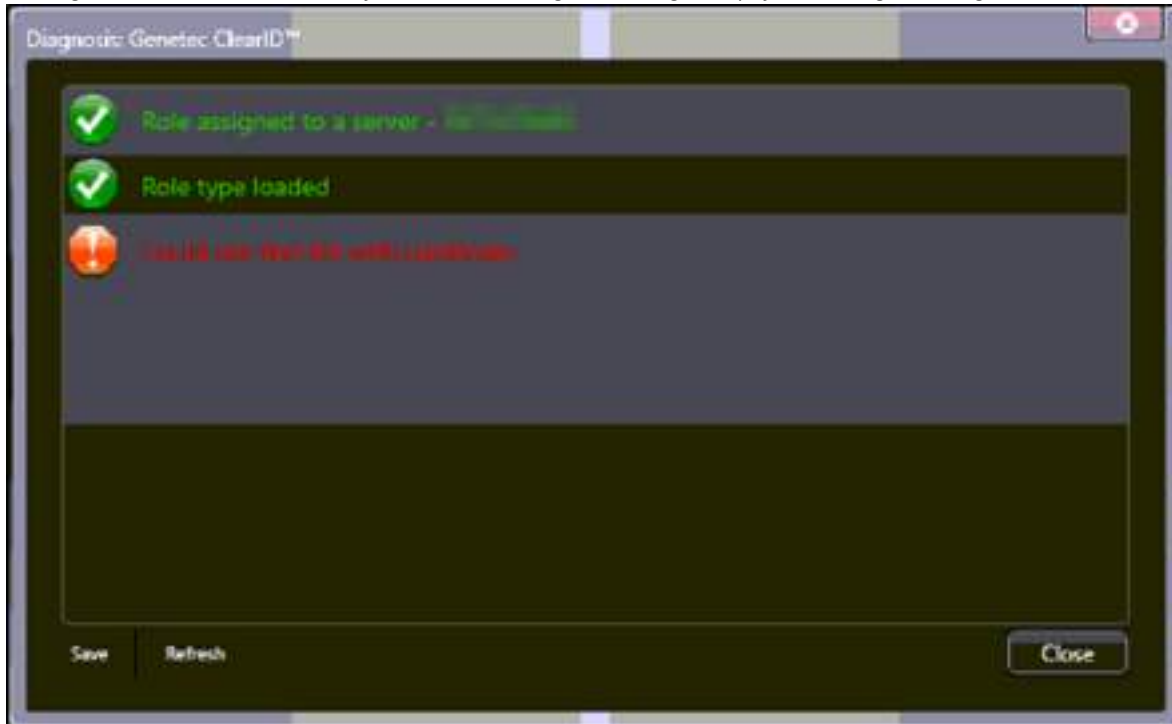
Solution 3: Confirm that the plugin is installed on your Security Center computer: from the homepage in Security Desk or Config Tool, click About > Installed components and look in the list for the entry Genetec.Iams.SCPlugin.Client.

Solution 4: Confirm that your system has a license (certificate) for the plugin: from the homepage in Security Desk or Config Tool, click About > Certificates, look in the list for the name of the plugin, and make sure that your access permissions are set to Unlimited or a number representing the number of licenses.

14.2 | Plugin role could not find file with certificate

When adding the Genetec ClearID™ plugin role, the role is unable to start and a Could not find file with certificate error message is displayed.

In Config Tool, in the Roles section of the System task the following error message is displayed in the diagnosis dialog.



Cause

The CD-SC-PLUGIN license is missing for that system (GSC does not have the ClearID license part).

Solution

Make sure that the plugin role is correctly configured with the required license part.

1. In Config Tool, click About > Certificates and look for ClearID.
2. If the ClearID certificate is not found, add the CD-SC-PLUGIN part to the license, apply the license to the system, and restart the system.

14.3 | Custom fields not displayed in Security Desk

If custom fields are not displayed in Security Desk, check the user privileges and ensure that the relevant user or user groups have been configured for the custom field.

To troubleshoot the issue, learn about the possible causes and their respective solutions.

Incorrect user privileges

Description of cause: A custom field is not displayed because the user lacks the required privileges.

Solution: Add the required privileges.

1. From the Config Tool homepage, open the User management task.

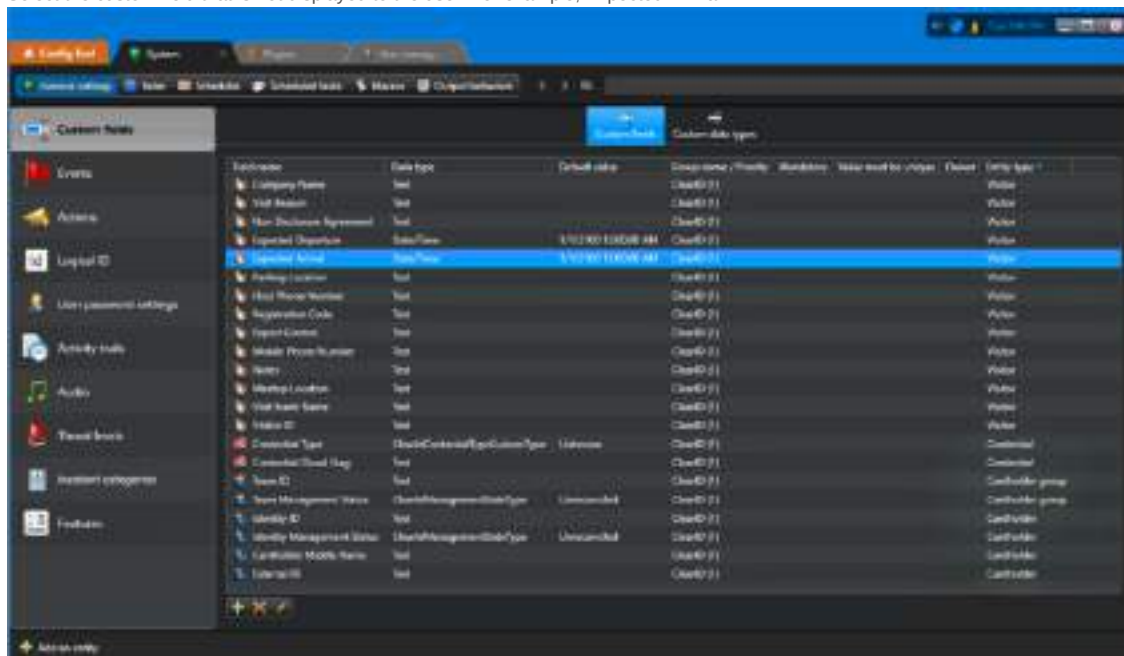
2. Select the relevant user, and click the Privileges tab.
3. Set the following privileges to Allow:
 - Application privileges > Security Desk
 - Application privileges > Config Tool
 - Administrative privileges > System management > View role properties
 - Administrative privileges > System management > View server properties
 - Task privileges > Administration > Plugins
4. (Optional) Set the custom field privileges that you require to Allow.
 - Administrative privileges > Access control management > View cardholder group properties > Modify cardholder group properties > Modify custom fields
 - Administrative privileges > Access control management > View cardholder properties > Modify cardholder properties > Modify custom fields
 - Administrative privileges > Access control management > View credential properties > Modify credential properties > Modify custom fields
 - Administrative privileges > Access control management > View visitor properties > Modify visitor properties > Modify custom fields
 - Administrative privileges > System management > View general settings > Modify custom field definitions
5. Click Apply.

Custom field not configured for user or user group

Description of cause: The custom field has not been configured to display to the user or user group.

Solution: Configure the custom field to display to the user or user group.

1. From the Config Tool homepage, open the System task.
2. Click General settings > Custom Fields.
3. Select the custom field that is not displayed to the user. For example, Expected Arrival.



4. Click Edit the item (✎) to modify the custom field settings.
5. In the Security section of the Edit custom field dialog box, click Add an item (+).
6. Navigate to and select a user or user group from the list and click OK.

In the following example, we configured the *Expected Arrival* custom field so that it is visible to the *Genetec Receptionists* user group.

Edit custom field

Definition

Entity type: Visitor

Data type: Date/Time

Name: Expected Arrival

Default value: 01 / 01 / 2100 12 : 00 : 00 AM

Layout (Optional)

Group name: ClearID

Priority: 1

Security

Visible to administrators and

Genetec Receptionists

+ X

Cancel Save and close

7. Click Save and close then click Apply.

Browse

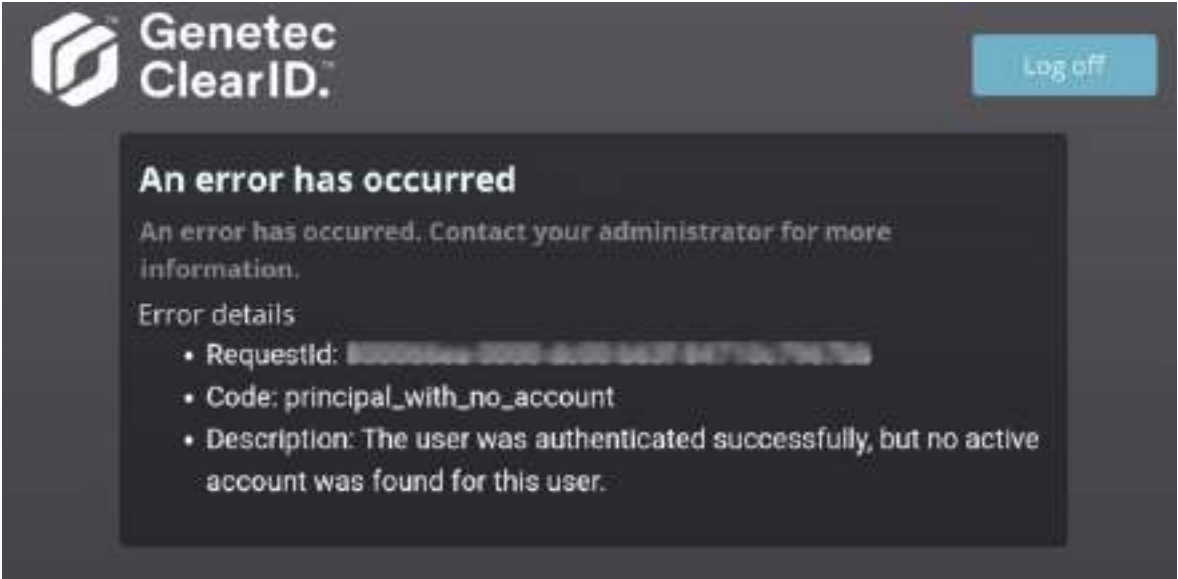
- Granting user privileges for the ClearID plugin
- About custom fields in ClearID

14.4 | No active account found for user

If no active account was found for the user during single sign-on (SSO) logon, use another identity or grant access to the Genetec ClearID™ web portal.

Cause

The user was authenticated successfully, but no active account was found for the user.



The identity associated with the email that was used to log on does not have web portal access.

Solution

Grant user access to the web portal.

14.5 | Visit email notifications not received by visitors

If visitors aren't receiving email notifications, check that the visit event or visit area request has been approved.

To troubleshoot the issue, learn about the possible causes and their respective solutions.

Cause

Visit email notifications aren't received because the visit event or visit area request wasn't approved.

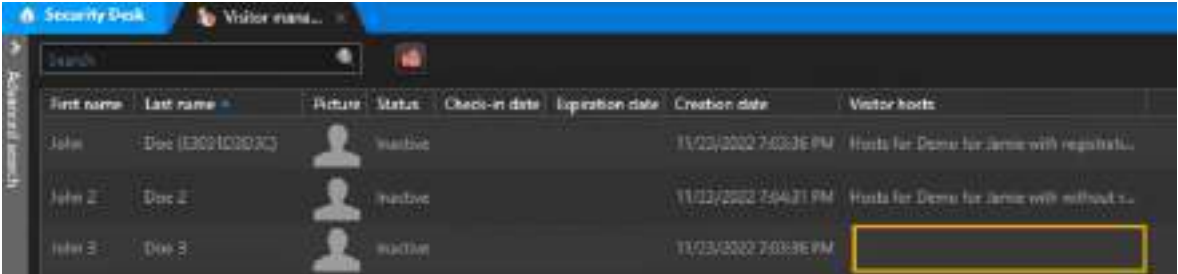
Solution

Review any visit event or visit area requests to identify the request waiting for approval:

- 1. Approve area access requests.
- 2. Approve visit events.

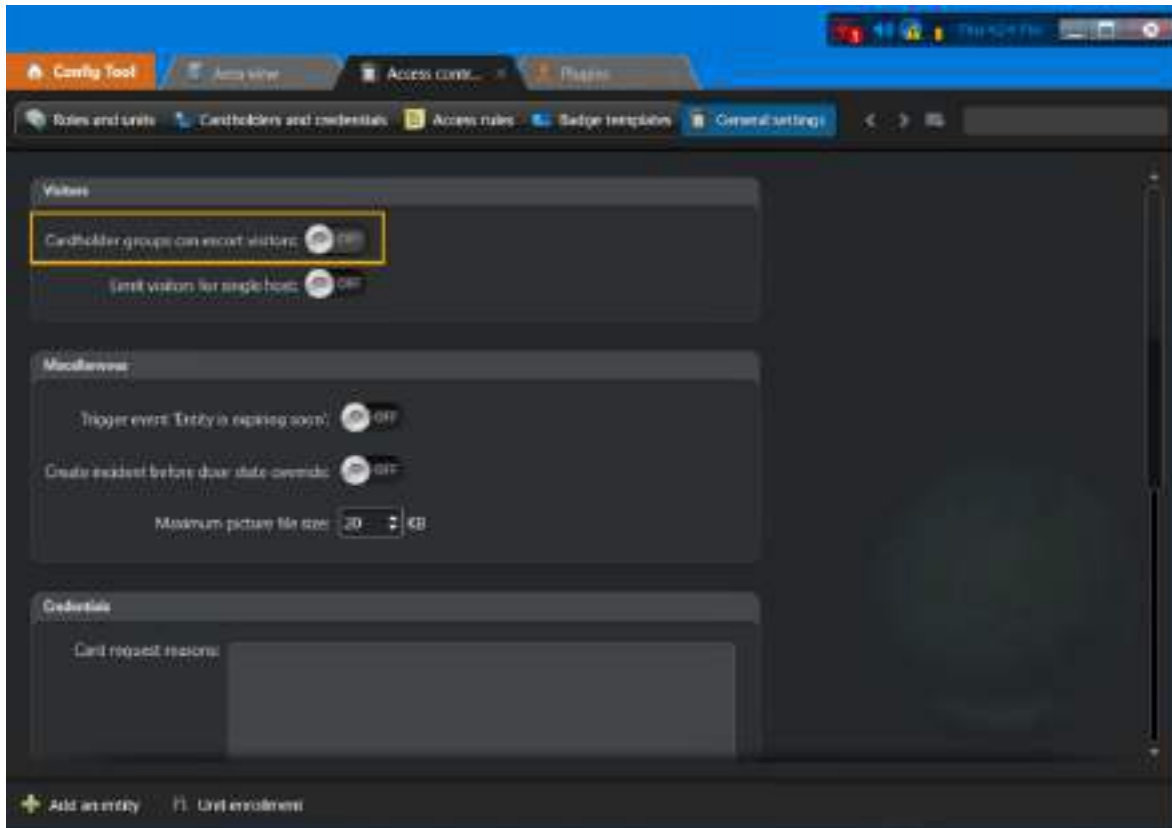
14.6 | Visitor hosts fields in Security Desk are empty

If the Visitor hosts fields in Security Desk are empty, then the Cardholder groups can escort visitors setting might not be configured correctly for Genetec ClearID™.



Cause

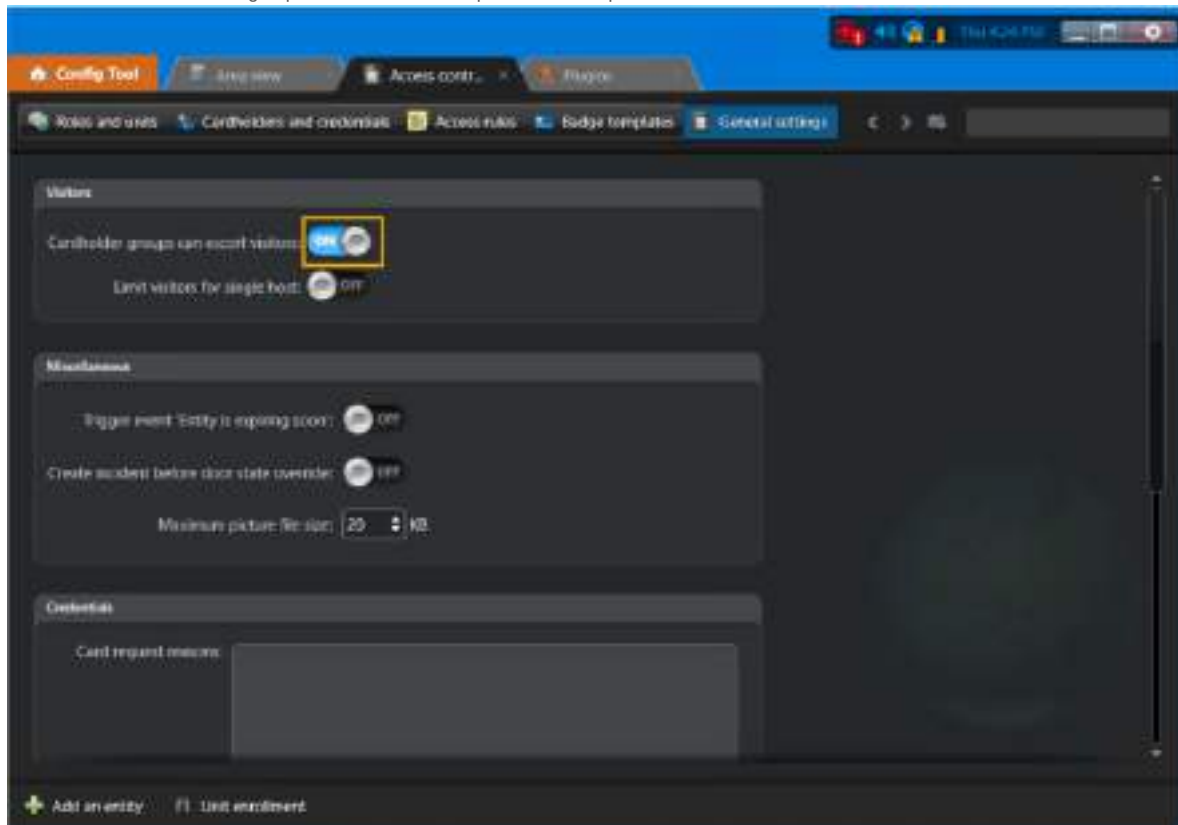
In the Visitors section of the Access control task, the Cardholder groups can escort visitors setting in Config Tool could be disabled (OFF).



Solution

In the Visitors section of the Access control task, make sure that the Cardholder groups can escort visitors setting is enabled (ON).

1. From the Config Tool homepage, open the Access control task.
2. Click General settings.
3. Click or slide the Cardholder groups can escort visitors option to the ON position.



4. (Optional) In ClearID, create a new visit request to verify that the option is working as expected.
5. (Optional) In Security Desk, check that the Visitor hosts field contains host information.

14.7 | ClearID One Identity Synchronization Tool connectivity issues

If you encounter connectivity issues when using the Genetec ClearID™ One Identity Synchronization Tool, check your API integration or Azure AD application connection details.

To help you troubleshoot the issue, learn about the possible causes and their respective solutions.

Unable to connect to Genetec ClearID™

Description: The synchronization tool is unable to connect to ClearID.

Solution: Review the One Identity ConfigurationTool logs.

1. Click , then click Open logs folder.

Tip: You can also open the ConfigurationTool logs manually here:
Code

```
%ProgramData%\Genetec\OneIdentity\Logs\ConfigurationTool
```



2. Review the One Identity ConfigurationTool logs for error messages related to ClearID connectivity issues.
3. Check your API integration connection.
 - a. Click Administration > Automation and select your API integration.
 - b. Check that your API integration key and Client ID details are correct.
4. [Check your connection settings.](#)

Unable to connect to Azure AD

Description: The synchronization tool is unable to connect to Azure Active Directory.

Solution: Review the One Identity ConfigurationTool logs.

1. Click , then click Open logs folder.

Tip: You can also open the ConfigurationTool logs manually here:
Code

```
%ProgramData%\Genetec\OneIdentity\Logs\ConfigurationTool
```



2. Review the One Identity ConfigurationTool logs for error messages related to Azure AD connectivity issues.
3. Check your Azure AD application connection details.

Browse

- [Synchronizing identities using One Identity Synchronization Tool in ClearID](#)

14.8 | ClearID One Identity Synchronization Tool data synchronization issues

If you encounter connectivity issues when using the Genetec ClearID™ One Identity Synchronization Tool, check your service logs for errors. To help you troubleshoot the issue, learn about the possible causes and their respective solutions.

Missing data fields

Description: Data fields are missing.

Solution: Review the One Identity Service logs.

1. Click , then click Open logs folder.

Tip: You can also open the ConfigurationTool logs manually here:
Code

```
%ProgramData%\Genetec\OneIdentity\Logs\Service
```



2. Review the One Identity Service logs for error messages related to missing data fields.

For more information about attribute fields, see [One Identity Synchronization Tool attribute fields](#).

3. [Check your Azure AD API permissions.](#)

Missing name fields (first name, last name)

Description: Name fields (first name or last name) are missing.

Solution: Review the One Identity Service logs.

1. Click , then click Open logs folder.

Tip: You can also open the ConfigurationTool logs manually here:

Code

```
%ProgramData%\Genetec\OneIdentity\Logs\Service
```



2. Review the One Identity Service logs for error messages related to name fields.

For more information about attribute fields, see [One Identity Synchronization Tool attribute fields](#).

3. Check your Azure AD API permissions.

Missing email addresses

Description: Email address fields are missing.

Solution: Review the One Identity Service logs.

1. Click , then click Open logs folder.

Tip: You can also open the ConfigurationTool logs manually here:

Code

```
%ProgramData%\Genetec\OneIdentity\Logs\Service
```



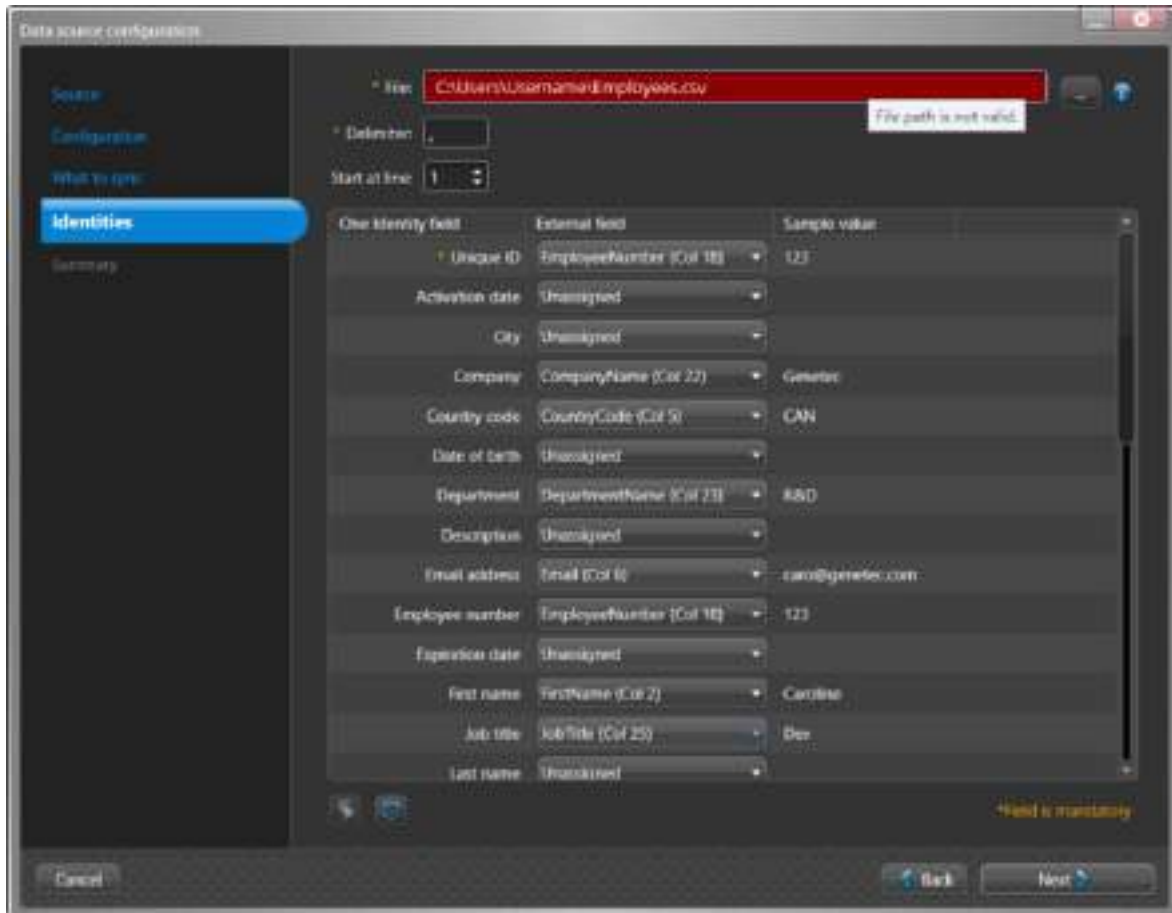
2. Review the One Identity Service logs for error messages related to email address fields.

For more information about attribute fields, see [One Identity Synchronization Tool attribute fields](#).

3. Check your Azure AD API permissions.

File path is not valid

Description: User permission issues encountered when using CSV files as the data source for Identities because the file path is not valid.



Solution:

Best Practice: To avoid user permission issues when using CSV files with the ClearID One Identity Synchronization Tool, save your files to a C: or C:\temp folder location. Do not save your CSV files in user-controlled file or folder locations (c:\Users folders or desktop folder location) or you might encounter File path is not valid user permissions issues.

Browse

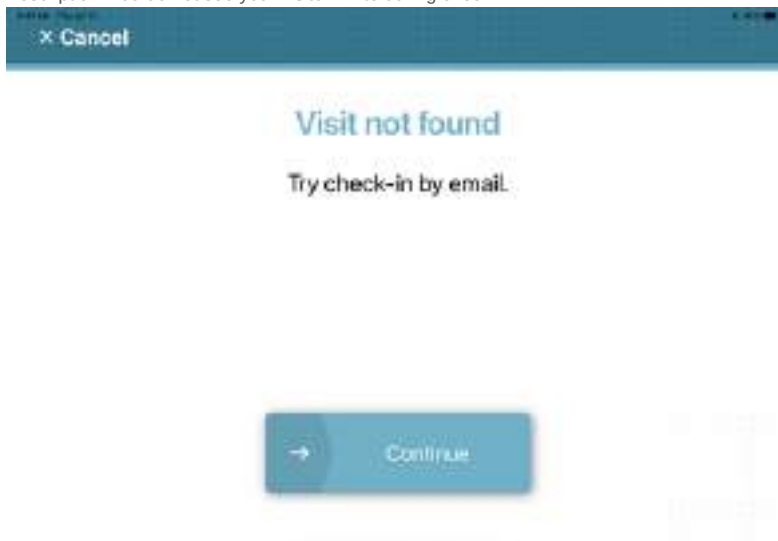
- Synchronizing identities using One Identity Synchronization Tool in ClearID

14.9 | ClearID Self-Service Kiosk issues

If the Genetec ClearID™ Self-Service Kiosk check-in function or the kiosk does not work as expected, you can perform additional troubleshooting steps.

Visitor invite or visit event not found

Description: You do not see your visitor invite during check-in.



The *visit not found* issue can occur for various reasons:

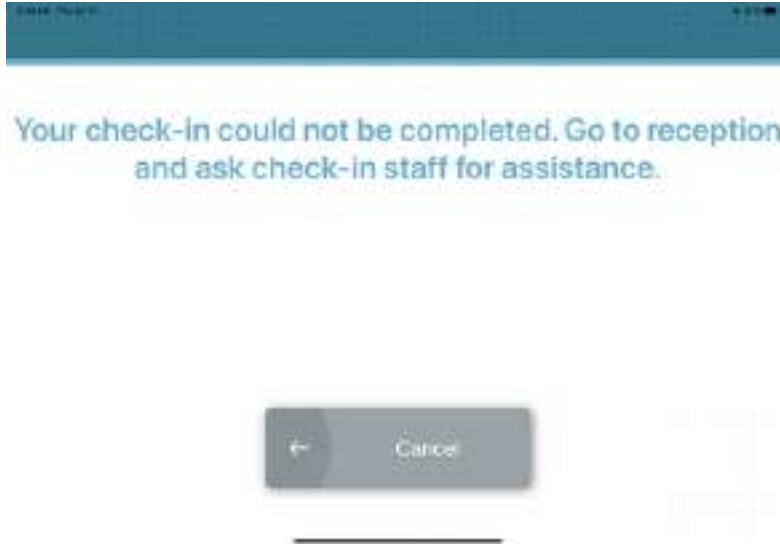
- Visitor check-in is too early (1hr+ before event start time).
- Visitor check-in is too late (1hr+ after event end time).
- Visitor is not listed in visit event invite.
- The visitor name in the visit event invite contains a mistake or typo.

Solution:

- Check the visit event start and end times. Visitors can check in up to 1 hour before or after a visit event.
- Check visitor names listed in the visit event. Look for any visitors not listed or any mistakes in the visitor details.

Check-in could not be completed

Description: You are unable to complete your check-in.



Solution: Check your site and area settings. Self check-in can fail due to one or more of the following:

1. Visitor management is not enabled for the site.
 - a. In Genetec ClearID™, click Organization > Sites.
 - b. Select your site and click Visitor Management.
 - c. Select Enable visitor management for this site.
 - d. Click Save.
2. Visitor management permissions for the site have not been configured.
 - a. In ClearID, click Organization > Sites.
 - b. Select your site and click Visitor Management > Permissions.
 - c. Check identity permissions.
 - d. Modify permissions as required and click Save.

For example, Add role permissions or give all identities access to invite visitors.
3. Visitor management is enabled for the site but no areas are defined or there is no default area.
 - a. In ClearID, check visitor management is enabled for the area. (Areas > Select an area > Visitor Management).
 - b. Check the Automatically add this area when creating visit requests is enabled.
4. Visitor management is enabled for the site and there is at least one default area under that site. However, the host does not have the authority to invite visitors for that site.
 - a. Refer to [Step 2](#).
5. Site is set to approval required. Visit event approval workflow should be set to No approval required.
 - a. In ClearID, click Organization > Sites and select your site.
 - b. Click Visitor Management, then in Advanced section check Visitor event approval workflow is set to No approval required.

Camera errors

Description: The Self-Service Kiosk can occasionally encounter the following camera issues:

- Unable to initialize the front camera.
- An error was encountered while configuring the camera. Try again.

Solution: Check the following:

1. On the iPad, tap Settings and scroll down to the Self-Service Kiosk app then tap Camera to enable the camera.
2. On the iPad, tap Settings > Privacy & Security and check that the Self-Service Kiosk has access to the camera.

Tip: These settings might not be visible on your iPad if you have not used the Scan QR code function before. In this situation, you can try the following: Tap Check-in > QR code, then tap Cancel and try the previous solution steps again.

14.10 | ClearID Self-Service Kiosk label printer issues

If the Genetec ClearID™ Self-Service Kiosk label printer is not performing as expected, you can check the configuration, check the hardware, or perform additional troubleshooting steps.

To help you troubleshoot Self-Service Kiosk label printer issues, refer to the possible causes and their respective solutions that follow.

No Bluetooth label printers detected

Description: No Bluetooth label printers were detected. This issue can be caused by a configuration or hardware issue.

Solution:

1. Check that the printer is powered on and ready for use.
2. Check that Bluetooth is enabled on the label printer.
 - a. In the Settings menu, select Bluetooth > Bluetooth (On/Off) > On and press OK.



- b. In the Settings menu, select Bluetooth > Automatic Reconnection (On/Off) > On and press OK.



3. Check that Bluetooth is enabled in the ClearID Self-Service Kiosk mobile app.
4. Check that Bluetooth is enabled on the iPad.
5. Check that the printer is paired with the ClearID Self-Service Kiosk.
6. (Optional) Perform a hard reset of the Self-Service Kiosk iPad.
 - a. Configure your Self-Service Kiosk iPad.
 - b. Do one of the following:
 - Configuring the ClearID Self-Service Kiosk label printer for Bluetooth mode (Brother QL-820NWBc or QL-820NWB).
 - Configuring the ClearID Self-Service Kiosk label printer for Bluetooth mode (Brother TD-4550DNWB).
 - c. Select a label printer.
 - d. Print a test badge.

No Wi-Fi label printers detected

Description: No label printers were detected on the Wi-Fi network. This issue can be caused by a configuration or hardware issue.

Solution:

1. Check that the printer is powered on and ready for use.
2. Check that the Wi-Fi network is available.

The Wi-Fi network must be enabled for use and support the following:

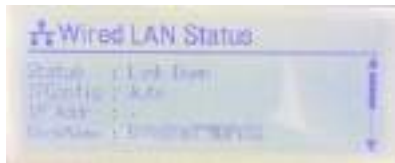
 - Bonjour - required for device search.
 - SNMP - required to check printer status information.
 - UDP or TCP Port 9100 - required to send print data.
3. Check that Wi-Fi is enabled on the label printer.
 - a. In the Settings menu, select WLAN > WLAN (On/Off) > On and press OK.



4. Check that Wi-Fi is enabled on the iPad.
5. Check that the Self-Service Kiosk iPad and the label printer are on the same Wi-Fi network.
6. (Optional) Perform a hard reset of the Self-Service Kiosk iPad.
 - a. Configure your Self-Service Kiosk iPad.
 - b. Do one of the following:
 - Configuring the ClearID Self-Service Kiosk label printer for Wi-Fi mode (Brother QL-820NWBc, QL-820NWB, or QL-810W).
 - Configuring the ClearID Self-Service Kiosk label printer for Wi-Fi mode (Brother TD-4550DNWB).
 - c. Select a label printer.
 - d. Print a test badge.

No Ethernet label printers detected

Description: The label printer is showing the Wired LAN Status Link Down.

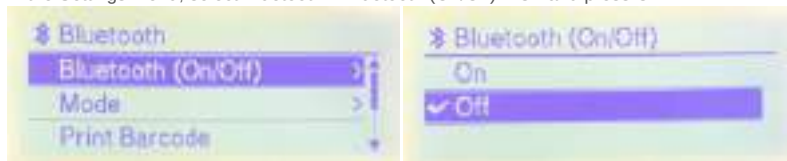


Solution:

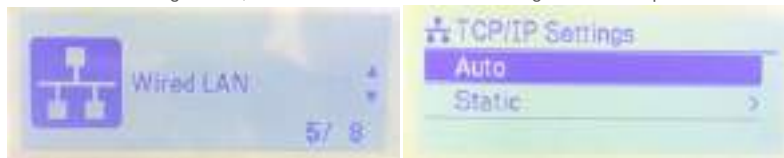
1. Check that the printer is powered on and ready for use.
2. Check that the Wi-Fi function on the label printer is turned off.
 - a. From the label printer Settings menu, turn OFF WLAN (Wi-Fi).



3. Check that the Bluetooth function on the label printer is turned off.
 - a. In the Settings menu, select Bluetooth > Bluetooth (On/Off) > Off and press OK.



4. Check that the Ethernet network is available.
5. Check that Ethernet is enabled on the label printer.
 - a. In the Settings menu, select Wired LAN > TCP/IP Settings > Auto and press OK.



6. Check that the printer is connected to a LAN port and not to a WAN port (either on your router or your organizations network).
7. Verify that you are using the correct type of LAN cable.
Best Practice: Use a straight-through Category 5 (or greater) twisted-pair cable for 10BASE-T or 100BASE-TX Fast Ethernet Network.
8. (Optional) Perform a hard reset of the Self-Service Kiosk iPad.
 - a. Configure your Self-Service Kiosk iPad.
 - b. Do one of the following:
 - Configuring the ClearID Self-Service Kiosk label printer for Ethernet mode (Brother QL-820NWBc or QL-820NWB).
 - Configuring the ClearID Self-Service Kiosk label printer for Ethernet mode (Brother TD-4550DNWB).
 - c. Select a label printer.
 - d. Print a test badge.

Printing: A printing error has occurred. There is no paper in the printer.

Description: The label printer has run out of labels or has jammed.

Solution:

1. Check for the end of the label roll and replace if necessary:
 - o Brother QL-820NWBc or QL-820NWB: DK Roll - 62mm Black (Brother Part No: DK-2205) or 62mm Red and Black (Brother Part No: DK-2251)
 - o Brother TD-4550DNWB: RD Roll - 57mm Black (Brother Part No: RD001U1S)
2. Check the printer for a label jam or feed error.

Brother QL-820NWBc or QL-820NWB: A printing error has occurred

Description: The Brother QL-820NWBc or QL-820NWB label printer has encountered an unknown printing error.



Solution:

1. Check the [Label Printer Led Status indicators FAQ](#) database for possible causes.
2. Check the [Connecting to a Mobile Device](#) section for possible causes.
3. Check the [FAQs & Troubleshooting Printing](#) section for possible causes.

Brother QL-820NWBc or QL-820NWB: Printer turns off unexpectedly

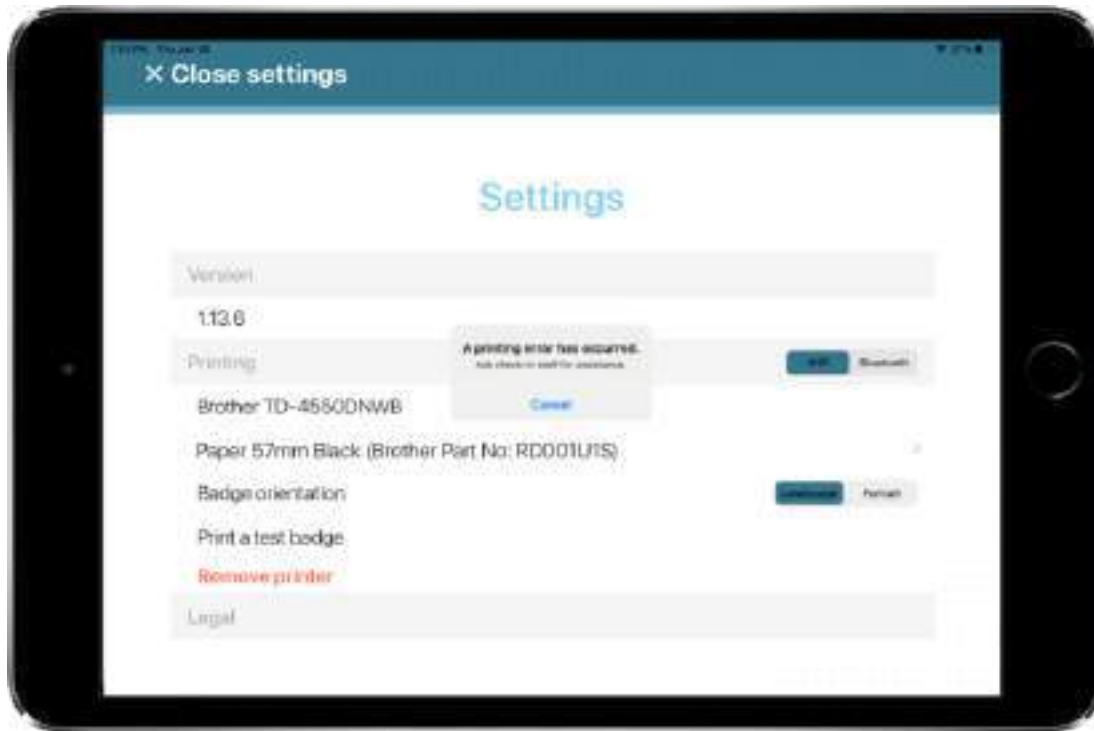
Description: The label printer turns off automatically at the same time every day.

Solution: Change the settings from the printer menu.

1. Press the Menu button.
2. Select Settings using the ▲ ▼ buttons, and then press the OK button.
3. Select Auto Power Off using the ▲ ▼ buttons, and then press the OK button.
4. Select Adapter using the ▲ ▼ buttons, and then press the OK button.
5. Select Off using the ▲ ▼ buttons, and then press the OK button.
6. (Optional) Also set the time to Off for [Li-ion battery], following the steps above.

Brother TD-4550DNWB: A printing error has occurred

Description: The Brother TD-4550DNWB label printer has encountered an unknown printing error.



Solution:

1. Check the [Label Printer Led Status indicators FAQ](#) database for possible causes.
2. Check the [Connecting to a Mobile Device](#) section for possible causes.
3. Check the [FAQs & Troubleshooting Printing](#) section for possible causes.

Brother TD-4550DNWB: Badge printout never arrives

Description: When printing a badge, the badges are sent to the printer but the printed badge never arrives.

Solution:

1. Check the printer LCD display to confirm you are not in a configuration or settings menu.
NOTE: Leaving the printer in a configuration or settings menu can cause badge printing to be paused until you complete your changes.
2. If you left the printer in a configuration or settings menu, press the Menu button or use the printer controls to return to the homepage.

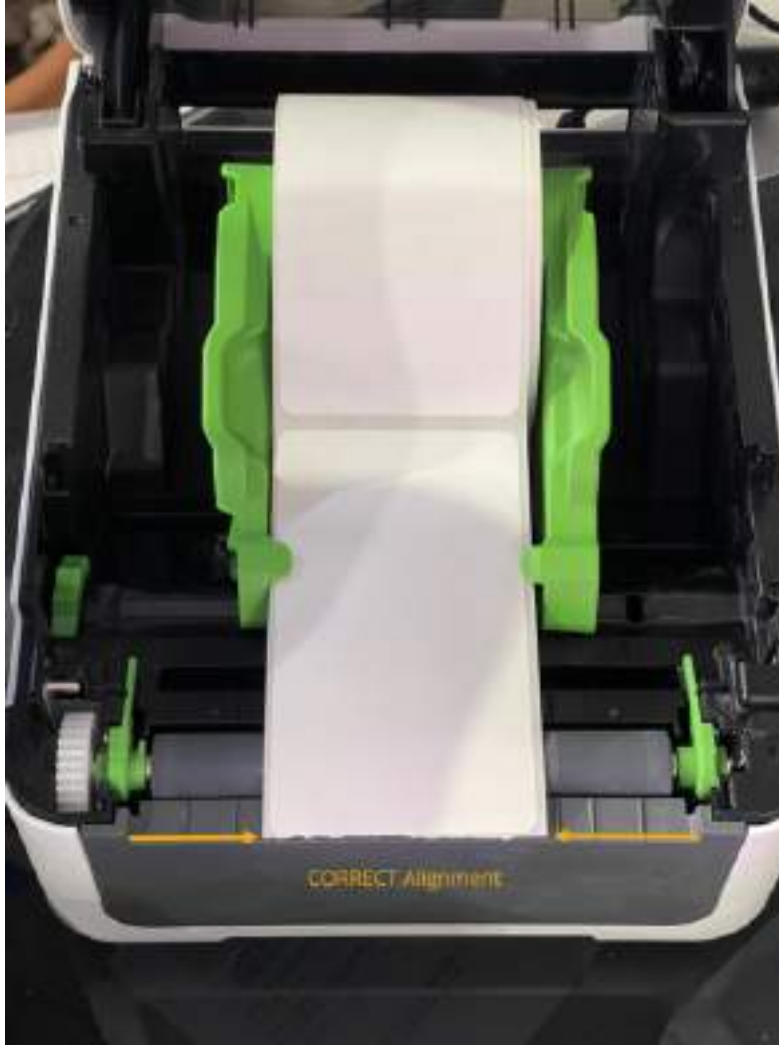
After returning to the homepage, badge printing should resume as normal.

Brother TD-4550DNWB: Badges do not print as expected

Description: The label printer prints a partial label or label orientation appears to be messed up. For example, in some situations the printer can print half a badge or print across two labels.

Solution:

1. Before printing any badges, check your label alignment and orientation.



IMPORTANT: The first label must be aligned with the front edge of the printer to ensure correct printing. Make sure that none of the labels have advanced past the front edge of the printer before printing. The printer only detects the label edges automatically after printing the first label, if the first label is misaligned badge printing issues can occur.

For more information about how to load labels or sensor positioning for different label types, see [Load the RD roll](#) and [Check the Sensor Position](#) in the Brother online printer documentation.

Browse

- [Resetting the ClearID Self-Service Kiosk mobile app](#)
- [Firewall ports used in ClearID](#)