



# Security Center SaaS Deployment Guide

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

Document last updated: September 6, 2024

# Legal notices

---

©2024 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: Security Center SaaS Deployment Guide

Original document number: EN.600.001

Document number: EN.600.001

Document update date: September 6, 2024

You can send your comments, corrections, and suggestions about this guide to [documentation@genetec.com](mailto:documentation@genetec.com).

# About this guide

---

This guide is intended for integrators who are planning to purchase Security Center SaaS and deploy hybrid components. It introduces our unified SaaS solution and describes the prerequisites and initial tasks to set up the system.

## Notes and notices

The following notes and notices might appear in this guide:

- **Tip:** Suggests how to apply the information in a topic or step.
- **Note:** Explains a special case or expands on an important point.
- **Important:** Points out critical information concerning a topic or step.
- **Caution:** Indicates that an action or step can cause loss of data, security problems, or performance issues.
- **Warning:** Indicates that an action or step can result in physical harm, or cause damage to hardware.

**IMPORTANT:** Content in this guide that references information found on third-party websites was accurate at the time of publication, however, this information is subject to change without prior notice from Genetec Inc.

# Contents

---

## Preface

Legal notices . . . . .	ii
About this guide . . . . .	iii

## Chapter 1: Getting started

About Security Center SaaS . . . . .	2
Setup overview . . . . .	3
Signing in to Security Center SaaS . . . . .	4

## Chapter 2: Requirements

Presale checklist . . . . .	6
Network requirements . . . . .	7
Port requirements . . . . .	8
Port requirements for direct-to-cloud cameras . . . . .	8
Port requirements for appliances . . . . .	11
Port requirements for clients . . . . .	18
Port requirements for Federation . . . . .	20
Supported devices . . . . .	21
Supported features . . . . .	22

## Chapter 3: User management

Adding users . . . . .	24
Adding groups . . . . .	27

## Chapter 4: Device management

Adding devices . . . . .	30
Adding Axis direct-to-cloud cameras . . . . .	31
Adding Axis Powered by Genetec devices . . . . .	35
Signing in to an Axis Powered by Genetec device . . . . .	38
Adding Genetec Cloudlink 310 appliances . . . . .	40
Applying a static IP configuration to Genetec Cloudlink 310 . . . . .	42
Adding cameras to Genetec Cloudlink 310 using automatic discovery . . . . .	43
Adding cameras to Genetec Cloudlink 310 manually . . . . .	44
Adding Synergis Cloud Link appliances . . . . .	45
How privacy protection works in Security Center SaaS . . . . .	47

## Chapter 5: Federation through reverse tunneling

What is reverse tunneling . . . . .	50
Deploying Security Center Federation using reverse tunneling . . . . .	52
Creating reverse tunnels on the Federation host . . . . .	53
Opening reverse tunnels between remote sites and the Federation host . . . . .	55
Connecting the Federation host to remote sites through reverse tunnels . . . . .	57
Resetting reverse tunnels . . . . .	59

Glossary . . . . .	61
--------------------	----

Technical support . . . . . 66

# Getting started

This section includes the following topics:

- ["About Security Center SaaS"](#) on page 2
- ["Setup overview"](#) on page 3
- ["Signing in to Security Center SaaS"](#) on page 4

# About Security Center SaaS

---

Security Center SaaS is a unified hybrid-cloud solution offering physical security as a service. It integrates advanced security capabilities, emphasizes cybersecurity and privacy, and manages complex security tasks on premises, in the cloud, or both. With the flexibility of Security Center SaaS, organizations can efficiently monitor and respond to security threats from one place.

To introduce yourself to Security Center SaaS and learn more about the product, see the following:

## On the TechDoc Hub

- [Security Center SaaS User Guide for Web](#)

## Security Center SaaS resources

- [Security Center SaaS brochure](#)
- [Security Center SaaS product page](#)
- [Introducing Genetec™ Security Center SaaS](#)
- [How to modernize your existing security systems using hybrid-cloud](#)
- [Physical security designed to last](#)
- [How to choose a cloud-based physical security solution that will stand the test of time](#)

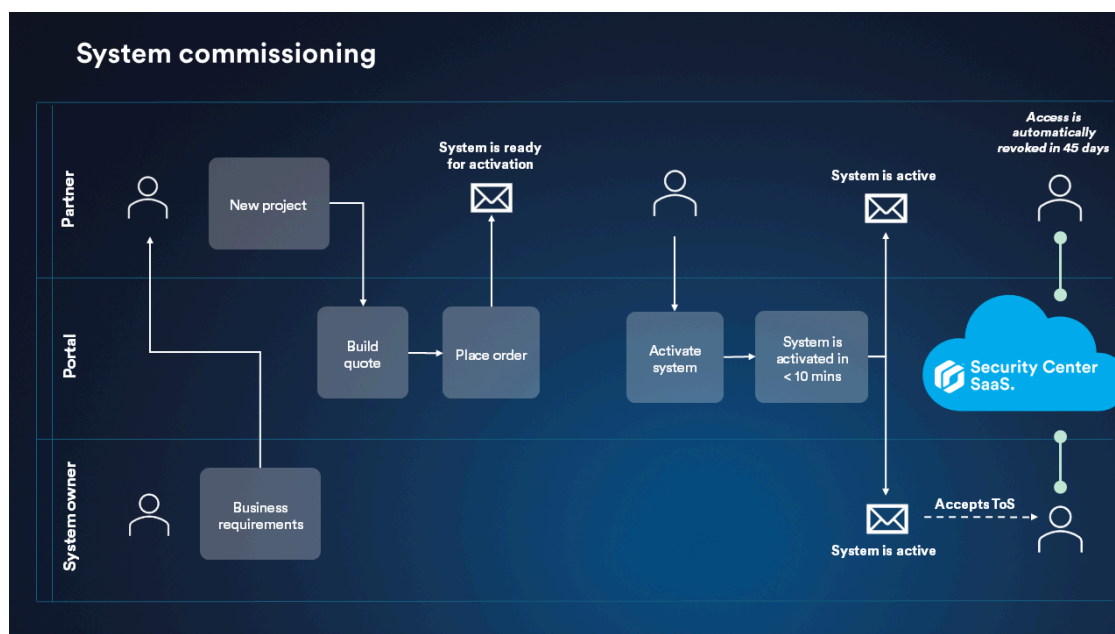
## Cloud-managed appliance resources

- [Cloud-managed appliances product page](#)
- [Genetec Cloudlink™ 310 datasheet](#)

## Setup overview

Setting up Security Center SaaS involves planning, ordering, activating, and configuring the system.

1. [Learn about Security Center SaaS and how it works.](#)
2. Review the Security Center SaaS requirements:
  - a. [Presale checklist](#)
  - b. [Network requirements](#)
  - c. [Ports and protocols](#)
  - d. [Supported devices](#)
3. Commission a new system:



- a. Review business requirements
  - b. Build quote
  - c. Place order
  - d. Activate system
4. [Sign in to Security Center SaaS.](#)
  5. [Create your users and apply roles.](#)
  6. [Create groups](#) to define inherited user permissions based on group membership.
  7. [Add devices](#)

**NOTE:** The visibility of local devices depends on the location of your appliances. For devices to be discoverable, the appliance must be on the same local network as the device.

8. (Optional) [Configure federation through reverse tunneling.](#)
9. (Optional) Download desktop clients from the Security Center SaaS Welcome page.
10. (Optional) Install mobile clients from the Apple App Store or Google Play.



# Signing in to Security Center SaaS

---

After you activate your user account, sign in to your Security Center SaaS web portal to manage devices and users in the Genetec™ Configuration application.

## What you should know

Use a valid user account from a supported identity provider when accessing Security Center SaaS. The system ID can change depending on which user account signs in.

## Procedure

- 1 Enable cookies and JavaScript in your web browser.
- 2 In your web browser, go to <https://securitycentersaas.genetec.cloud/>.
- 3 On the *Welcome* page, enter your email and click **Sign in**.
- 4 If you have more than one system, select the system that you require.

**TIP:** To switch systems, you can also click **Change system** from the **Profile** options in the Configuration sidebar.

# Requirements

This section includes the following topics:

- ["Presale checklist"](#) on page 6
- ["Network requirements"](#) on page 7
- ["Port requirements"](#) on page 8
- ["Supported devices"](#) on page 21
- ["Supported features"](#) on page 22

## Presale checklist

---

Use this checklist to collect information about the customer's environment and to ensure that it meets Security Center SaaS requirements.

- Check the internet Service Level Agreement (SLA) with the customers internet provider.
- Resolve any outstanding IT or security concerns before purchase.
- Make sure that Security Center SaaS supports the features that you need.

**NOTE:** Plugin integrations are not supported.

Estimate the number of simultaneous users of the following software:

- Genetec™ Configuration on desktop, web, and mobile
- Genetec™ Operation on desktop, web, and mobile

Check Access Control information:

- Number of Synergis™ Cloud Link units
- Number of Axis Powered by Genetec units
- Number of Access Control system devices (readers, inputs, and outputs)
- Estimated number of cardholders and credentials to be handled

Check Video information:

- Number of camera devices including models
- Number of Genetec Cloudlink™ appliances
- FPS, resolution, and retention to ensure that the correct package is chosen

Check Federation™ information:

- Video compression standards (only H.264 is supported)
- ISP policies: Static versus dynamic IP addressing
- Required firewall configuration
- Number of remote systems and their corresponding federated camera connections
- Available upload bandwidth per site (see [Bandwidth considerations](#))
- Any required expansion resources on site (such as IP door controllers)

### Related Topics

[Supported devices](#) on page 21

# Network requirements

---

To successfully deploy Security Center SaaS in the cloud, network infrastructure must meet the required performance criteria, and network policy must adhere to the setup recommendations.

## General network requirements

Security Center SaaS have the following network requirements:

- **Azure® connections:** High-latency connections might negatively impact the availability of remote sites. A latency of 150 ms or less to the closest Azure® data center is mandatory. Use the [Azure® Storage Latency Test](#) to determine which Azure® data center is the best for hosting your servers.
- **Internet service level:** A service level of 99.9% guaranteed by the customer's Internet service provider (ISP) is highly suggested.
- **Bandwidth:** Bandwidth considerations depend on the number of cameras performing recording or playback functions, and whether you are recording locally or pushing your recordings to the cloud. Playback has no effect on the number of cameras that can be viewed simultaneously. These considerations do not apply if the client workstation is in the same network as the camera being viewed.

## Federation network requirements

Federation™ in Security Center SaaS has the following extra considerations and requirements:

- **Bandwidth:** The number of cameras that can be viewed simultaneously depends on several factors:
  - Outbound bandwidth from the remote site
  - Inbound bandwidth to the client workstation
  - Quality of requested video streams**NOTE:** All managed devices always go through the cloud.
- **Multi-streaming:** Cameras at remote sites should support multiple streams. These multiple streams ensure that a lower bandwidth stream can be used for outbound video streams from the remote sites. Only a single stream is supported for managed devices.

## Port requirements

To enable communication with cameras, appliances, clients, and on-premises Security Center systems, you must open specific network ports.

- [Port requirements for direct-to-cloud \(D2C\) cameras](#)
- [Port requirements for appliances](#)
- [Port requirements for clients](#)
- [Port requirements for Federation](#)

### Port requirements for direct-to-cloud cameras

To enable communication with direct-to-cloud (D2C) cameras, you must open specific outbound ports for the associated domains.

#### All D2C cameras

For all D2C cameras, open the following outbound ports for the associated domains to enable them to connect to cloud services, be managed, and stream video.

Outbound port	Endpoint domain	Port usage
UDP 53		Connection to the Domain Name System (DNS)
	Domains : *.blob.core.windows.net *.genetec.cloud login.genetec.com	
	Details for the Australia region:	
TCP 443	eastau.video.genetec.cloud australiaeast.tds.genetec.cloud auescsaas01.blob.core.windows.net auescsaas02.blob.core.windows.net auescsaas03.blob.core.windows.net auescsaas04.blob.core.windows.net auescsaas05.blob.core.windows.net auescsaas06.blob.core.windows.net auescsaas07.blob.core.windows.net auescsaas08.blob.core.windows.net auescsaas09.blob.core.windows.net auescsaas10.blob.core.windows.net auescsaas11.blob.core.windows.net auescsaas12.blob.core.windows.net auescsaas13.blob.core.windows.net auescsaas14.blob.core.windows.net auescsaas15.blob.core.windows.net auescsaas16.blob.core.windows.net	Management and recording offload

Outbound port	Endpoint domain	Port usage
Details for the Canada region:		
	centralca.video.genetec.cloud cancentral.tds.genetec.cloud	
	cacscsaas01.blob.core.windows.net cacscsaas02.blob.core.windows.net cacscsaas03.blob.core.windows.net cacscsaas04.blob.core.windows.net cacscsaas05.blob.core.windows.net cacscsaas06.blob.core.windows.net cacscsaas07.blob.core.windows.net cacscsaas08.blob.core.windows.net cacscsaas09.blob.core.windows.net cacscsaas10.blob.core.windows.net cacscsaas11.blob.core.windows.net cacscsaas12.blob.core.windows.net cacscsaas13.blob.core.windows.net cacscsaas14.blob.core.windows.net cacscsaas15.blob.core.windows.net cacscsaas16.blob.core.windows.net	
Details for the Europe region:		
	westeu.video.genetec.cloud westeurope.tds.genetec.cloud	
	weuscsaas01.blob.core.windows.net weuscsaas02.blob.core.windows.net weuscsaas03.blob.core.windows.net weuscsaas04.blob.core.windows.net weuscsaas05.blob.core.windows.net weuscsaas06.blob.core.windows.net weuscsaas07.blob.core.windows.net weuscsaas08.blob.core.windows.net weuscsaas09.blob.core.windows.net weuscsaas10.blob.core.windows.net weuscsaas11.blob.core.windows.net weuscsaas12.blob.core.windows.net weuscsaas13.blob.core.windows.net weuscsaas14.blob.core.windows.net weuscsaas15.blob.core.windows.net weuscsaas16.blob.core.windows.net	

Outbound port	Endpoint domain	Port usage
Details for the US region:		
	<pre> eastus2.video.genetec.cloud eastus2.tds.genetec.cloud  eus2scsaas01.blob.core.windows.net eus2scsaas02.blob.core.windows.net eus2scsaas03.blob.core.windows.net eus2scsaas04.blob.core.windows.net eus2scsaas05.blob.core.windows.net eus2scsaas06.blob.core.windows.net eus2scsaas07.blob.core.windows.net eus2scsaas08.blob.core.windows.net eus2scsaas09.blob.core.windows.net eus2scsaas10.blob.core.windows.net eus2scsaas11.blob.core.windows.net eus2scsaas12.blob.core.windows.net eus2scsaas13.blob.core.windows.net eus2scsaas14.blob.core.windows.net eus2scsaas15.blob.core.windows.net eus2scsaas16.blob.core.windows.net </pre>	
TCP 1935	<b>IMPORTANT:</b> Ensure that you include the Cloud Security Center Virtual Machine associated with your system: <i>*.gsc-cloud.com</i> in your allowlist.	Interactive Connectivity Establishment (ICE) TCP in Web Real-Time Communication (WebRTC) for live streaming
TCP 443	<i>turn.video.geneteccloud.com</i>	Traversal Using Relays around NAT (TURN) server and Session Traversal Utilities for NAT (STUN) server for live video streaming
UDP 3478	<i>stun.relay.metered.ca</i>	
TCP 3478	<i>global.relay.metered.ca</i>	
TCP 80	<i>stun.relay.metered.ca</i> <i>global.relay.metered.ca</i>	WebRTC relay (STUN and TURN)

## Axis D2C cameras

Axis D2C cameras need extra connections to Axis services for onboarding, correct operation, and maintenance.

Outbound port	Endpoint domain	Port usage
UDP 123	<i>pool.ntp.org</i> <b>NOTE:</b> An Axis domain might replace this domain in the future	Network Time Protocol (NTP)
	<i>*.connect.axis.com</i>	
TCP 443	Details: <pre> cep.prod.flagsmith.connect.axis.com cep.otelcol.connect.axis.com eu.prod.otelcol.connect.axis.com appinsights.connect.axis.com prod.adm.connect.axis.com signaling.prod.webrtc.connect.axis.com onboardme.prod.oneclick.connect.axis.com </pre>	Device management and diagnostics

Outbound port	Endpoint domain	Port usage
	<i>*-st.axis.com</i>	
	Details:	
TCP 443	dispatchus1-st.axis.com dispatchse1-st.axis.com dispatchse2-st.axis.com dispatchjp1-st.axis.com dispatcher-st.axis.com	Device onboarding
TCP 443	<i>s3-ats-migration-test.s3.eu-west-3.amazonaws.com</i>	Test Amazon Web Services (AWS) Public Key Infrastructure (PKI)

## Port requirements for appliances

To enable communication with appliances, you must open specific network ports.

### Genetec Cloudlink 310 to Security Center SaaS

For Genetec Cloudlink™ video, the following ports must be open for the associated domains. Opening the ports ensures that the devices can connect to cloud services, be managed, and stream video.

Outbound port	Endpoint domain	Port usage
	Network Time Protocol (NTP) servers are selected from the following sources (highest priority to lowest priority):	
	1. Manual NTP configuration in Genetec Cloudlink	
	2. DHCP	
UDP 123	3. Default NTP servers: <ul style="list-style-type: none"> <li><i>time1.google.com</i></li> <li><i>time2.google.com</i></li> <li><i>time3.google.com</i></li> <li><i>time4.google.com</i></li> </ul>	Connection to an NTP server.



Outbound port	Endpoint domain	Port usage
	<p>Genetec Cloudlink communicates with the following domains:</p> <ul style="list-style-type: none"> <li><i>*.azurecr.io</i></li> <li><i>*.azure-devices.net</i></li> <li><i>*.azure-devices-provisioning.net</i></li> <li><i>global.azure-devices-provisioning.net</i></li> <li><i>*.cloudapp.azure.com</i></li> <li><i>*.blob.core.windows.net</i></li> <li><i>*.in.applicationinsights.azure.com</i></li> <li><i>*.genetec.cloud</i></li> <li><i>login.genetec.com</i></li> <li><i>eastus2-3.in.applicationinsights.azure.com</i></li> <li><i>eastus2.livediagnostics.monitor.azure.com</i></li> </ul>	
TCP 443	<p>Details for the Australia region:</p> <pre> genetec-dm-hub-prod-eau-0.azure-devices.net edgeosprodeauappstore.azurecr.io edgeosprodeauappstore.australiaeast.data.azurecr.io prod0eafwimages.blob.core.windows.net prod0eadevicesdiags.blob.core.windows.net  eastau.video.genetec.cloud australiaeast.tds.genetec.cloud  tds1astleastrz.blob.core.windows.net tds2astleastrz.blob.core.windows.net tds3astleastrz.blob.core.windows.net tds4astleastrz.blob.core.windows.net tds5astleastrz.blob.core.windows.net tds6astleastrz.blob.core.windows.net tds7astleastrz.blob.core.windows.net tds8astleastrz.blob.core.windows.net  auescsaas01.blob.core.windows.net auescsaas02.blob.core.windows.net auescsaas03.blob.core.windows.net auescsaas04.blob.core.windows.net auescsaas05.blob.core.windows.net auescsaas06.blob.core.windows.net auescsaas07.blob.core.windows.net auescsaas08.blob.core.windows.net auescsaas09.blob.core.windows.net auescsaas10.blob.core.windows.net auescsaas11.blob.core.windows.net auescsaas12.blob.core.windows.net auescsaas13.blob.core.windows.net auescsaas14.blob.core.windows.net auescsaas15.blob.core.windows.net auescsaas16.blob.core.windows.net </pre>	Connection to the cloud.

Outbound port	Endpoint domain	Port usage
Details for the Canada region:		
	genetec-dm-hub-prod-cca-0.azure-devices.net edgeosprodccaappstore.azurecr.io edgeosprodccaappstore.canadacentral.data.azurecr.io prod0ccafwimages.blob.core.windows.net prod0ccadevicesdiags.blob.core.windows.net  centralca.video.genetec.cloud cancentral.tds.genetec.cloud  tds1cancentralhrz.blob.core.windows.net tds2cancentralhrz.blob.core.windows.net tds3cancentralhrz.blob.core.windows.net tds4cancentralhrz.blob.core.windows.net tds5cancentralhrz.blob.core.windows.net tds6cancentralhrz.blob.core.windows.net tds7cancentralhrz.blob.core.windows.net tds8cancentralhrz.blob.core.windows.net  cacscsaas01.blob.core.windows.net cacscsaas02.blob.core.windows.net cacscsaas03.blob.core.windows.net cacscsaas04.blob.core.windows.net cacscsaas05.blob.core.windows.net cacscsaas06.blob.core.windows.net cacscsaas07.blob.core.windows.net cacscsaas08.blob.core.windows.net cacscsaas09.blob.core.windows.net cacscsaas10.blob.core.windows.net cacscsaas11.blob.core.windows.net cacscsaas12.blob.core.windows.net cacscsaas13.blob.core.windows.net cacscsaas14.blob.core.windows.net cacscsaas15.blob.core.windows.net cacscsaas16.blob.core.windows.net	

Outbound port	Endpoint domain	Port usage
Details for the Europe region:		
	edgeosprodweuappstore.azurecr.io edgeosprodweuappstore.westeurope.data.azurecr.io edgeosprodweuappstore.northeurope.data.azurecr.io prod0weudevicesdiags.blob.core.windows.net genetec-dm-hub-prod-weu-0.azure-devices.net  westeu.video.genetec.cloud westeurope.tds.genetec.cloud  tds1westeuhorizon.blob.core.windows.net tds2westeuhorizon.blob.core.windows.net tds3westeuhorizon.blob.core.windows.net tds4westeuhorizon.blob.core.windows.net tds5westeuhorizon.blob.core.windows.net tds6westeuhorizon.blob.core.windows.net tds7westeuhorizon.blob.core.windows.net tds8westeuhorizon.blob.core.windows.net  weuscsaas01.blob.core.windows.net weuscsaas02.blob.core.windows.net weuscsaas03.blob.core.windows.net weuscsaas04.blob.core.windows.net weuscsaas05.blob.core.windows.net weuscsaas06.blob.core.windows.net weuscsaas07.blob.core.windows.net weuscsaas08.blob.core.windows.net weuscsaas09.blob.core.windows.net weuscsaas10.blob.core.windows.net weuscsaas11.blob.core.windows.net weuscsaas12.blob.core.windows.net weuscsaas13.blob.core.windows.net weuscsaas14.blob.core.windows.net weuscsaas15.blob.core.windows.net weuscsaas16.blob.core.windows.net	

Outbound port	Endpoint domain	Port usage
Details for the US region:		
	edgeosprodeus2appstore.azurecr.io edgeosprodeus2appstore.eastus2.data.azurecr.io edgeosprodeus2appstore.southcentralus.data.azurecr.io edgeosprodeus2appstore.westus2.data.azurecr.io genetec-dm-hub-prod-eus2-0.azure-devices.net prod0eus2fwimages.blob.core.windows.net prod0eus2devicesdiags.blob.core.windows.net  eastus2.video.genetec.cloud eastus2.tds.genetec.cloud  tds1eastus2horizon.blob.core.windows.net tds2eastus2horizon.blob.core.windows.net tds3eastus2horizon.blob.core.windows.net tds4eastus2horizon.blob.core.windows.net tds5eastus2horizon.blob.core.windows.net tds6eastus2horizon.blob.core.windows.net tds7eastus2horizon.blob.core.windows.net tds8eastus2horizon.blob.core.windows.net  eus2scsaas01.blob.core.windows.net eus2scsaas02.blob.core.windows.net eus2scsaas03.blob.core.windows.net eus2scsaas04.blob.core.windows.net eus2scsaas05.blob.core.windows.net eus2scsaas06.blob.core.windows.net eus2scsaas07.blob.core.windows.net eus2scsaas08.blob.core.windows.net eus2scsaas09.blob.core.windows.net eus2scsaas10.blob.core.windows.net eus2scsaas11.blob.core.windows.net eus2scsaas12.blob.core.windows.net eus2scsaas13.blob.core.windows.net eus2scsaas14.blob.core.windows.net eus2scsaas15.blob.core.windows.net eus2scsaas16.blob.core.windows.net	
TCP 1935	<b>IMPORTANT:</b> Ensure that you include the Cloud Security Center Virtual Machine associated with your system: *.gsc-cloud.com in your allowlist.	Interactive Connectivity Establishment (ICE) TCP in Web Real-Time Communication (WebRTC) for live streaming
TCP 443	turn.video.geneteccloud.com	Traversal Using Relays around NAT (TURN) server and Session Traversal Utilities for NAT (STUN) server for live video streaming
UDP 3478	stun.relay.metered.ca	
TCP 3478	global.relay.metered.ca	

Outbound port	Endpoint domain	Port usage
UDP 53	DNS servers are selected from the following sources (highest to lowest priority). <ol style="list-style-type: none"> <li>1. Manual DNS configuration in the Edge OS (local device webpage).</li> <li>2. DHCP</li> <li>3. Default DNS servers: <ul style="list-style-type: none"> <li>• 1.1.1.1</li> <li>• 8.8.8.8</li> <li>• 1.0.0.1</li> <li>• 8.8.4.4</li> </ul> </li> </ol>	Connection to a DNS server.
ICMP Ping	8.8.8.8	Diagnostics to indicate if the appliance can reach a global, public endpoint.

### Genetec Cloudlink 310 to cameras

For Genetec Cloudlink video, the following ports must be open towards the on-premises local cameras. Opening the ports ensures that the Cloudlink can connect to those cameras, manage them, and stream video.

Inbound port	Outbound port	Port usage
	TCP 443	Camera connections
	TCP 80	HTTPS on port 443 is preferred. Genetec Cloudlink only falls back to HTTP on port 80 if secure communication isn't available.
	TCP 554	RTSP for video requests
	UDP 3702	Camera discovery requests on 239.255.255.250 (multicast)
UDP 10000 to 10599		Real-Time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP) communication from cameras to the Genetec Cloudlink™ 310 unit
UDP 20000		Camera discovery responses

### Synergis Cloud Link appliances

For Synergis™ Cloud Link, the following ports must be open for the associated domains. Opening the ports ensures that the devices can connect to the cloud services, be managed, and ensures correct access control operations.

Outbound port	Endpoint domain	Port usage
TCP 443	<p>The Synergis Cloud Link communicates with the following domains and URLs:</p> <ul style="list-style-type: none"> <li>*.geneteccloud.com</li> <li>*.servicebus.windows.net</li> <li>*.blob.core.windows.net</li> <li>*.global.azure-devices-provisioning.net</li> <li>*.azure-devices.net</li> <li>google.com</li> </ul>	Connection to the cloud
	Domain details:	
	acaas-gateway-prod01.geneteccloud.com serbusnwskuumgkdlgi.servicebus.windows.net evhubnwskuumgkdlgi.servicebus.windows.net evhubbacknwskuumgkdlgi.servicebus.windows.net storsyncnwskuumgkdlgi.blob.core.windows.net storhealnwskuumgkdlgi.blob.core.windows.net storgatwnwskuumgkdlgi.blob.core.windows.net global.azure-devices-provisioning.net	
	Details for the Australia region:	
	iothub844650092.azure-devices.net google.com	
	Details for the Canada region:	
	iothub1887217071.azure-devices.net	
	Details for the Europe region:	
	iothub645286700.azure-devices.net	
	Details for the US region:	
	iothub1914824792.azure-devices.net	
UDP 123	Default: <i>time.windows.com</i>	Connection to a Network Time Protocol (NTP) server

## Axis Powered by Genetec appliances

For Axis Powered by Genetec appliances, the following outbound ports must be open for the associated domains. Opening the ports ensures that the devices can connect to cloud services, be managed, and ensure correct access control operations.

Outbound port	Endpoint domain	Port usage
TCP 443	<p>The Axes Powered by Genetec devices communicate with the following domains and URLs:</p> <ul style="list-style-type: none"> <li>*.geneteccloud.com</li> <li>*.servicebus.windows.net</li> <li>*.blob.core.windows.net</li> <li>*.global.azure-devices-provisioning.net</li> <li>*.Azure-devices.net</li> <li>google.com</li> <li>*.connect.axis.com</li> <li>*st.axis.com</li> </ul>	Connection to the cloud
	<p>Details:</p> <pre>acaas-gateway-prod01.geneteccloud.com serbusnwskuumgkdlgi.servicebus.windows.net evhubbnwskuumgkdlgi.servicebus.windows.net storsyncnwskuumgkdlgi.blob.core.windows.net storhealnwskuumgkdlgi.blob.core.windows.net storgatwnwskuumgkdlgi.blob.core.windows.net global.azure-devices-provisioning.net iothub1914824792.azure-devices.net google.com  cep.prod.flagsmith.connect.axis.com cep.otelcol.connect.axis.com eu.prod.otelcol.connect.axis.com appinsights.connect.axis.com prod.adm.connect.axis.com signaling.prod.webrtc.connect.axis.com onboardme.prod.oneclick.connect.axis.com</pre>	
UDP 123	ntp.pool.org	Connection to a Network Time Protocol (NTP) server

## Port requirements for clients

To enable communication with clients, you must open specific network ports.

The following ports must be open for the associated domains, so the client can connect to cloud services, select the correct organization, and authenticate.

Outbound port	Endpoint domain	Port usage
Web clients		
TCP 443	securitycentersaas.genetec.cloud us.securitycentersaas.genetec.cloud	Security Center SaaS Web Services

Outbound port	Endpoint domain	Port usage
	<a href="https://login.genetec.com">login.genetec.com</a> <a href="https://id.login.genetec.com">id.login.genetec.com</a> <a href="https://assets.login.genetec.com">assets.login.genetec.com</a> <a href="https://challenges.cloudflare.com">challenges.cloudflare.com</a>	Genetec™ single sign-on (SSO)
	<a href="https://login.microsoftonline.com">login.microsoftonline.com</a> <a href="https://aadcdn.msauth.net">aadcdn.msauth.net</a> <a href="https://login.live.com">login.live.com</a>	
	<a href="https://events.launchdarkly.com">events.launchdarkly.com</a> <a href="https://app.launchdarkly.com">app.launchdarkly.com</a> <a href="https://clientstream.launchdarkly.com">clientstream.launchdarkly.com</a>	
	<a href="https://sgnlr-uni-prodglobal-eastus2.service.signalr.net">sgnlr-uni-prodglobal-eastus2.service.signalr.net</a> <a href="https://canadacentral-1.in.applicationinsights.azure.com">canadacentral-1.in.applicationinsights.azure.com</a>	Monitoring & eventing
	<a href="https://az416426.vo.msecnd.net">az416426.vo.msecnd.net</a> <a href="https://dc.services.visualstudio.com">dc.services.visualstudio.com</a> <a href="https://widget.intercom.io">widget.intercom.io</a> <a href="https://js.intercomcdn.com">js.intercomcdn.com</a>	Dependencies
Genetec™ Operation web and mobile applications		
TCP 443	<a href="https://*.gsc-cloud.com">*.gsc-cloud.com</a> <a href="https://a.tile.openstreetmap.org">a.tile.openstreetmap.org</a> <a href="https://b.tile.openstreetmap.org">b.tile.openstreetmap.org</a>	HTTPS port
Genetec™ Configuration web		
TCP 443	<a href="https://eastus2.video.genetec.cloud">eastus2.video.genetec.cloud</a>	HTTPS port for video operations
Genetec Operation and Genetec Configuration desktop applications		
TCP 5500	<a href="https://*.gsc-cloud.com">*.gsc-cloud.com</a>	Genetec Security Center TLS proxy
TCP 554 TCP 560	<a href="https://*.gsc-cloud.com">*.gsc-cloud.com</a>	RTSP port (over TLS)
TCP 960	<a href="https://*.gsc-cloud.com">*.gsc-cloud.com</a>	Live and playback stream requests
TCP 443	<a href="https://downloadcenter1.genetec.com">downloadcenter1.genetec.com</a>	HTTPS



## Port requirements for Federation

For Federation™ of on-premises Security Center systems into Security Center SaaS, you must open firewall ports to allow communication between the sites.

### Federation of on-premises system into Security Center SaaS

The following table lists the default network ports that are used in a Federation setup. The administrator can choose to use different ports. For more information on port usage, ask your Genetec™ Channel Partner for the latest Federation port diagrams.

Computer	Inbound	Endpoint domain	Port usage
Directory (on-premises)	TCP 5500	*.gsc-cloud.com	Reverse tunnel communication

## Supported devices

---

For a list of devices and the associated firmware that are supported with Security Center SaaS, see [Supported Device List](#).

To avoid potential issues, install the recommended firmware version for your device. For detailed information about your particular device, see your device's documentation or visit the manufacturer's website.

For information about device compatibility, see [Security Center SaaS Device Compatibility Guidelines](#).

## Supported features

---

For an overview of the key features and differences between Security Center SaaS and Security Center on-premises, [download the Security Center SaaS Feature matrix](#).

# User management

This section includes the following topics:

- ["Adding users"](#) on page 24
- ["Adding groups"](#) on page 27

# Adding users

---

Before you can manage devices and users in Genetec™ Configuration, you must first add users in Security Center SaaS. Different roles can also be added to the users to grant different system privileges.

## What you should know

Security Center SaaS supports *third-party authentication* through Microsoft Entra ID or by using the OpenID Connect protocol. For help with integrating your *identity provider* with Security Center SaaS, contact the Genetec™ Technical Assistance Center (GTAC).

## Procedure

- 1 In Genetec Configuration web, select **Users** from the left sidebar, and click **Add user**.
- 2 In the *Add user* dialog, enter the required information.

3 Select one or more roles for the user:

In Security Center SaaS, we provide some default roles to get you started.

**TIP:** If you need different roles or more granular controls, use Genetec Configuration desktop to configure users or roles as needed.

- **Owner:** This role is designed for system owners. It grants user management privileges and the ability to accept terms and conditions. Only an Owner can grant or remove this role.
- **Administrator:** This role is designed for system administrators. It provides full access to both Genetec Configuration and Genetec™ Operation.
- **Operator:** This role is designed for security operators who monitor real-time events within the system. It provides access to Genetec Operation.

**Add user** [X]

First name  
Jane

Last name  
Doe

Email  
janedoe@test.com

Roles

☐ **Owner**  
This role is designed for system owners. It grants user management privileges and the ability to accept terms and conditions. Only an Owner can grant or remove this role.

☒ **Administrator**  
This role is designed for system administrators. It provides full access to both Genetec™ Configuration and Genetec™ Operation.

☒ **Operator**  
This role is designed for security operators who monitor real-time events within the system. It provides access to Genetec™ Operation.

☒ Send an activation link to the user now

Cancel Add user

4 (Optional) Send an activation email to the user immediately by selecting **Send an activation link to the user**.

**TIP:** You can create all your users first and send activation emails later.

5 Click **Add user**.

The user is created.

If an activation link was sent immediately, the new user receives a notification email inviting them to complete their registration, accept terms of use, and [sign in to the system](#).

## After you finish

If required, send an activation email to pending users:

- Filter the *Users* page for Status:Pending.
- Select a user.
- In the side pane, click **Send invitation**.

## Adding groups

Set up groups in Security Center SaaS to have users automatically inherit privileges based on their group membership.

### Procedure

- 1 In Genetec™ Configuration web, select **Users** from the left sidebar, and click the **Groups** tab.
- 2 Click **Add group**.
- 3 In the *Add group* dialog, enter the required information.
- 4 Select one or more roles for the group:

In Security Center SaaS, we provide some default roles to get you started.

**TIP:** If you require different roles or more granular controls use Security Center SaaS desktop to configure users or roles as needed.

- **Administrator:** This role is designed for system administrators. It provides full access to both Genetec™ Configuration and Genetec™ Operation.
- **Operator:** This role is designed for security operators who monitor real-time events within the system. It provides access to Genetec Operation.

**Add group** [X]

Name

Head Office Operators

Description (optional)

Montreal Head Office Operators

Roles

☐ **Administrator**  
This role is designed for system administrators. It provides full access to both Genetec™ Configuration and Genetec™ Operation.

☒ **Operator**  
This role is designed for security operators who monitor real-time events within the system. It provides access to Genetec™ Operation.

Cancel Create

- 5 Click **Create**.  
The group is created.
- 6 Select the new group from the **Groups** list.



- 7 In the group side pane, click **Add user** , select users to add to the group, and click **Add user** .

**Head Office Operators**

**General**

Name  
Head Office Operators

Description  
Montreal Head Office Operators

Users 3 items [+ Add user](#)

Operator 1

Operator 2

Operator 3

Roles

☐ **Administrator**  
This role is designed for system administrators. It provides full access to both Genetec™ Configuration and Genetec™ Operation.

☒ **Operator**  
This role is designed for security operators who monitor real-time events within the system. It provides access to Genetec™ Operation.

**Cancel** **Save**

- 8 Click **Save**.

# Device management

This section includes the following topics:

- ["Adding devices"](#) on page 30
- ["Adding Axis direct-to-cloud cameras"](#) on page 31
- ["Adding Axis Powered by Genetec devices"](#) on page 35
- ["Adding Genetec Cloudlink 310 appliances"](#) on page 40
- ["Adding Synergis Cloud Link appliances"](#) on page 45
- ["How privacy protection works in Security Center SaaS"](#) on page 47

# Adding devices

---

To add your devices you can scan a QR code, enter the information manually, or automatically discover devices on the local network.

## Procedure

- 1 In Genetec™ Configuration web, select **Devices** from the left sidebar, and click **Add device**.
- 2 Choose one of the following:
  - Scan QR code
  - Use device information
- 3 If you selected **Scan QR code**, choose one of the following:
  - [Add a Genetec Cloudlink 310 appliance](#).
  - [Add a Synergis™ Cloud Link appliance](#).
- 4 If you selected **Use device information**, choose one of the following:
  - Access control devices:
    - [Add an Axis Powered by Genetec appliance manually](#).
    - [Add a Synergis Cloud Link appliance manually](#).
  - Video devices:
    - [Add an Axis direct-to-cloud camera manually](#).
    - [Add a Genetec Cloudlink 310 appliance manually](#).

# Adding Axis direct-to-cloud cameras

---

Before you can view, record, and upload video to Cloud Storage, you must add your direct-to-cloud (D2C) cameras in Security Center SaaS.

## Before you begin

- Have the device serial number and Owner Authentication Key (OAK) ready. You can find this information in the *Axis Communications: Owner Authentication Key* document that is included with the device. Alternatively, you can obtain this information from the camera's web page.
- If the camera has been activated on another system, perform a factory reset before adding it to [Security Center SaaS](#).

## What you should know

Enrolling an Axis direct-to-cloud camera in Security Center SaaS automatically does two things:

- Upgrades the device firmware to the latest version.  
Security Center SaaS ensures that all your devices are running the latest firmware, when it becomes available.
- Generates a username and password for the device and deletes all previous credentials.  
Security Center SaaS manages passwords for you, ensuring that all your devices are protected by strong passwords.

For supported devices and firmware, see [Supported Device List](#) and [Security Center SaaS Device Compatibility Guidelines](#).

Direct-to-cloud requires a corresponding product subscription.

## Procedure

- 1 From the *Devices* page in Genetec™ Configuration web, click **Add device** and click **Use device information**.

- 2 In the *Add device* dialog box, click **Serial number + Owner Authentication Key (OAK)** and enter the required information:
  - **Name:** Enter a descriptive name for the device.
  - **Serial number:** Enter the device serial number.
  - **Owner Authentication Key (OAK):** Enter the Axis OAK.

← Add device ×

Name  
Main office - Lobby

Serial number  
B8AFR6ER432L

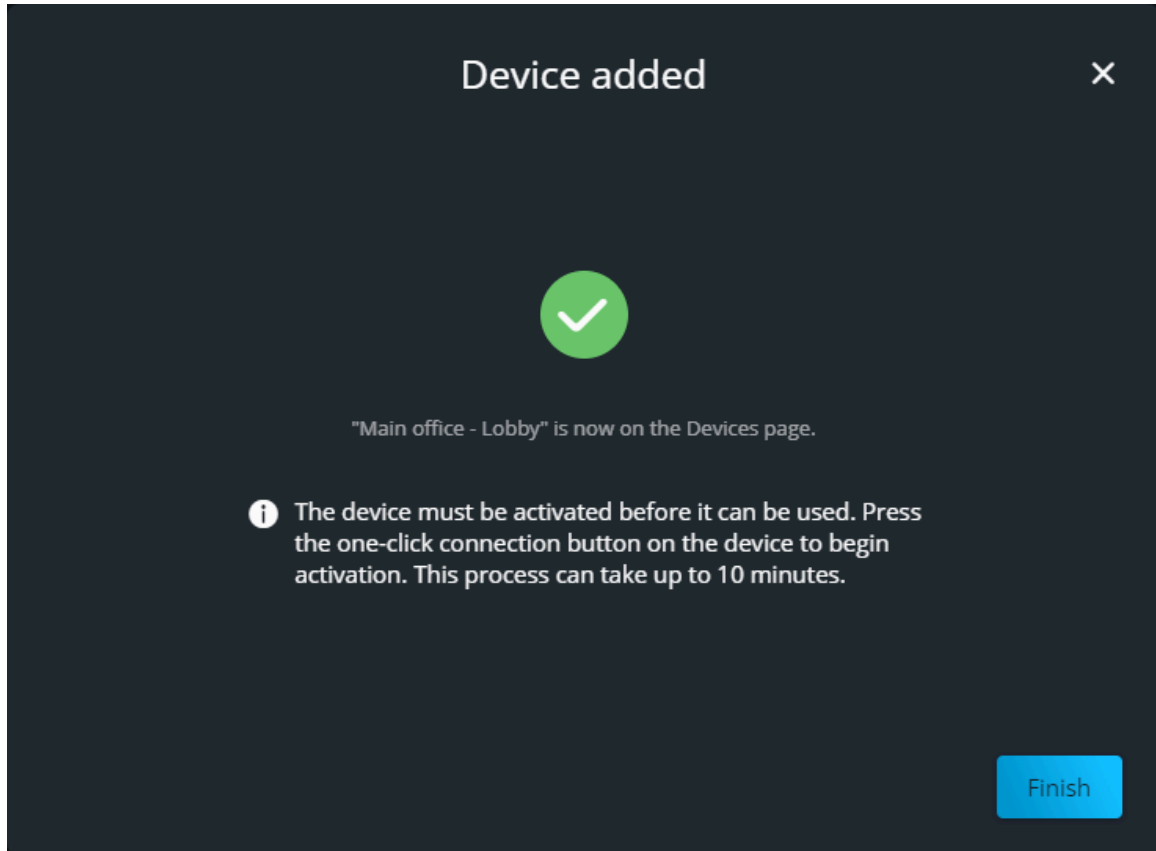
Owner Authentication Key (OAK)  
D2CG-RR63-9C59

**i** When added, a new username and password are automatically generated for the device. These credentials can be retrieved from the device details. All other users on the device will be deleted.

Continue

- 3 Click **Continue**.  
The camera is added to the device list.

- 4 In the *Device added* dialog box, read the instructions and click **Finish**.



- 5 If you have physical access to the camera, press the control button on the camera body. Activation can take up to 10 minutes. This activation process includes installing firmware, downloading application updates, and bringing the camera online. You can continue with other tasks while the device activation completes in the background.
- 6 If you don't have physical access to the camera, enable the one-click cloud connection in software:
- a) On the camera's web page, click **System > Network**.
  - b) Under *One-click cloud connection*, set **Allow O3C** to *Always* and click **Save**.
- The camera is now available in Security Center SaaS.


### After you finish



- To configure basic camera settings, select the device and click the *Settings* tab in the side pane.


- If you need to change camera settings that aren't available in Genetec Configuration, sign in to the device. To obtain the camera credentials, select the device and click **View credentials** on the *Overview* page of the device side pane.


### View credentials ×

Device  
**Main office - Lobby**

Username  
**AMgenetec** 

Password  
.....  

 To access the web interface, your workstation must be connected to the same network as the device.

[Open web interface](#)  Close

# Adding Axis Powered by Genetec devices

---

After unpacking and connecting the Axis Powered by Genetec device to your company LAN, you must add the device to Security Center SaaS before it can be used.

## Before you begin

Have your device serial number and Owner Authentication Key (OAK) ready. You find this information on the *Axis Communications: Owner Authentication Key* document included in the device packaging.

## What you should know

Enrolling an Axis Powered by Genetec device in Security Center SaaS automatically does two things:

- Upgrades the device firmware to the latest version.  
Security Center SaaS ensures that all your devices are running the latest firmware, when it becomes available.
- Generates a username and password for the device and deletes all previous credentials.  
Security Center SaaS manages passwords for you, ensuring that all your devices are protected by strong passwords.

## Procedure

- 1 From the *Devices* page in Genetec™ Configuration web, click **Add device** and click **Use device information**.



- 2 In the *Add device* dialog box, click **Serial number + Owner Authentication Key (OAK)** and enter the required information:
  - **Name:** Enter a descriptive name for the device.
  - **Serial number:** Enter the device serial number.
  - **Owner Authentication Key (OAK):** Enter the Axis OAK.

← Add device X

**i** When added, a new username and password are automatically generated for the device. These credentials can be retrieved from the device details. All other users on the device will be deleted.

Name  
Main entrance

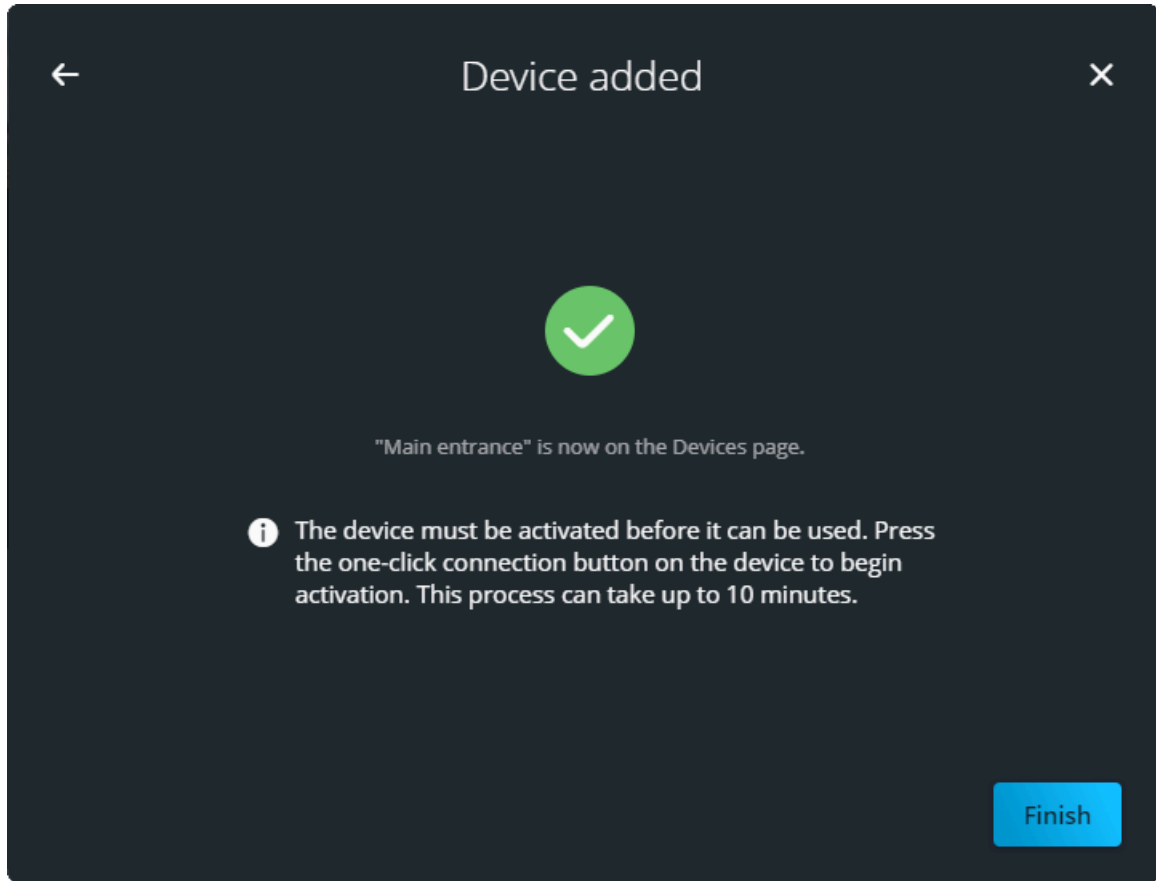
Serial number  
B8A44F6D82BA

Owner Authentication Key (OAK)  
3EFC-D4E5-978D

Continue

- 3 Click **Continue**.  
The device is added.

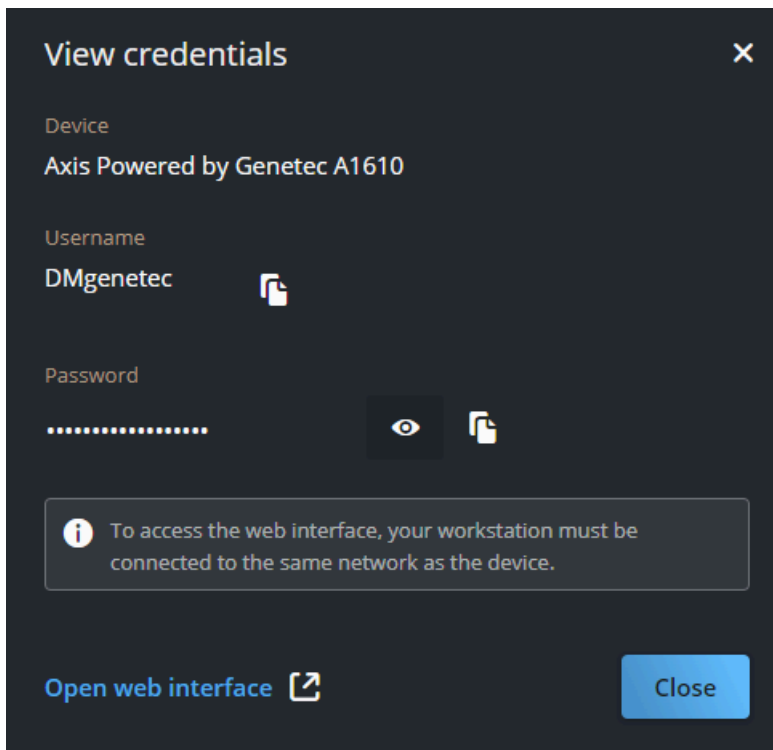
- 4 In the *Device added* dialog box, read the instructions and click **Finish**.



The device is added to the device list with the **Device type** indicating *Unknown* and the **Status** indicating *Action required*.

- 5 Open the casing of your Axis Powered by Genetec device and press the control button to begin activation. Activation can take up to 15 minutes. The device is ready for use when its **Status** is *Online*.

- 6 To view the device credentials, select the device and click **View** credentials the *Overview* page of the device side pane.



Click  to view the password.

**NOTE:** The **Open web interface** shortcut only works when you're connected to the same local network as the device.

## After you finish

If you need to change the default settings of the device, such as the reader and credential settings [sign in to the device](#). For information on how to configure the device, see the [Axis Powered by Genetec Help](#).

## Signing in to an Axis Powered by Genetec device

To configure an Axis Powered by Genetec door controller, you need to sign in to the AXIS device interface with a web browser.

### What you should know

- The AXIS device interface is the administrative web portal for the Axis Powered by Genetec device. For more information, see [The device interface](#) in the *Axis Powered by Genetec Help*.
- There are two ways to sign in:
  - If you have not enrolled the device in Security Center SaaS, sign in directly to the device using a web browser.
  - If you have enrolled the device in Security Center SaaS, sign in from the Genetec™ Configuration device overview panel.

### Procedure

**To sign in directly from a web browser:**

- 1 Open a web browser, and enter `https://` followed by the controller hostname or IP address.  
The Axis Powered by Genetec device is factory configured for DHCP. The default device hostname consists of `AXIS-`, followed by the device's MAC address. The MAC address is also the serial number. It can be found on a label at the bottom of the device or on the *Axis Communications: Owner Authentication Key* document included in the device packaging.  
**Example:** `https://AXIS-B8A44F6554C4`
- 2 (First sign in only) Set the default administrator user password.  
If it is your first sign in, or if you performed a factory reset, the default administrator username is `root` without password. You set the password the first time that you sign in. For more information, see [Set a new password for the root account](#) in the *Axis Powered by Genetec Help*.  
**IMPORTANT:** After setting the password, wait 5 minutes for the Synergis™ Softwire app to initialize.
- 3 In the *Sign in* dialog box, enter the username and password, and then click **Sign in**.  
The AXIS device interface opens on the *Status* page or the last page that you visited.

**To sign in from Genetec Configuration:**

- 1 From the device list, click the Axis Powered by Genetec device you want to connect to.
- 2 In the *Overview* panel, click **View credentials**.  
The *View credentials* dialog box opens.

**View credentials** [X]

Device  
Axis Powered by Genetec A1610

Username  
DMgenetec [Copy]

Password  
..... [Eye] [Copy]

**i** To access the web interface, your workstation must be connected to the same network as the device.

[Open web interface](#) [External Link] **Close**

- 3 Click **Open web interface**.  
A new browser page named AXIS opens with the *Sign in* dialog box.
- 4 Copy and paste the **Username** and **Password** from the *View credentials* dialog box to the *Sign in* dialog box, and click **Sign in**.  
The AXIS device interface opens on the *Status* page.

# Adding Genetec Cloudlink 310 appliances

---

After starting Genetec Cloudlink™ 310 and connecting the appliance for the first time, you must add the appliance to Security Center SaaS before it can be used.

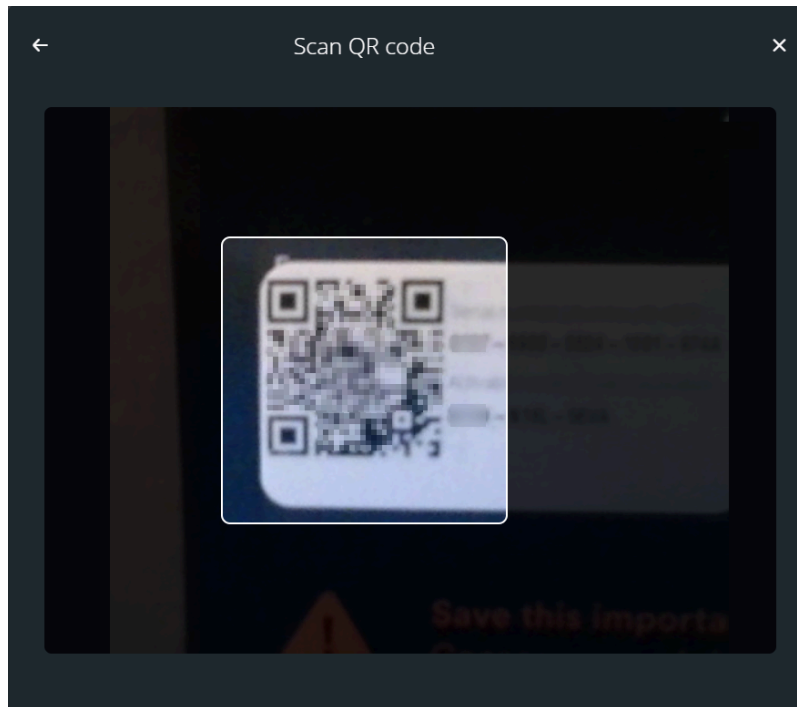
## Before you begin

- If required, [apply a static IP configuration to the appliance](#).
- Have the device QR code or serial number and activation code ready. You can find this information on the *Add this appliance to Security Center SaaS* insert card that is included with the appliance.

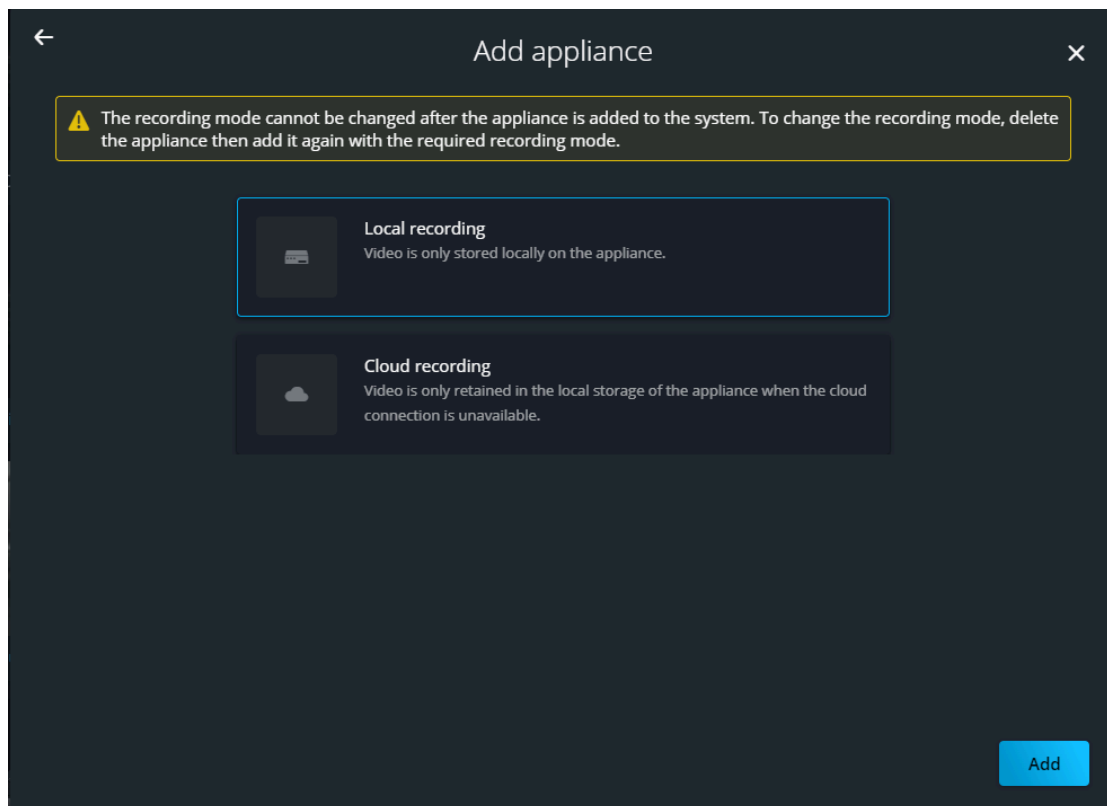
## Procedure

- 1 From the *Devices* page in Genetec™ Configuration web, click **Add device**.
- 2 Do one of the following:
  - Click **Scan QR code** to add the appliance using a QR code.
  - Click **Use device information** to add the appliance using the serial number and activation code.

- 3 If you selected **Scan QR code**:
- a) If required, allow or enable camera access in your web browser.
  - b) Position the QR code in front of your camera.



- c) In the *Add appliance* dialog, select a recording mode.



- d) Click **Add**, then click **Finish**.

The initial setup can take a few minutes. During this time, the device shows *Connecting* while the required applications are downloaded and installed.

**TIP:** Select the device tile to display status information.

4 If you selected **Use device information**:

- a) Click **Serial number + Activation code**.
- b) Enter the serial number and activation code.
- c) Click **Add**, then click **Finish**.

The initial setup can take a few minutes. During this time, the device shows *Connecting* while the required applications are downloaded and installed.

**TIP:** Select the device tile to display status information.

The Genetec Cloudlink 310 is now available in Security Center SaaS.

## After you finish

- [Add local cameras using automatic discovery](#).
- [Add local cameras manually](#).

## Applying a static IP configuration to Genetec Cloudlink 310

If DHCP is not available on your network, you must apply a static IP configuration to Genetec Cloudlink™ 310 before it can be used.

### Before you begin

**BEST PRACTICE:** Set up Genetec Cloudlink 310 in a pre-deployment environment with DHCP and Universal Plug and Play (UPnP) enabled.

### What you should know

By default, Genetec Cloudlink 310 uses DHCP to obtain an IP address and is discoverable by UPnP. If an IP address cannot be obtained from DHCP, the appliance automatically falls back to a link-local address in the range of *169.254.0.0/16*.

To retrieve the IP address, you can use network discovery or connect a monitor to the unit.

### Procedure

- 1 On a computer connected to the same subnet, open a web browser and connect to <https://<appliance>>, where *<appliance>* is the hostname or IP address of your unit.

The default hostname is printed on the unit label beside *Nom/Name*.

**NOTE:** Genetec Cloudlink 310 uses a self-signed certificate. When connecting to the unit, the browser might warn you that the connection is unsafe. If you get this warning message, ignore it and proceed with the connection.

The appliance web page opens.

- 2 Enter the username "admin" and your password, and then click **Connect**.

If you are connecting to the appliance for the first time, the default password is printed on the unit label beside *PWD*. You will be asked to change this password after logging on.

- 3 From the Genetec Cloudlink 310 homepage, click the **Settings** tab.

- 4 Under *Interfaces*, select **Static**, and input the network configuration.

The following values are required:

- IP Address
- Subnet Mask
- Default Gateway
- DNS Settings

**NOTE:** To add name servers and search domains, you must click **Add** after each entry.

- 5 Click **Save**.

The static IP configuration is applied. You might not be able to reconnect to the unit before moving it to the required location.

## After you finish

The Genetec Cloudlink 310 appliance is now ready for deployment in your static IP network.

## Adding cameras to Genetec Cloudlink 310 using automatic discovery

Use automatic discovery to add cameras on the local network to the Genetec Cloudlink™ 310 appliance in Security Center SaaS.

### Before you begin

- Ensure that the Cloudlink 310 is online.
- Have the camera username and password ready.
- Ensure that WS-Discovery is enabled on the camera and that discovery is allowed on the local network.

### What you should know

- Cameras must be on the same subnet as a Cloudlink 310 appliance.
- You can only add one camera at a time.
- Only Axis or ONVIF-compliant cameras are currently supported.

### Procedure

- 1 From the *Devices* page in Genetec™ Configuration web, click **Add device**.

The system searches for cameras automatically. A list shows discovered cameras that aren't in the system.

**IMPORTANT:** Automatic discovery might detect cameras that aren't officially supported in Security Center SaaS.

For supported devices and firmware, see [Supported Device List](#) and [Security Center SaaS Device Compatibility Guidelines](#).

- 2 Click **Add** next to the required camera.

**TIP:** If the list is long, you can search for a camera by name or IP address.

If the required camera wasn't discovered, you can try to [add the camera manually](#).

- 3 In the **Add camera** dialog, enter the required information, and click **Add**.

The camera is added. You can close the dialog and perform other tasks while the camera is connecting.

## After you finish

- To configure basic camera settings, select the device and click the *Settings* tab in the side pane.



- If you need to change any camera settings that aren't available in Genetec Configuration, sign in to the device.

## Adding cameras to Genetec Cloudlink 310 manually

If automatic discovery doesn't work or isn't available, you must add cameras to Genetec Cloudlink™ 310 manually in Security Center SaaS.

### Before you begin

- Ensure that the Cloudlink 310 is online.
- Have the camera IP address, username, and password ready.

### What you should know

- Cameras must be on the same subnet as the associated Cloudlink 310 appliance.
- Only Axis or ONVIF-compliant cameras are currently supported.

### Procedure

- 1 From the *Devices* page in Genetec™ Configuration web, click **Add device**.
- 2 In the *Searching for cameras* dialog, click **Use device information**.
- 3 In the *Add device* dialog, click **IP address, username, and password**.
- 4 Enter the required information and click **Continue**.  
The camera is added.
- 5 Click **Finish**.

### After you finish

- To configure basic camera settings, select the device and click the *Settings* tab in the side pane.
- If you need to change any camera settings that aren't available in Genetec Configuration, sign in to the device.

# Adding Synergis Cloud Link appliances

After you've connected to your Synergis™ Cloud Link appliance for the first time, add it to Security Center SaaS before using it.

## Before you begin

- Have the device QR code or serial number and activation code ready. You can find this information on the *Add this appliance to Security Center SaaS* insert card that is included with the appliance.
- If your Synergis Cloud Link unit was previously enrolled in an on-premises Security Center system or in a hosted Security Center SaaS Edition (Classic) system, do the following:
  1. [Upgrade your unit to Synergis Cloud Link 3.1.1 or later.](#)
  2. In the Synergis™ Appliance Portal, click **Configuration** > **Unit-wide parameters** and select the **Communicate with the cloud for enrollment** option.

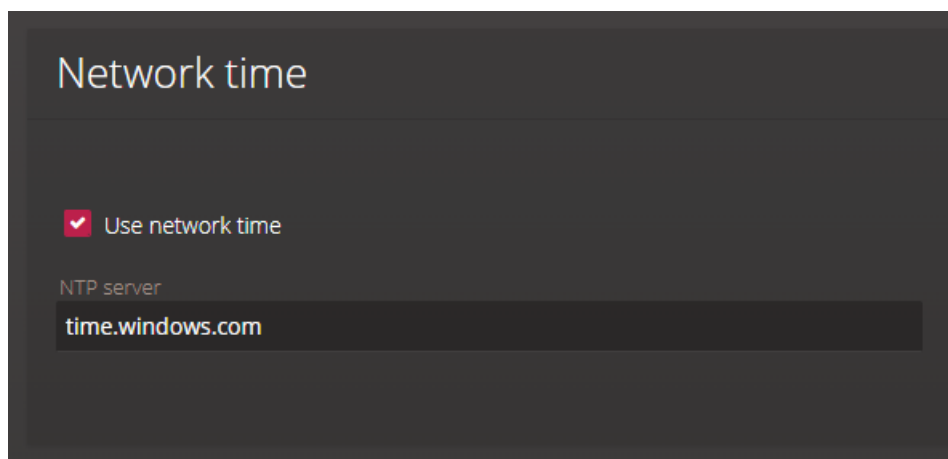
For more information, see [Configuring unit-wide parameters for Synergis Cloud Link units.](#)

## What you should know

For supported devices and firmware, see [Supported Device List](#) and [Security Center SaaS Device Compatibility Guidelines](#).

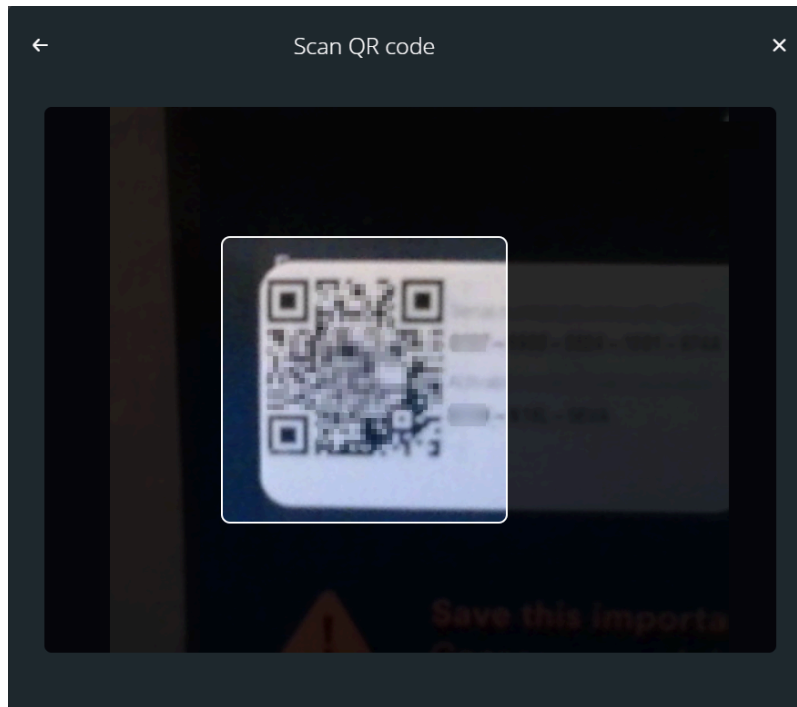
## Procedure

- 1 Configure the Network Time Protocol (NTP) server to avoid time differences for events or device synchronization issues.
  - a) In your web browser, enter `https://` followed by the Synergis™ appliance's hostname or IP address.  
**Example:** `https://SCLXXXXXXXXXXXX`, where XXXXXXXXXXXX represents the MAC address.
  - b) If you opened a new browser session to sign in to the Synergis appliance, you get a certificate error message. Follow your browser's on-screen instructions to continue to the website.
  - c) Enter the username and password, and then click **Log on**.
  - d) Click **Configuration** > **Network**.
  - e) In the *Network time* section, select **Use network time** and enter `time.windows.com`.



- 2 From the *Devices* page in Genetec™ Configuration web, click **Add device**.

- 3 Do one of the following:
  - Click **Scan QR code** to add the appliance using a QR code.
  - Click **Use device information** to add the appliance using the serial number and activation code.
- 4 If you selected **Scan QR code**:
  - a) If required, allow or enable camera access in your web browser.
  - b) Position the QR code in front of your camera.



- c) Click **Add**, then click **Finish**.  
 The initial setup can take a few minutes. During this time, the device shows *Connecting* while the required applications are downloaded and installed.  
**TIP:** Select the device tile to display status information.
- 5 If you selected **Use device information**:
  - a) Click **Serial number + Activation code**.
  - b) Enter the serial number and activation code.
  - c) Click **Add**, then click **Finish**.  
 The initial setup can take a few minutes. During this time, the device shows *Connecting* while the required applications are downloaded and installed.  
**TIP:** Select the device tile to display status information.

The Synergis Cloud Link is now available in Security Center SaaS.

## After you finish

Connect and configure interface modules.

## Related Topics

[Logging on to the Synergis appliance](#)

# How privacy protection works in Security Center SaaS

---

In Security Center SaaS, privacy protection anonymizes video by pixelating parts of a video stream where movement is detected. The identity of individuals or moving objects is protected, without obscuring movements and actions or preventing monitoring.

Privacy protection is a default feature in Security Center SaaS. This differs from enabling privacy protection in Security Center on-premises, which requires the installation and configuration of the KiwiVision™ Privacy Protector module.

## Activating privacy protection on cameras in Genetec Configuration

In Genetec Configuration, administrators can activate and deactivate privacy protection as needed on individual cameras.



To activate privacy protection:

1. On the *Devices* page, select a camera.
2. In the side pane of the camera, click the **Settings** tab.
3. Select the **Activate privacy protection** checkbox.

**NOTE:** Security Center SaaS only applies privacy protection to video streams displayed in a video tile. This uses fewer computing resources and less storage than KiwiVision™, which applies privacy protection to all video streams, even those that aren't displayed.

## Deactivating privacy protection on video streams

In Genetec Configuration and Genetec Operation, you can deactivate privacy protection in video tiles that are actively displaying live or playback video.

- **Genetec Configuration:** Click the privacy protection icon () in the video tile.
- **Genetec Operation:** Right-click on a video tile and select **Deactivate privacy protection**.
- **Genetec Operation web:** In the selected video tile, click **Show more** () and select **Deactivate privacy protection**.

**NOTE:** Deactivating privacy protection in a video tile doesn't change the privacy protection setting on the camera that provides the stream. If an operator deactivates privacy protection in a video tile, it remains active in all other video tiles.

## Privacy protection and video streaming

There are two types of streams related to privacy protection:

- **Public streams:** Contains privacy-protected content with video anonymization applied.
- **Private streams:** The original video stream from the video unit, where video isn't anonymized or masked.

Security Center SaaS only saves private streams. When users play back these streams, privacy protection is applied to video through Genetec™ Cloud Services. Security Center on-premises differs by saving private and public streams by default.

## Exported video

To apply privacy protection to exported video, the feature must be activated on the camera and enabled in the video tile when the operator exports the video.

If privacy protection is active on a camera, but inactive in the video tile when the operator exports the video, privacy protection isn't applied to exported video.

## Camera compatibility

Security Center SaaS doesn't support privacy protection on the following camera types:

- 360-degree fisheye cameras
- PTZ cameras

## Licensing

No additional license is required to activate privacy protection on cameras.

# Federation through reverse tunneling

This section includes the following topics:

- ["What is reverse tunneling"](#) on page 50
- ["Deploying Security Center Federation using reverse tunneling"](#) on page 52
- ["Creating reverse tunnels on the Federation host"](#) on page 53
- ["Opening reverse tunnels between remote sites and the Federation host"](#) on page 55
- ["Connecting the Federation host to remote sites through reverse tunnels"](#) on page 57
- ["Resetting reverse tunnels"](#) on page 59

# What is reverse tunneling

Reverse tunneling is a method of securing communication between clients and servers that are behind a firewall. This technique enhances security and simplifies firewall management. When using a reverse tunnel, the server initiates a connection to the client. This tunnel connection is secured by a previously shared keyfile that contains an identity certificate. When established, the reverse tunnel allows bidirectional communication without opening inbound firewall ports.

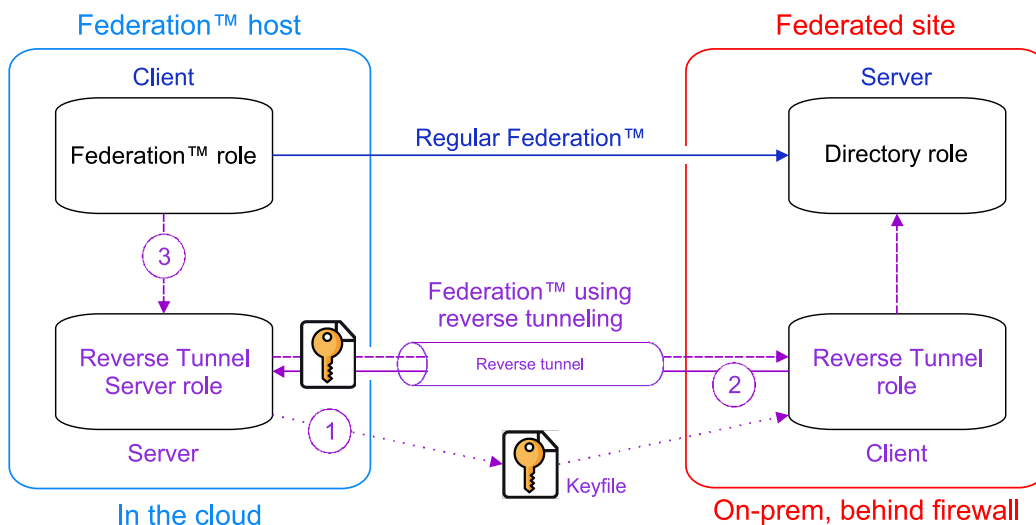
## Context

In Security Center SaaS, reverse tunneling is typically used to connect one or more remote Security Center systems to the Federation™ host in the cloud. Using a reverse tunnel simplifies the firewall management and configuration of Security Center Federation. By default, the tunnel uses outbound TCP 5500 to connect the remote site to the Federation host.

**NOTE:** If required, reverse tunneling can be used to connect Security Center SaaS to an external Federation host, such as a system on-premises, or Security Center SaaS Edition (Classic). For help setting up this configuration, contact the Genetec™ Technical Assistance Center (GTAC).

Regular Federation can be challenging to set up due to the number of ports required to connect the Federation host to the Security Center main server at the remote site. The following diagram shows the communication flow of a regular Federation, shown in blue, and a Federation over reverse tunnel, shown in purple.

In a regular Federation, the Federation host is the client that initiates a connection to federated site, which acts as a server. This flow is reversed in a Federation over reverse tunnel.



To use reverse tunneling, you must create a [Reverse Tunnel Server](#) role on the Federation host and a [Reverse Tunnel](#) role at the remote site. Reverse tunneling works as follows:

1. The Reverse Tunnel Server role generates a keyfile, which includes an identity certificate, network connectivity information, and a one-time use token.
2. The Reverse Tunnel role accepts the keyfile to open the reverse tunnel.
3. The Security Center Federation™ role connects to the federated site through the reverse tunnel.

## Limitations and requirements

- **Reverse tunneling only supports TCP:** The network segment used for tunneling between the remote site and the Federation host must support unicast TCP. After video reaches the cloud, the *Best available* transport protocol can be used.

- **Video streams must go through a redirector before and after the tunnel:** The tunneling mechanism is only implemented at the level of video redirectors, and is transparent to the client application.



# Deploying Security Center Federation using reverse tunneling

---

To deploy Security Center Federation™ using reverse tunneling, you must first create a reverse tunnel on the Federation host for each remote site. After creating the reverse tunnel, open it from the remote site before you federate it.

## Before you begin

Prepare the following:

- Names of remote sites to federate and the version of Security Center they are running.
- Credentials to sign in to the remote systems as the following Security Center users:
  - [The Federation user](#)
  - An administrator
- An external storage device to save the *tunnel keyfiles* created for the remote systems.
- The system that hosts the Reverse Tunnel Server role must be reachable from remote sites that can use DNS to resolve the server hostname.

## What you should know

If possible, use a workstation that can access the Federation host and remote sites.

## Procedure

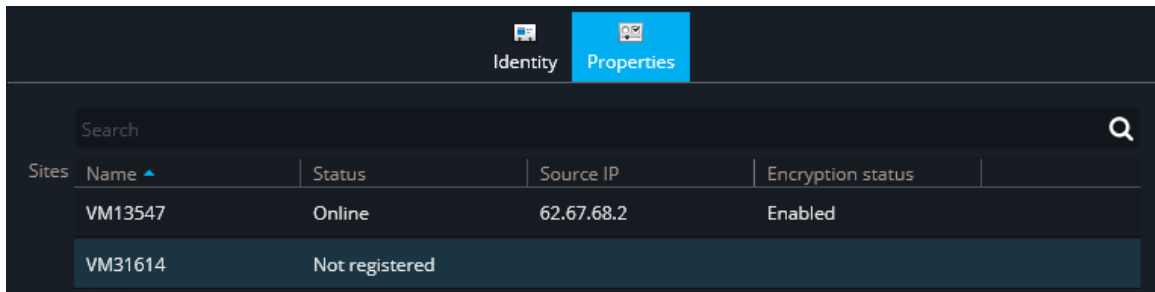
- 1 [Create reverse tunnels for each remote site on the Federation host.](#)
- 2 [Open the reverse tunnel between remote sites and the Federation host.](#)
- 3 [Connect the Federation host to remote sites through the reverse tunnel.](#)

## Creating reverse tunnels on the Federation host

To open a reverse tunnel between a remote site and the Federation™ host, you must first create a reverse tunnel for the remote site on the Federation host.

### Procedure

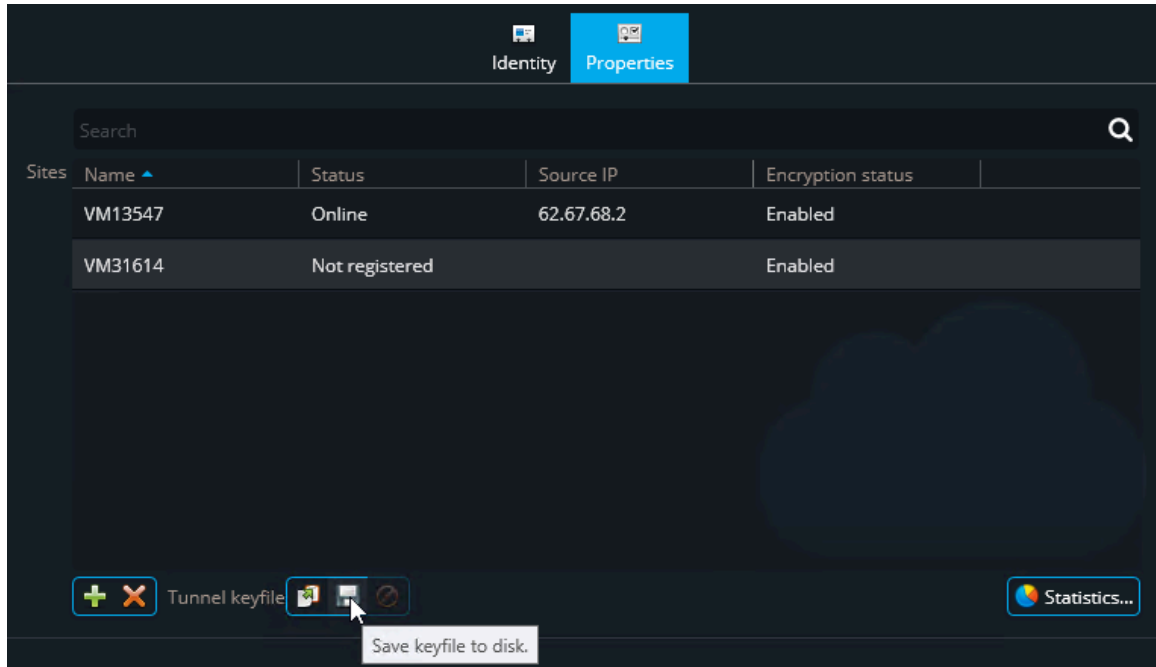
- 1 In Genetec™ Configuration desktop, sign in to the Federation host system.
- 2 Open the *System* task and click **Roles > Reverse Tunnel Server > Properties**.
- 3 At the bottom of the page, click **Add an item** (+).
- 4 In the **Name** field, enter a unique name to identify the remote site you want to federate and click **Add**.  
A reverse tunnel is created with the status *Not registered*.



Search				
Sites	Name ▲	Status	Source IP	Encryption status
	VM13547	Online	62.67.68.2	Enabled
	VM31614	Not registered		

- 5 Click **Apply**.  
By default, all reverse tunnels have encryption enabled. Video is encrypted while in transit from the remote site to the Federation host.  
**IMPORTANT:** Fusion stream encrypted video cannot be played back in Genetec™ Operation web and mobile.

6 Get the keyfile by doing one of the following:



- If your workstation can access the remote site, click **Copy keyfile to clipboard** (📄).
- If your workstation cannot access the remote site, click **Save keyfile to disk** (💾), and specify the file location.

A file named <SiteName>.keyfile is saved to the folder that you select.

7 Click **Apply**.

## After you finish

Open the tunnel from the remote site using the tunnel keyfile.

# Opening reverse tunnels between remote sites and the Federation host

To establish a reverse tunnel connection between a remote site and the Federation™ host, you must open the tunnel from the remote site.

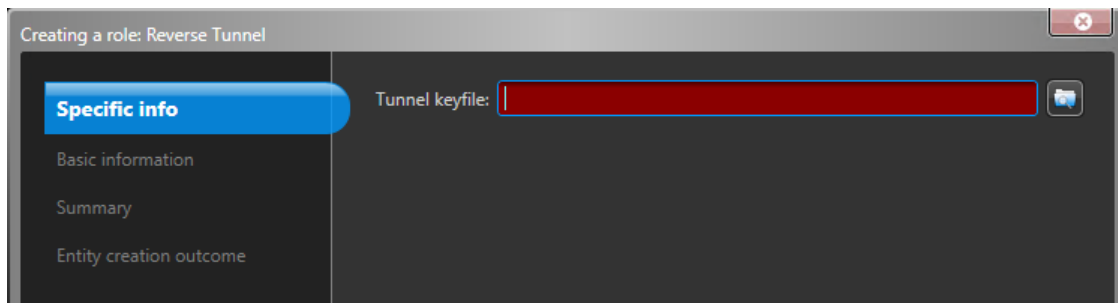
## Before you begin

Create a reverse tunnel on the Federation host and generate a tunnel keyfile.

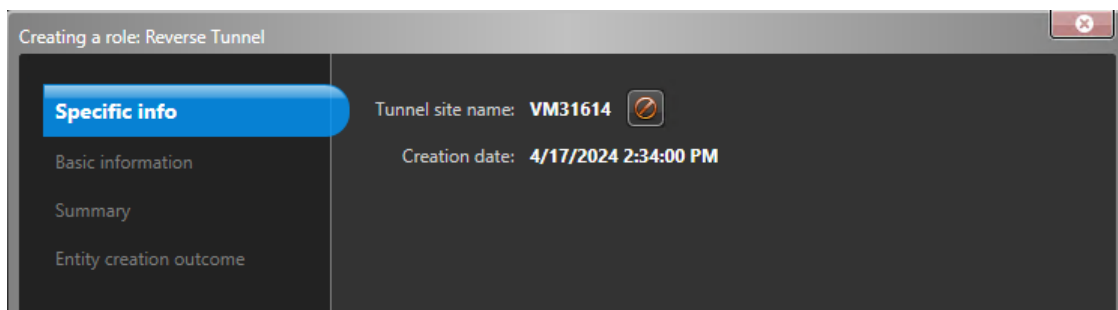
**NOTE:** For security reasons, a keyfile can only be used once.

## Procedure

- 1 In Config Tool, sign in to the remote system.
- 2 Open the *System* task, and click the **Roles** view.
- 3 Click **Add an entity > Reverse Tunnel**.
- 4 On the *Specific info* page, enter the keyfile for this tunnel.  
Do one of the following:
  - If the keyfile was copied to the clipboard, paste it into the **Tunnel keyfile** field.
  - Click **Select file** (📁), browse for the keyfile, and click **Open**.



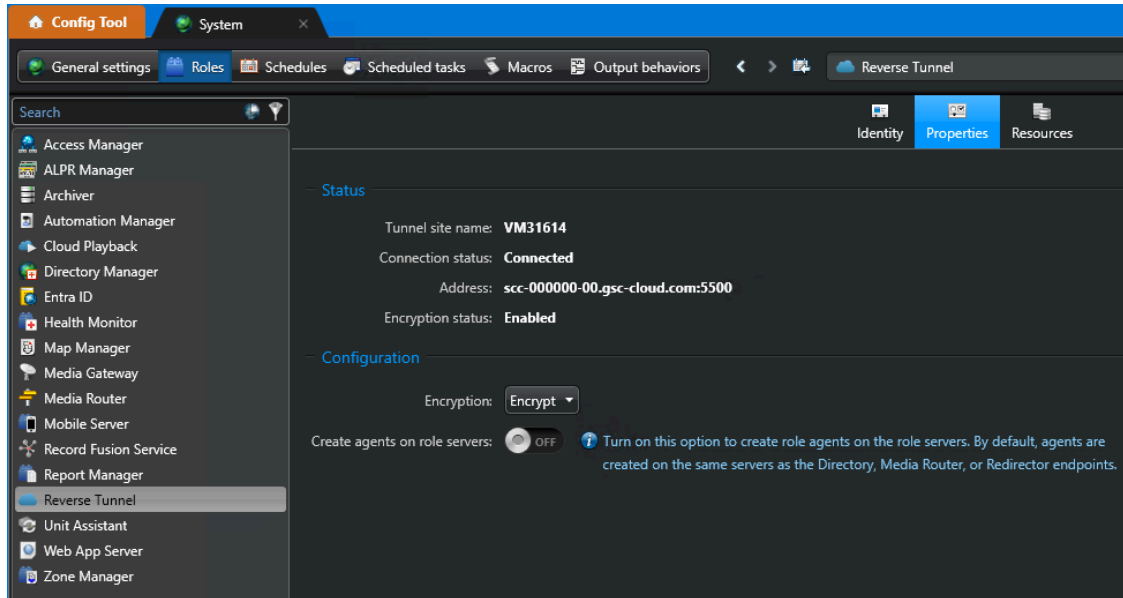
The tunnel site name and the time it was created are displayed.



- 5 Confirm that you have the correct name and click **Next**.  
If you used the wrong keyfile, click **Clear** (🗑️) and try again.
- 6 (Optional) Enter the role name and description.  
The default role name is Reverse Tunnel1. If multiple hosts federate this site, choose a different name for each host.

7 Click **Next** > **Create** > **Close**.

The Reverse Tunnel role is created. It takes a few seconds for the role to connect to the Reverse Tunnel Server role on the Federation host.

8 (Optional) Click the **Properties** tab and select an **Encryption** option.

**IMPORTANT:** By default, connections to a Security Center SaaS Federation host require encryption.

- **Encrypt:** Encrypt video in transit from the remote site to the Federation host.
- **Prefer encryption:** Encrypt video in transit if both the remote site and the Federation host support TLS. Use this option if you are not certain of the capabilities of the Federation host.
- **Do not encrypt:** Do not encrypt video in transit. Only use this option if the video is encrypted through other methods.

9 (Optional) Turn on the **Create agents on role servers** option.

By default, servers hosting Directory, Media Router, and Redirector roles all require internet access for reverse tunneling.

When this option is enabled, only servers listed on the *Resources* need outbound internet access for reverse tunneling.

10 (Optional) Click the **Resources** tab and configure failover for the Reverse Tunnel role.

For information about role failover, see [Setting up role failover](#) on the TechDoc Hub.

## After you finish

1. [Sign in to the Federation host](#) and confirm that the status of the remote site is **Online**.
2. [Connect the Federation host to the remote site through the reverse tunnel](#).

# Connecting the Federation host to remote sites through reverse tunnels

To connect the Security Center SaaS Federation™ host to a remote site using reverse tunneling, you must follow a specific pattern for the Directory name while configuring the Security Center Federation™ role.

## Before you begin

[Open a reverse tunnel on a remote site.](#)

## What you should know

In Security Center SaaS, the Security Center Federation roles necessary to federate your remote systems are created for you. Configure these roles to connect to your remote systems with the required options.

## Procedure

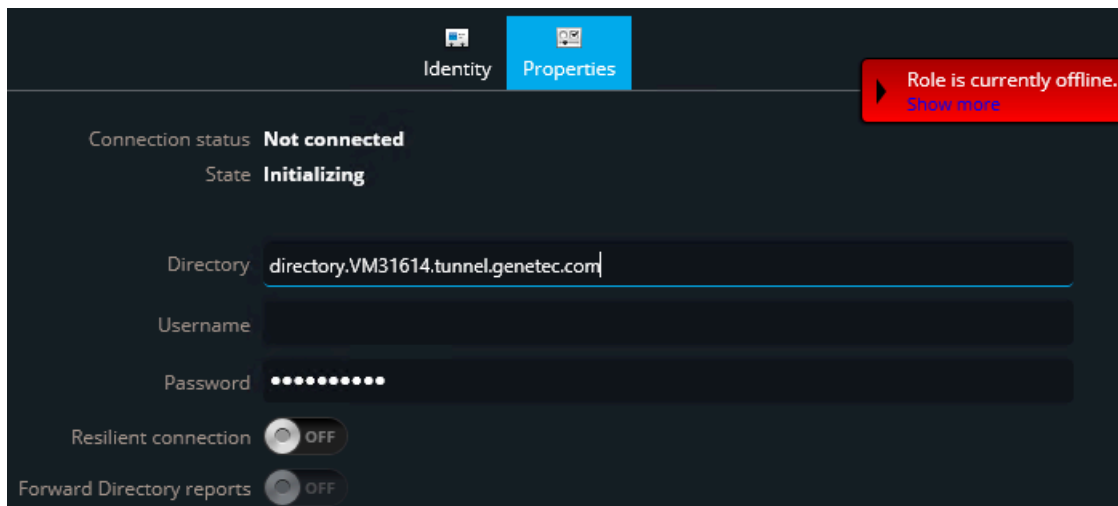
- 1 In Genetec™ Configuration desktop, sign in to your Security Center SaaS system.
- 2 Open the *System* task and click the **Roles** view.
- 3 If required, do the following:
  - a) In the entity tree, select an *UnconfiguredFederation* and activate the role.
  - b) On the **Identity** tab, enter a new name and description for this Federation.
- 4 Select a Security Center Federation role (🌐), click the **Properties** tab, and enter the reverse tunnel name in the **Directory** field.

The reverse tunnel name is formatted as: `directory.<sitename>.tunnel.genetec.com`, where `<sitename>` is the name for the remote site in the Reverse Tunnel Server role.

For example, if the remote site is named VM31614, enter:

`directory.VM31614.tunnel.genetec.com`

The string is not case-sensitive.



## 5 Configure the other Federation role settings as needed:

- **Username and password:** Credentials used by the Federation role to sign in to the remote Security Center system. The rights and privileges of that user determine what your local users can see and do on the federated remote system.
- **Resilient connection:** Turn this option on to automatically attempt to reconnect the Federation role to the remote site if the connection is interrupted. If the role has been unable to reconnect by the **Reconnection timeout**, the connection is considered lost and the role goes into a warning state.  
**NOTE:** Activating Resilient connection is highly recommended for remote systems that might have an unstable connection to the cloud.
- **Reconnection timeout:** The number of seconds that the Federation role attempts to reconnect to the Directory before the connection is considered lost.
- **Forward Directory reports:** Turn this option on to view user activities and configuration changes performed at the federated site. User activities include viewing cameras, activating the PTZ, and so on. This information is provided by the *Activity trails* and *Audit trails* reports on the Federation™ host, if the Federation™ user has the privileges and access rights to view them. You can also view the federated units in the *Hardware inventory* task.
- **Default live stream:** The default video stream that is used for live video from federated cameras. **Remote** is selected by default.

If your workstation does not require specific video stream settings for Federation™, you can use the default stream settings from Genetec™ Operation instead.

- **Enable playback requests:** Turn this option on for users to view playback video from federated cameras.
- **Federate alarms:** Turn this option on for users to receive alarms from the federated system.
- **Federate custom icons:** Turn this option on for federated entities to share custom icons with the Federation host. This means that entity icons in the Federation host appear identical to the federated system. It can take a few minutes to synchronize custom icons.
- **Federated events:** Select events to receive from the federated system. Events are necessary if you plan to monitor federated entities in Genetec Operation, or to configure event-to-actions for the federated entities.

6 Click **Apply**.

The Federation role is configured.

The connection status should say *Synchronizing entities*, or *Connected*.

7 After the role successfully connects to the remote system, open the *Area view* task.

## 8 Expand the Federation role in the Area view and verify that all federated entities were successfully imported.

The entity hierarchy corresponds to the Area view on the federated system.

**NOTE:** It can take up to an hour after synchronizing a new role for video to work.

## Resetting reverse tunnels

---


If the identity certificate of the Federation™ host or remote site is modified while the reverse tunnel is disconnected, you must reset the tunnel by generating and applying a new keyfile.



### What you should know

For security reasons, a reverse tunnel keyfile can only be used once. The tunnel keyfile is only needed to establish the first connection from the remote site to the host.

**NOTE:** A tunnel reset is not required if the Federation host certificate is replaced while the tunnel is connected. The new host certificate is propagated to the remote system automatically.

### Procedure

- 1 Generate a new keyfile on the Federation host:
    - a) In Genetec Configuration desktop, sign in to the Federation host system.
    - b) Open the *System* task and click **Roles > Reverse Tunnel Server > Properties**.
    - c) Select the site with the broken tunnel and click **Force re-enrollment of this site** (.
    - d) click **OK > Apply**.

The status of the site reverts to **Not registered**.
    - e) Get the keyfile by doing one of the following:
      - If your workstation can access the remote site, click **Copy keyfile to clipboard** (.
      - If your workstation cannot access the remote site, click **Save keyfile to disk** () and specify the file location.
- A file named `<SiteName>.keyfile` is saved to the folder that you select.



## 2 Apply the new keyfile to the remote site:

- a) In Config Tool, sign in to the remote system.
- b) Open the *System* task and click **Roles** > **Reverse Tunnel** > **Properties**.
- c) (Optional) Select an **Encryption** option.

**IMPORTANT:** By default, connections to a Security Center SaaS Federation host require encryption.

- **Encrypt:** Encrypt video in transit from the remote site to the Federation host.
- **Prefer encryption:** Encrypt video in transit if both the remote site and the Federation host support TLS. Use this option if you are not certain of the capabilities of the Federation host.
- **Do not encrypt:** Do not encrypt video in transit. Only use this option if the video is encrypted through other methods.

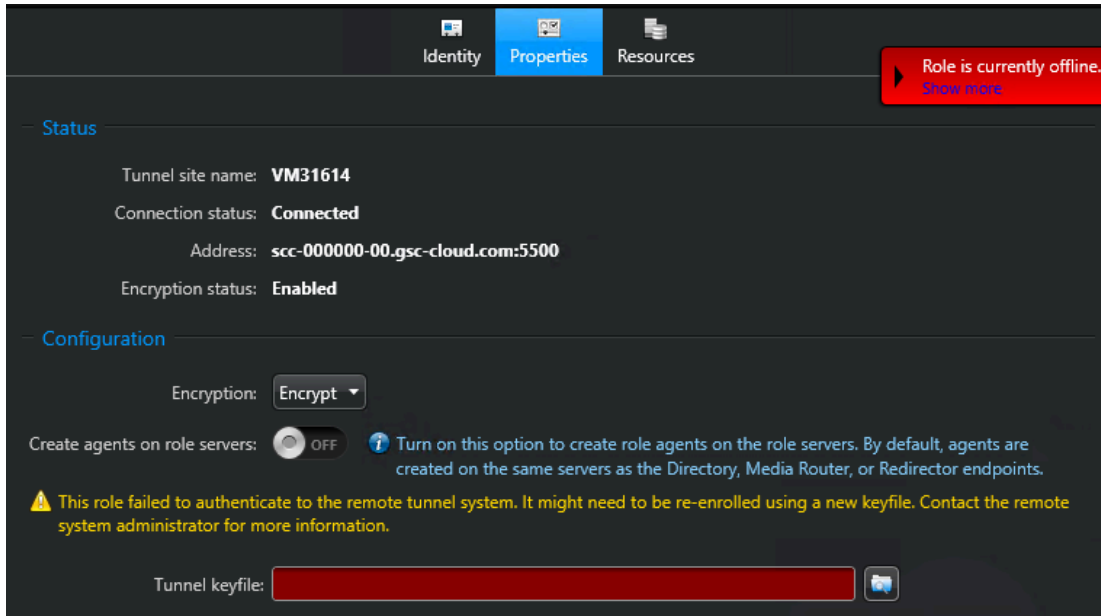
d) (Optional) Turn on the **Create agents on role servers** option.

By default, servers hosting Directory, Media Router, and Redirector roles all require internet access for reverse tunneling.

When this option is enabled, only servers listed on the *Resources* need outbound internet access for reverse tunneling.

## e) Enter the keyfile by doing one of the following:

- If the keyfile was copied to the clipboard, paste it into the **Tunnel keyfile** field.
- Click **Select file** (📎), browse for the keyfile, and click **Open**.

3 Click **Apply**.

The **Connection status** changes to **Connected**.

**After you finish**

[Sign in to the Federation host](#) and confirm that the status of the remote site is **Online**.

# Glossary

## Access control

The *Access control* task is the administration task for configuring your access control entities, which include roles, units, cardholders, credentials, and access rules.

## access rule

An access rule entity defines a list of cardholders to whom access is either granted or denied based on a schedule. Access rules can be applied to secured areas and doors for entries and exits, or to intrusion detection areas for arming and disarming.

## active alarm

An active alarm is an alarm that has not yet been acknowledged.

## alarm

An alarm entity informs users of a situation that requires immediate attention and provides details on how it can be handled in Security Center. For example, an alarm can indicate which entities (usually cameras and doors) best describe the situation, who must be notified, how it must be displayed to the user, and so on.

## alarm acknowledgment

An alarm acknowledgment is the final user response to an alarm that ends its lifecycle and removes it from the active alarm list.

## antipassback

Antipassback is an access restriction placed on a secured area that prevents a cardholder from entering an area that they have not yet exited from, and vice versa.

## bookmark

A bookmark is an indicator of an event or incident that is used to mark a specific point in time in a recorded video sequence. A bookmark also contains a short text description that can be used to search for and review the video sequences at a later time.

## camera

A camera entity represents a single video source in the system. The video source can either be an IP camera, or an analog camera that connects to the video encoder of a video unit. Multiple video streams can be generated from the same video source.

## cardholder

A cardholder entity represents a person who can enter and exit secured areas by virtue of their credentials (typically access cards) and whose activities can be tracked.

## cardholder group

A cardholder group is an entity that defines the common access rights of a group of cardholders.

## Config Tool

Config Tool is the Security Center administrative application used to manage all Security Center users and to configure all Security Center entities such as areas, cameras, doors, schedules, cardholders, patrol vehicles, ALPR units, and hardware devices.

## credential

A credential entity represents a proximity card, a biometrics template, or a PIN required to gain access to a secured area. A credential can only be assigned to one cardholder at a time.

## custom event

A custom event is an event added after the initial system installation. Events defined at system installation are called system events. Custom events can be user-defined or automatically added through plugin installations. Unlike system events, custom events can be renamed and deleted.

**door**

A door entity represents a physical barrier. Often, this is an actual door but it could also be a gate, a turnstile, or any other controllable barrier. Each door has two sides, named *In* and *Out* by default. Each side is an access point (entrance or exit) to a secured area.

**door contact**

A door contact monitors the state of a door, whether it is open or closed. It can also be used to detect an improper state, such as door open too long.

**door side**

Every door has two sides, named *In* and *Out* by default. Each side is an access point to an area. For example, passing through one side leads into an area, and passing through the other side leads out of that area. For the purposes of access management, the credentials that are required to pass through a door in one direction are not necessarily the same that are required to pass through in the opposite direction.

**entity**

An entity represents anything in your system that requires configuration. This can be a physical device, such as a camera or a door, or an abstract concept, such as an alarm, a schedule, a user, a role, a plugin, or an add-on.

**event**

An event is a record of an activity or incident that occurred in the system. Security personnel can monitor events in real time and investigate them later. Events can also trigger automations in the system.

**event-to-action**

An event-to-action links an action to an event. For example, you can configure an alarm to trigger when a door is forced open.

**failover**

Failover is a backup operational mode in which a role (system function) is automatically transferred from its primary server to a secondary server that is on standby. This transfer between servers occurs only if the primary server becomes unavailable, either through failure or through scheduled downtime.

**Federation™**

Federation™ joins multiple, independent Genetec™ security systems into a single virtual system. With this feature, users on a central system, called the Federation host, can view and control entities that belong to remote systems.

**Federation™ host**

The Federation™ host is the Security Center or Security Center SaaS system that runs Federation™ roles. Users on the Federation™ host can view entities that belong to federated systems and control the entities directly from their system.

**Genetec Configuration**

Genetec™ Configuration is the Security Center SaaS administrative application used to manage all Security Center SaaS users and to configure all Security Center SaaS entities such as areas, cameras, doors, schedules, cardholders, and hardware devices.

**Genetec Operation**

Genetec™ Operation is the unified user interface of Security Center SaaS. It provides consistent operator flow across all Security Center SaaS main systems. The unique task-based design of Genetec Operation lets operators efficiently control and monitor multiple security and public safety applications.

**identity provider**

An identity provider is a trusted, external system that administers user accounts, and is responsible for providing user authentication and identity information to relying applications over a distributed network.

**incident category**

An incident category is an entity that represents a grouping of incident types that have similar characteristics.

**map**

A map entity is a two-dimensional diagram that enables you to interact with your security equipment, while providing a reference to their physical locations and statuses.

**map link**

A map link is a map object that brings you to another map with a single click.

**map object**

Map objects graphically represent entities, cities, highways, and other geographical features on maps. Using map objects, you can interact with your system without leaving the map.

**map preset**

A map preset is a saved map view. Every map has at least one preset, called the *default view*, that is displayed when a user opens the map.

**Maps**

The *Maps* task is an operation task that heightens your situational awareness by providing the context of a map to your security monitoring and control activities.

**Media Router**

The Media Router is the central role that handles all audio and video stream requests in Security Center or Security Center SaaS. It establishes streaming sessions between the stream source, such as a camera or an Archiver role, and the client applications that request the sessions. The location and transmission capabilities of each party determine the routing decisions.

**People counting**

The *People counting* task is an operation task that keeps count in real-time of the number of cardholders in all secured areas of your system.

**privacy protection**

In Security Center, privacy protection is software that anonymizes or masks parts of a video stream where movement is detected. The identity of individuals or moving objects is protected, without obscuring movements and actions or preventing monitoring.

**redirector**

A redirector is a server assigned to host a redirector agent created by the Media Router role.

**redirector agent**

A redirector agent is an agent created by the Media Router role to redirect data streams from one IP endpoint to another.

**Reports**

The *Reports* task enables users to generate customized queries about entities, activities, and events for investigation or maintenance purposes.

**reverse tunnel**

A reverse tunnel is a private communication channel open between a server inside a secured LAN and a client outside. In the Security Center implementation, certificate authentication is used to protect against manipulator-in-the-middle attacks.

**Reverse Tunnel**

The Reverse Tunnel role is used on the federated system to connect to the Federation™ host residing in the cloud. The connection is established using a keyfile generated from the cloud system. The keyfile can only be used once to ensure maximum security.

**reverse tunneling**

Reverse tunneling is a method of securing communication between clients and servers that are behind a firewall. This technique enhances security and simplifies firewall management. When using a reverse tunnel, the server initiates a connection to the client. This tunnel connection is secured by a previously shared keyfile

that contains an identity certificate. When established, the reverse tunnel allows bidirectional communication without opening inbound firewall ports.

### **Reverse Tunnel Server**

The Reverse Tunnel Server role is used on the Federation™ host to manage reverse tunnels. Reverse tunnels are created using this role, but must be opened from the federated sites using the Reverse Tunnel roles.

### **role**

A role is a software component that performs a specific job within Security Center or Security Center SaaS.

### **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.

### **Security Center Federation™**

The Security Center Federation™ role connects the local system to an independent remote Security Center system. After connecting to the remote system, your local system acts as the Federation™ host and you can view federated entities and events locally.

### **Security Center SaaS**

Security Center SaaS is a unified hybrid-cloud solution offering physical security as a service. It integrates advanced security capabilities, emphasizes cybersecurity and privacy, and manages complex security tasks on premises, in the cloud, or both. With the flexibility of Security Center SaaS, organizations can efficiently monitor and respond to security threats from one place.

### **task**

A task is a customizable user interface designed to handle a specific aspect of your work. For example, you can employ a monitoring task to observe real-time system events, an investigation task to identify suspicious activity, or an administration task to configure system settings.

### **third-party authentication**

Third-party authentication uses a trusted, external identity provider to validate user credentials before granting access to one or more IT systems. The authentication process returns identifying information, such as a username and group membership, that is used to authorize or deny the requested access.

### **threat level**

A threat level warns system users of changing security conditions, such as a fire or a shooting, in a specific area or the entire system. Specific handling procedures can be automatically applied when a threat level is raised or canceled.

### **tile**

A tile is an individual window within the canvas, used to display a single entity. The entity displayed is typically the video from a camera, a map, or anything of a graphical nature. The look and feel of the tile depends on the displayed entity.

### **tile ID**

The tile ID is the number displayed at the upper left corner of the tile. This number uniquely identifies each tile within the canvas.

### **tile pattern**

The tile pattern is the arrangement of tiles within the canvas.

### **user**

A user entity is an account with access to the system. System administrators create user entities and configure their rights and privileges on the system.

**user group**

A user group is an entity that defines a group of users who share common properties and privileges. By becoming member of a group, a user automatically inherits all the properties of the group. A user can be a member of multiple user groups. User groups can also be nested.

**zone**

A zone is an entity that monitors a set of inputs and triggers events based on their combined states. These events can be used to control output relays.

# Technical support

Genetec™ Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a customer of Genetec Inc., you have access to TechDoc Hub, where you can find information and search for answers to your product questions.

- **Genetec TechDoc Hub:** Find articles, manuals, and videos that answer your questions or help you solve technical issues.

Before contacting GTAC or opening a support case, it is recommended to search TechDoc Hub for potential fixes, workarounds, or known issues.

To access the TechDoc Hub, log on to [Genetec Portal](#) and click [TechDoc Hub](#). Unable to find what you are looking for? Contact [documentation@genetec.com](mailto:documentation@genetec.com).

- **Genetec Technical Assistance Center (GTAC):** Contacting GTAC is described in the [Genetec Advantage Description](#).

## Technical training

In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to <http://www.genetec.com/support/training/training-calendar>.

## Hardware product issues and defects

Contact GTAC at <https://portal.genetec.com/support> to address any issue regarding Genetec appliances or any hardware purchased through Genetec Inc.