



Security Center Hardening Guide 5.10

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

Document last updated: October 12, 2021

Legal notices

©2021 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™, Community Connect™, Curb Sense™, Federation™, Flexreader™, Genetec Airport Sense™, Genetec Citigraf™, Genetec Clearance™, Genetec ClearID™, Genetec Mission Control™, Genetec Motoscan™, Genetec Patroller™, Genetec Retail Sense™, Genetec Traffic Sense™, KiwiVision™, KiwiSecurity™, Omnicast™, Privacy Protector™, Sipelia™, Stratocast™, Streamvault™, 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 Hardening Guide 5.10

Original document number: EN.501.003-V5.10.2.0(1)

Document number: EN.501.003-V5.10.2.0(1)

Document update date: October 12, 2021

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

About this guide

This guide outlines our recommended procedures to improve your system security.

The verification of the compliance for some of the items defined in this guide is implemented in the Security score widget in Security Center. For more information, see the *Security Center Administrator Guide*.

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: Introduction to the Security Center Hardening Guide

About hardening	2
What's new in Security Center Hardening Guide 5.10	3

Chapter 2: User Management

Changing the default administrator password in Security Center (Basic)	6
Enforcing strong passwords (Advanced)	7
Best practices for a strong password policy	7
Changing password settings for users	8
Setting passwords for Media Gateway RTSP streaming (Basic)	9
Using a local service account for Genetec™ Server (Basic)	12
Changing the default logon password for Security Center servers (Basic)	13
Changing the password for Security Center servers in Genetec™ Server Admin (Basic)	14
Activating auto lock on Security Desk workstations (Basic)	16
About configuring Federation™ users (Basic)	17
Using Windows Active Directory Integration (Advanced)	18
Using a third-party identity provider to authenticate a Security Center user (Advanced)	19
Deactivating all local users (Advanced)	20
Restricting Server Admin access to local connections (Advanced)	21
Restricting user privileges (Advanced)	22
Restricting client application connections to a specific Directory (Advanced)	25

Chapter 3: System

Using the recommended security settings in InstallShield (Basic)	27
Reviewing which data is collected for the Product Improvement Program (Basic)	28
Using trusted certificates on Security Center servers (Advanced)	30
Controlling access to your resources using partitions (Advanced)	32
Disabling backward compatibility (Advanced)	33
Disabling backward compatibility for the Map Manager role (Advanced)	34
Deactivating unused roles (Advanced)	35
Using a Directory gateway for external access to Security Center (Basic)	36
Running macros with limited access rights (Advanced)	38

Chapter 4: Genetec™ Update Service (GUS)

About keeping Security Center updated with Genetec™ Update Service (Basic)	40
Connecting to Genetec™ Update Service with Server Admin credentials (Basic)	41
Using a proxy server to connect Genetec™ Update Service to the internet (Basic)	42

Chapter 5: Video

Refusing basic authentication (Basic)	44
Enabling basic authentication (Basic)	44
Enabling secure communication in the Media Router (Basic)	46

Upgrading video unit firmware (Basic)	47
Ensuring that your cameras have strong administrator passwords (Basic)	49
Rotating your camera passwords periodically (Advanced)	50
Connecting to cameras through HTTPS (Advanced)	51
Encrypting data in transit and at rest with fusion stream encryption (Advanced)	52
Requesting and installing encryption certificates (Advanced)	52
Enabling fusion stream encryption (Advanced)	53
Deactivating unused services on video units (Advanced)	54

Chapter 6: Access Control

Using dedicated users with restricted privileges for connecting to Global Cardholder Synchronizer role (Basic)	56
Enabling Secure mode on HID units (Basic)	57
Using strong passwords on access control units (Basic)	58
Applying critical firmware updates to access control equipment (Basic)	59
Applying the latest cumulative security rollup available for Synergis™ units (Basic)	60
Using trusted certificates on Synergis™ units (Advanced)	61
Disabling the ability to drive output relays from the Synergis™ unit web interface (Basic)	64
Using secure reader connections (Basic)	65
Deactivating peer-to-peer and global antipassback for the Access Manager role (Basic)	66

Chapter 7: Logging

Logging Activity trails for security-related events (Basic)	68
---	----

Chapter 8: Web Server

Changing default Web Server ports (Basic)	70
Disabling unlimited session time in Security Center Web Server (Basic)	71
Installing a valid certificate on the Security Center Web Server (Advanced)	72

Chapter 9: Genetec™ Mobile

Changing the default Mobile Server port (Basic)	74
Always use trusted connections by enforcing certificate validity (Advanced)	75
Verifying the list of mobile devices connected to Security Center (Advanced)	76

Chapter 10: License Plate Recognition

Changing the default administrator password on a SharpV camera (Basic)	78
Encrypting the connection to the SharpV web portal (Basic)	79
Encrypting the connection to the SharpV web portal using a self-signed certificate (Basic)	79
Encrypting the connection to the SharpV web portal using a certificate issued by a trusted certificate authority (CA) (Basic)	81
Using the LPM protocol to connect SharpV cameras with Security Center (Basic)	83
Changing the default password of a SharpX unit (Basic)	85
Encrypting the connection to the SharpX web portal (Basic)	86
Encrypting the connection to the SharpX portal using a self-signed certificate (Basic)	86
Encrypting the connection to the SharpX portal using a certificate from a certificate authority (Basic)	86
Restricting access to the AutoVu™ root folder (Basic)	87
Using a network location for the AutoVu™ root folder (Advanced)	88
Encrypting communication between Genetec Patroller™ and Security Center (Basic)	89
Encrypting the Genetec Patroller™ database (Advanced)	91
Restricting access to the Genetec Patroller™ workstation (Basic)	92

Selecting a Genetec Patroller™ logon type (Basic)	93
Disabling Simple Host functionality in Genetec Patroller™ (6.5 SR1 and later) (Basic)	94
Chapter 11: Database	
About connecting to SQL Server with an account that has administrative privileges (Basic)	96
About the encryption of communication between databases and Genetec™ services (Basic)	99
About the encryption of database files (Advanced)	100
Authenticating database connections (Advanced)	101
Revoke permission to execute certain stored procedures (Advanced)	103
Chapter 12: Windows	
Synchronizing all clocks within your system (Advanced)	105
About running client applications without administrative privileges (Basic)	106
About Windows security baselines (Basic)	107
Using BitLocker full volume encryption (Advanced)	108
Using safe TLS versions (Advanced)	109
Glossary	110
Where to find product information	118
Technical support	119

Introduction to the Security Center Hardening Guide

This section includes the following topics:

- ["About hardening"](#) on page 2
- ["What's new in Security Center Hardening Guide 5.10"](#) on page 3

About hardening

Hardening is the process of enhancing hardware and software security. When hardening a system, basic and advanced security measures are put in place to achieve a more secure operating environment.

The Security Center default settings offer a balance between system security, usability, and performance. By hardening your system, you are optimizing it for more security, but potentially at the expense of some usability or performance. Hardening is an incremental process. How much you harden your security system depends on your threat model and the sensitivity of your information.

The *Security Center Hardening Guide* outlines our recommended procedures to improve your system security.

We define two levels of security in this guide:

- **Basic level:** Security measures for systems that require minimal security.
- **Advanced level:** Security measures that provide higher security, but are more complex, or take longer to implement. Organizations with strict security policies should adhere to this level. Advanced includes all basic level security measures.

To help you improve your system security and identify areas of concern, the *Security score* widget rates your adherence to the *Security Center Hardening Guide*.

What's new in Security Center Hardening Guide 5.10

The Security Center Hardening Guide 5.10 includes the following new enhancements.

New topics

- (Access Control) Applying critical firmware updates to access control equipment
- (Access Control) Applying the latest cumulative security rollup available for Synergis™ units
- (Access Control) Using dedicated users with restricted privileges for connecting to Global Cardholder Synchronizer role
- (Access Control) Using secure reader connections
- (User Management) Best practices for a strong password policy
- (User Management) Deactivating all local users
- (Video) Rotating your camera passwords periodically

Updated topics

- (General) Stopped referencing Basic and Advanced in the same topic. All Basic tasks are included in the Advanced level.
- (Access Control) About using Global Cardholder Synchronizer
Title changed to "Using dedicated users with restricted privileges for connecting to Global Cardholder Synchronizer role".
- (Access Control) Analyzing the strength of administrator passwords on HID controllers
Title changed to "Using strong passwords on access control units". Updated steps to combine verifying and changing passwords and added new images.
- (Access Control) Changing the default administrator password for the Synergis™ unit
Topic moved under "Using strong passwords on access control units".
- (Access Control) Enabling Secure mode on HID units.
Added content from "Enabling Secure mode when enrolling HID Units".
- (Access Control) Synchronizing the Synergis™ unit with the Access Manager
Topic moved under "Using strong passwords on access control units".
- (Access Control) Using certificates signed by a certificate authority on the Synergis™ unit
Title changed to "Using trusted certificates on Synergis™ units".
- (Access Control) Using strong passwords on access control units
Removed reference to invalid password length.
- (System) Disabling backward compatibility for the Map Manager role
Clarified that if backward compatibility is disabled, client applications that are unable to authenticate cannot view background images.
- (User Management) Enforcing strong passwords
Clarified definition for **Expiry notification period** and referenced the new best practices.
- (User Management) Setting passwords for Media Gateway RTSP streaming
Clarified RTSP security considerations and added information on RTSPS.
- (User Management) Using Windows Active Directory Integration
Referenced the new best practices for strong passwords.
- (Video) Connecting to cameras through HTTPS
Removed incomplete list of supported camera manufacturers.

- (Video) Encrypting data in transit and at rest with fusion stream encryption
Clarified fusion stream encryption as encryption in transit and at rest.
- (Video) Enabling fusion stream encryption
Fixed procedure to match UI and added clarifications.
- (Video) Refusing basic authentication
Fixed procedure to match UI.
- (Windows) About configuring Windows securely
Title changed to "About Windows security baselines". Updated with information on SCT and the latest security baselines.

Removed topics

- (Access Control) Enabling Secure mode when enrolling HID Units
Merged with "Enabling Secure mode on HID Units".
- (Access Control) Updating firmware on the Synergis™ appliance
Merged with "Applying the latest cumulative security rollup available for Synergis™ units".
- (Access Control) Applying a cumulative security rollup to a Synergis™ appliance through Synergis™ Appliance Portal
Merged with "Applying the latest cumulative security rollup available for Synergis™ units".
- (Access Control) Whitelisting your IP addresses
Obsolete.

User Management

This section includes the following topics:

- ["Changing the default administrator password in Security Center \(Basic\)"](#) on page 6
- ["Enforcing strong passwords \(Advanced\)"](#) on page 7
- ["Setting passwords for Media Gateway RTSP streaming \(Basic\)"](#) on page 9
- ["Using a local service account for Genetec™ Server \(Basic\)"](#) on page 12
- ["Changing the default logon password for Security Center servers \(Basic\)"](#) on page 13
- ["Activating auto lock on Security Desk workstations \(Basic\)"](#) on page 16
- ["About configuring Federation™ users \(Basic\)"](#) on page 17
- ["Using Windows Active Directory Integration \(Advanced\)"](#) on page 18
- ["Using a third-party identity provider to authenticate a Security Center user \(Advanced\)"](#) on page 19
- ["Deactivating all local users \(Advanced\)"](#) on page 20
- ["Restricting Server Admin access to local connections \(Advanced\)"](#) on page 21
- ["Restricting user privileges \(Advanced\)"](#) on page 22
- ["Restricting client application connections to a specific Directory \(Advanced\)"](#) on page 25

Changing the default administrator password in Security Center (Basic)

Security Center administrators must change the system's default administrator password to ensure its security.

What you should know

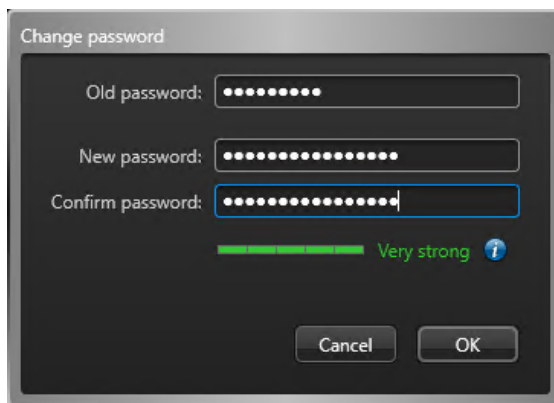
As a best practice, it is recommended to change your password regularly.

It is a best practice to only use passwords that are considered **Very strong** by the password strength meter in Security Center.

To change your Security Center administrator password:

- 1 From the Config Tool home page, click **About**.
- 2 In the *About* page, click **Change password**.
- 3 In the *Change password* dialog box, enter your old password.
- 4 Enter your new password and confirm it.

The password meter in the dialog box indicates your password's strength.



- 5 Click **OK**.

Enforcing strong passwords (Advanced)

To ensure your system's security, administrators must enforce a strong user password policy for every user account created in Security Center.

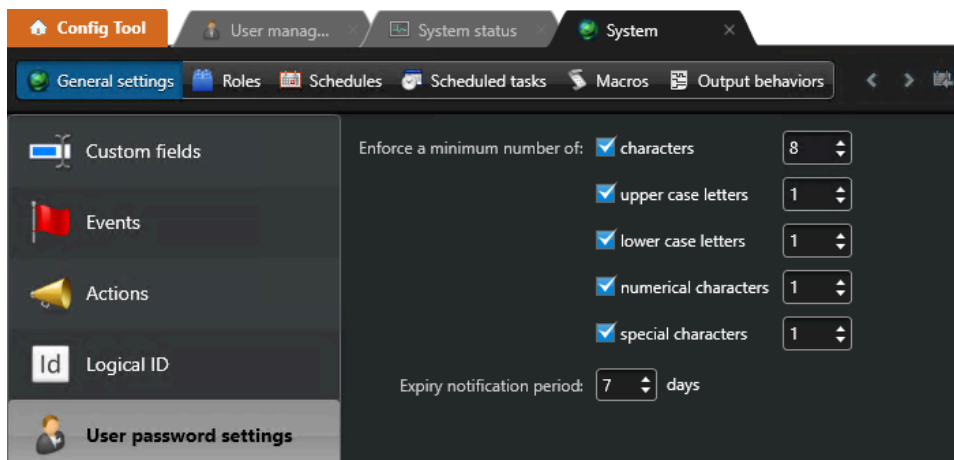
What you should know

A strong password policy aligns with the best practices published by the National Institute of Standards and Technology (NIST).

Password complexity requirements apply to all new passwords, and take effect when a user changes their current password.

To configure your password policy settings:

- 1 From the Config Tool home page, open the *System* task and click the **General settings** view.
- 2 Open the **User password settings** page.
- 3 Enter a value for each requirement in the **Enforce a minimum number of** section:
 - **Characters:** Minimum number of characters.
 - **Upper case letters:** Minimum number of upper case letters.
 - **Lower case letters:** Minimum number of lower case letters.
 - **Numerical characters:** Minimum amount of numbers.
 - **Special characters:** Minimum number of special characters.
 - **Expiry notification period:** Number of days before password expiry when the user is reminded to change their password.



- 4 Click **Apply**.

Best practices for a strong password policy

To ensure that your Security Center password policy follows established guidelines for computer security, it is highly recommended to align your policy with requirements published by the National Institute of Standards and Technology (NIST).

The NIST guidelines for password policies are available in [NIST Special Publication 800-63B "Digital Identity Guidelines: Authentication and Lifecycle Management"](#). This document is updated regularly as the recommendations evolve.

In the 03-02-2020 update, guidelines for passwords, or memorized secrets, have been greatly simplified and are summarized later in this section. Always refer to the NIST document for the latest information.

NIST guidelines for passwords:

- Passwords should be at least 8 characters long.
NOTE: We recommend passwords are at least 12 characters long.
- Besides length, no other complexity requirements, such as a minimum number of upper case, lower case, numeric, or special characters, should be imposed.
- No periodic password changes should be imposed. A password change should only be forced when there is evidence of compromise.

NIST no longer recommends enforcing complex passwords. Users often respond to composition rules in predictable ways, eliminating their benefit. Besides length, composition rules negatively impact usability while providing little or no improvement to password strength.

Changing password settings for users

You can set a user's password to expire after a certain amount of time, force users to change their password on next logon, or enforce a minimum complexity for all user passwords.

What you should know

Password complexity requirements apply to all new passwords, and take effect when a user changes their current password.

Only users who have the *Change own password* user privilege can change their own password. Otherwise, they must contact their administrator to change their password.

To change the password settings for a user:

- 1 From the Config Tool home page, open the *User management* task.
- 2 Select the user to configure, and click the **Properties** tab.
- 3 To change the user's password, click **Change password**, type a password, confirm the password, and click **OK**.
- 4 To set an expiry date for the user's password, switch the **Expires** option to **ON**, and select the number of days.
The system automatically warns users if their passwords are expiring soon, and gives them a chance to set a new password immediately. You can set the password expiry notification period to between 0 and 30 days from the System task.
- 5 To require the user to change their password the next time they log on to Genetec Patroller™ or Security Desk, switch the **Change on next logon** option to **ON**.
- 6 Click **Apply**.

Setting passwords for Media Gateway RTSP streaming (Basic)

To ensure restricted access to Media Gateway RTSP streams, administrators must set a strong password in the Media Gateway role for every authorized user account or enable RTSPS.

Before you begin

BEST PRACTICE: [Enforce a strong password policy in Security Center.](#)

What you should know

To prevent unauthorized access to Real Time Streaming Protocol (RTSP) video streams, we highly recommend enforcing user authentication for RTSP streaming. User authentication is required by default. When enabled, access to RTSP streams is granted by specifying authorized user accounts in the Media Gateway role.

IMPORTANT: RTSP communication is not secure. To protect Security Center credentials from exposure, a separate RTSP password is required for each specified user account.

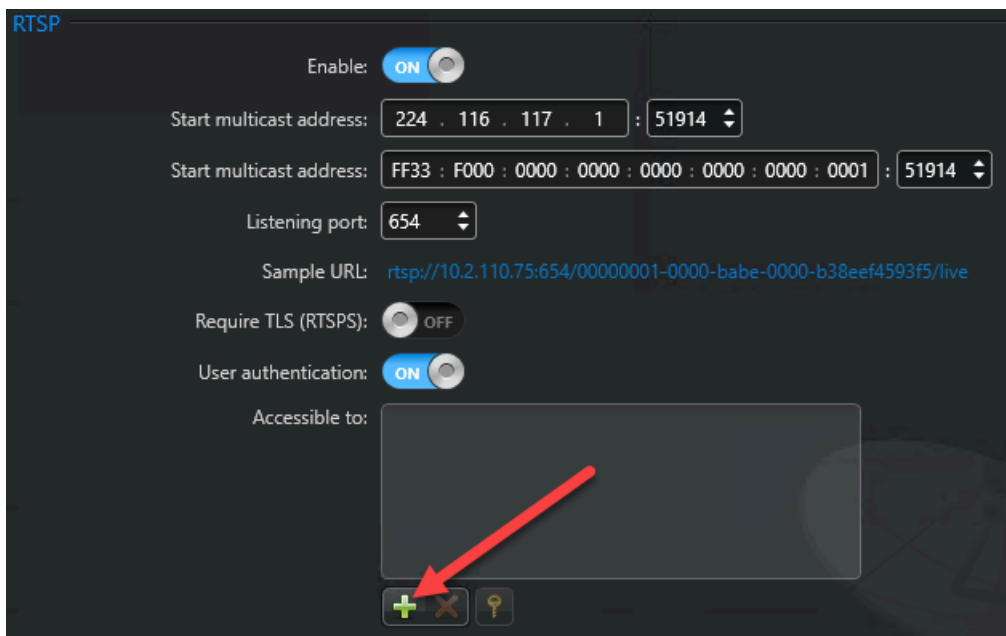
Password complexity requirements are enforced for RTSP passwords.

For enhanced security, Media Gateway offers RTSP streaming over TLS (RTSPS). With RTSPS, Security Center credentials are used to control access to video streams. RTSPS requires a player capable of decoding RTSP streams over TLS.

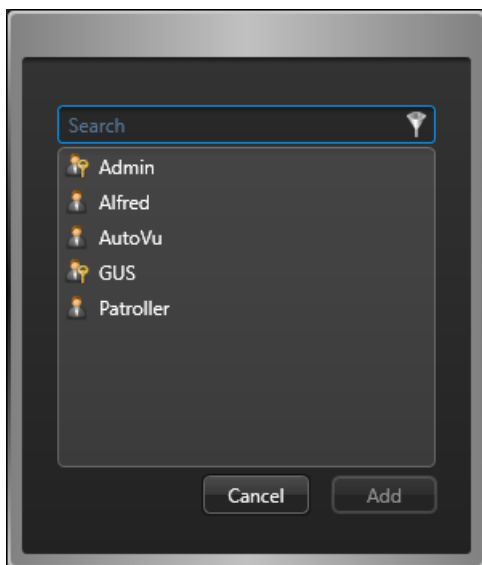
To set a password for Media Gateway RTSP streaming or enable RTSPS:

- 1 From the Config Tool home page, open the *System* task and click the **Roles** view.
- 2 Select the Media Gateway role and click the **Properties** tab.
- 3 If required, enable RTSP.
RTSP streaming is enabled. By default, **User authentication** is switched **ON**.

- 4 For unsecured RTSP streaming:
 - a) Under the *Accessible to* list, click **Add an item** (+) .



- b) Select a Security Center user to grant RTSP access and click **Add**.



The *New password* dialog box opens.



New password:

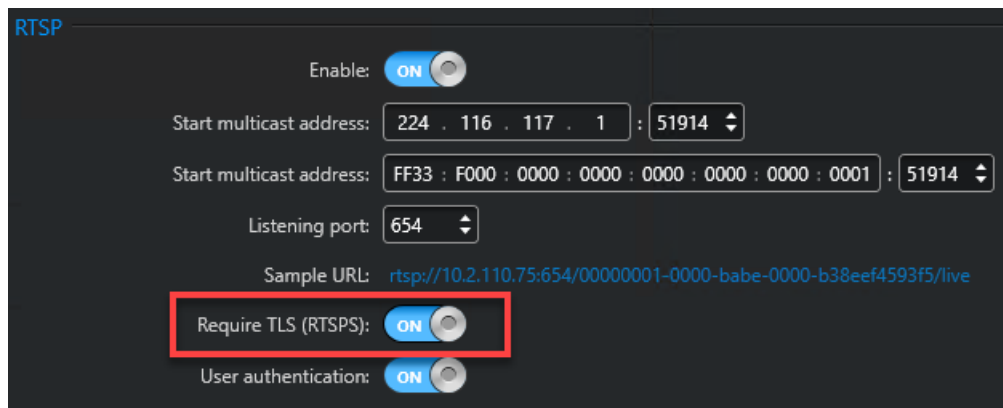
Confirm password:

■ Very weak ⓘ

⚠ The password requires 8 or more characters,
1 or more upper case letters,
1 or more lower case letters,
1 or more numerical characters and
1 or more special characters

Cancel OK

- c) Enter a password for RTSP streaming.
This password is different from the user password for the account.
BEST PRACTICE: Set a long, unique, and random password for each RTSP user.
 - d) Click **Apply**.
- 5 For RTSPS streaming:
- a) Enable **Require TLS (RTSPS)**



RTSP

Enable:

Start multicast address: 224 . 116 . 117 . 1 : 51914 ▾

Start multicast address: FF33 : F000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001 : 51914 ▾

Listening port: 654 ▾

Sample URL: <rtsp://10.2.110.75:654/00000001-0000-babe-0000-b38eef4593f5/live>

Require TLS (RTSPS):

User authentication:

- b) Click **Apply**.
Security Center user passwords are used for RTSPS streaming.

Using a local service account for Genetec™ Server (Basic)

To ensure your system's security, administrators must enter a password to access the configuration settings of their servers.

What you should know

Only local machine privileges are required by the local service account. Domain privileges are not.

BEST PRACTICE: In Windows, enable the **Passwords must meet complexity requirements** when accounts other than the local service account are used.

To set a secure password for your Security Center servers:

- 1 On the *Service Logon Parameters* page of the Genetec™ Security Center InstallShield, choose between using the default parameters or specifying your own.

If **Use default username and password option** is selected, Security Center uses the predefined LocalSystem account. This is the default and preferred option. If you want to use a different user account, administrator privileges are required, as this account is used to run the Genetec™ Server service.

- 2 Confirm the password and click **Next**.

Changing the default logon password for Security Center servers (Basic)

To ensure your system's security, you must set a secure password to access the configuration settings of your Security Center servers.

What you should know

It is a best practice to use a long, unique, random password for your main server. The minimum password length is eight characters.

To set a secure password for your Security Center servers during installation:

- 1 On the *Server configuration* page of the Security Center InstallShield, enter the following:
 - **Password/Confirm password:** Enter and confirm the password to open the web-based Server Admin.

BEST PRACTICE: If you are upgrading your Security Center installation, the existing server password is kept by default. If you were using a blank password, we recommend that you enter a new one that contains at least one uppercase character, one lowercase character, one number and one special character.

IMPORTANT: If you lose the server password, call Genetec™ Technical Support to reset it.

Genetec™ Security Center Installer

Server Configuration

Server port:

Web server port:

Password:

Confirm password:

- One lowercase character
- One uppercase character
- One number
- One special character
- 8 characters minimum
- No space or ' '

InstallShield™

< Back Next > Cancel

- 2 Confirm the password and click **Next**.

NOTE: If you are installing an expansion server, go to the *Server Configuration* page of the InstallShield, enter the same password that you created for your main server.

Genetec™ Security Center Installer

Server Configuration

Server port: 5500

Web server port: 80

— Main Server connection —

Server address: | | : 5500

Password: | |

Confirm password: | |

⚠ Please note that expansion password is the same as Main

InstallShield™ < Back Next > Cancel

Changing the password for Security Center servers in Genetec™ Server Admin (Basic)

If you need to change the password of your Security Center servers, you can do so in Genetec™ Server Admin.

What you should know

It is a best practice to use a long, unique, random password for your main server. The minimum password length is eight characters.

To change the password for your Security Center servers in Genetec™ Server Admin:

- 1 Open Genetec™ Server Admin and click the **Overview** page.
- 2 Click the **Modify** button.

Connection settings

Server admin remote access

Local machine only

Password

●●●●●●●●

Modify

- 3 Enter your old password, then enter a new password and confirm it.

Change password

Old password

Password

The password requires 8 or more characters

Confirm password

Cancel Save

- 4 Click **Save**.

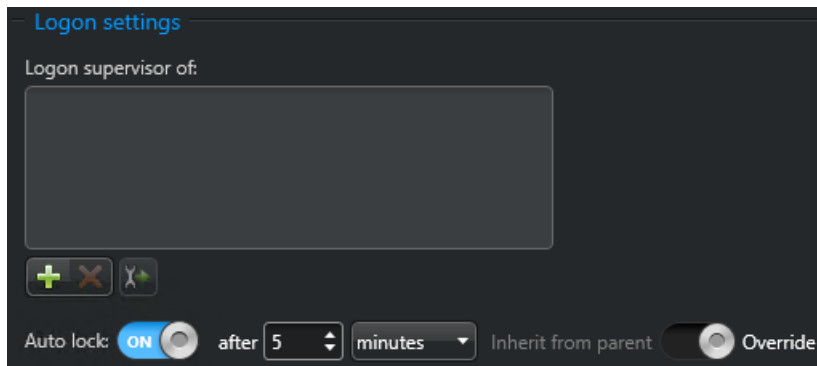
Activating auto lock on Security Desk workstations (Basic)

When the auto lock feature is activated, users are automatically logged off of Security Desk when no activity is detected from the user's workstation. This prevents intruders from accessing an unattended workstation.

To activate auto lock:

- 1 From the Config Tool home page, open the *User management* task.
- 2 Select a user or user group from the entity browser and click the **Advanced** tab.
- 3 In the *Logon settings* section, move the slider from **Inherit from parent** to **Override**.
- 4 Move the **Auto lock** slider to **ON**.
- 5 Set the amount of time that a workstation needs to be inactive before locking.

A default value of five minutes is adequate in most cases.



- 6 Click **Apply**.

About configuring Federation™ users (Basic)

The Federation™ role uses a remote user account to connect to a remote Security Center system.

If your system is federated by another system, the remote user account that the Federation™ role accesses should have minimum privileges.

NOTE: Make sure the user account does not have administrative privileges.

For more information on this feature, see the *Security Center Administration Guide*.

Using Windows Active Directory Integration (Advanced)

By synchronizing Windows Active Directory with Security Center's Active Directory role, you can log on to your system using your Windows credentials. When activated, you can manage all user accounts from a single location, which reduces errors and facilitates user account management.

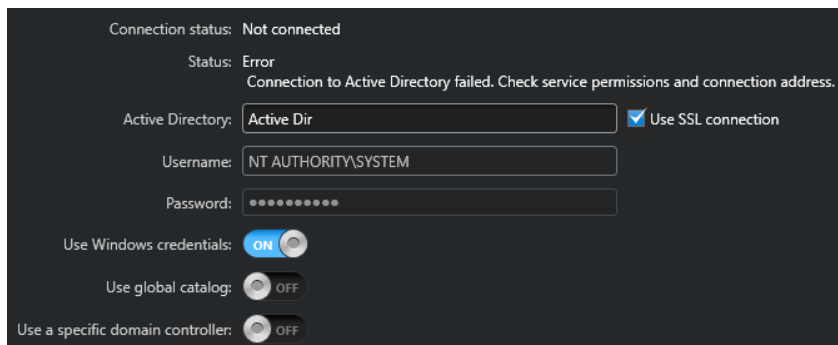
What you should know

A strong password policy that aligns with the [best practices](#) published by the National Institute of Standards and Technology (NIST) should be enforced for Active Directory user accounts.

To configure your Active Directory role:

- 1 From the Config Tool home page, open the *System* task and click on the **Roles** view
- 2 Select the **Active Directory** role from the entity browser.
- 3 Click the **Properties** tab and enter the required information.

NOTE: Use **SSL connection** must be selected.



- 4 Click **Apply**.

Using a third-party identity provider to authenticate a Security Center user (Advanced)

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.

Third-party authentication is available using the OpenID Connect, SAML 2.0, WS-Federation, and WS-Trust protocols. By using it, you can take advantage of advanced authentication requirements, like the use of smartcards or *multi-factor authentication*, to increase confidence in the user's identity.

For more information on third-party authentication, refer to "What is third-party authentication?" in the *Security Center Administrator Guide*.

Deactivating all local users (Advanced)

When using third-party authentication for Security Center users, we recommend deactivating all local user accounts to ensure every account follows the same authentication policies. This includes the default Admin account.

External identity providers can impose advanced authentication requirements, like the use of smartcards or [multi-factor authentication](#), to increase confidence that a user is who they say they are. After setting up third-party authentication, keeping local Security Center users active weakens the overall security of your system because local users do not follow the same authentication policies as those authenticated by the identity provider. Additionally, these separately managed accounts increase the attack surface of Security Center.

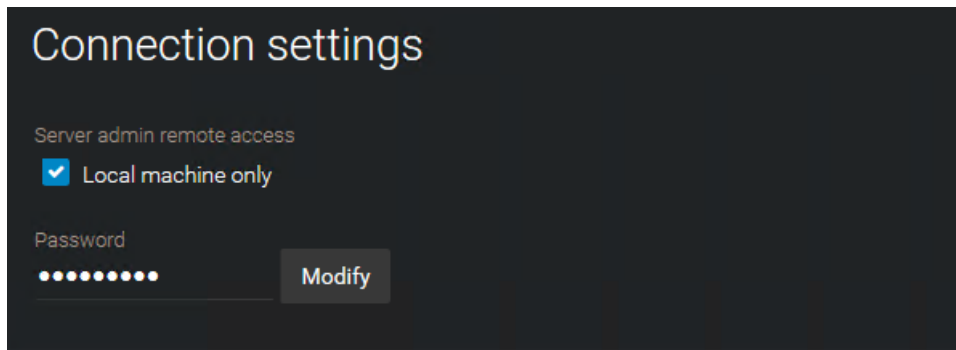
For more information on deactivating Security Center users, refer to "Deactivating user profiles" in the *Security Center Administrator Guide*.

Restricting Server Admin access to local connections (Advanced)

You can configure Server Admin so it can only be accessed by local users of the Security Center server: the machine where Genetec™ Server is installed.

To restrict Genetec™ Server Admin access:

- 1 Open Server Admin and click the **Overview** page.
- 2 In the *Connection Settings* section, under *Server admin remote access*, select **Local machine only**.



This option only allows the Server Admin to be accessed from the local machine.

- 3 Click **Save**.

Restricting user privileges (Advanced)

For security purposes, individual users should be assigned the minimum required privileges. Security Center features many templates with predefined sets of privileges, such as Operator, Investigator, Supervisor, and so on.

What you should know

Users have a set of basic privileges that are granted to them, or inherited from parent user groups. They also have a set of privileges for every partition in which they are an authorized user. Privileges granted or denied at the partition level replace the basic privileges.

BEST PRACTICE: Individual users should only have the minimum required privileges. When assigning privileges, Security Center offers templates with predefined sets of privileges that can be applied to users or groups.

To help you better understand what your users can do, Security Center includes a Privilege troubleshooter. The Privilege troubleshooter is a tool that helps you investigate the allocation of user privileges in your Security Center system. Use the troubleshooter to verify access rights and help you fix issues.

To assign privileges to a user:

- 1 From the Config Tool home page, open the *User management* task.
- 2 Select the user to configure, and click the **Privileges** tab.
- 3 Use one of the predefined privilege configurations as your starting point.

At the bottom of the page, click , and select one of the following:

- **Apply template:** Select one of the privilege templates to apply.

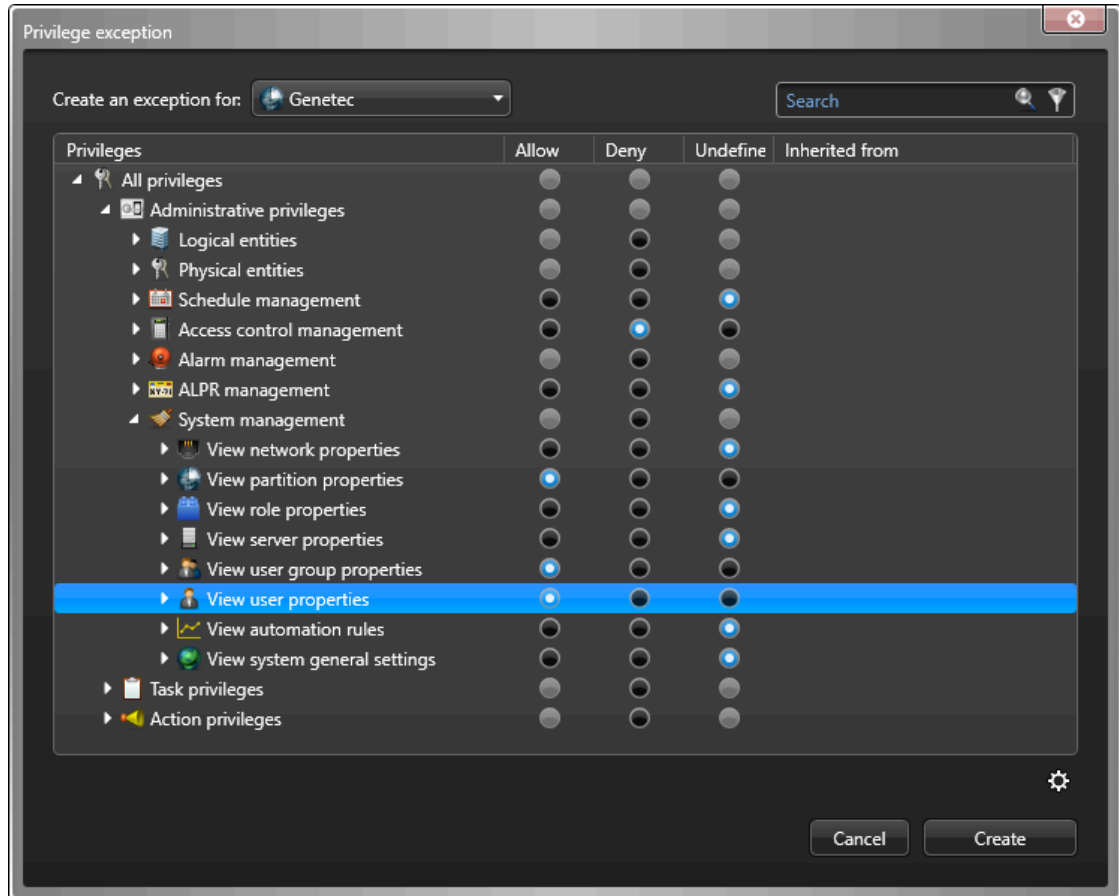
Privilege templates can be combined. This means that when you apply a privilege template, you always add privileges. Existing privileges can never be removed as a result of applying a privilege template. To start with a clean slate, go to the top of the privilege hierarchy (**All privileges**) and click **Undefined**.

- **Set configuration to read-only:** Set all entity configuration privileges found under the *Administrative privileges* group to *View properties* with *Modify properties* denied.
 - **Set configuration to read-write:** Set all entity configuration privileges found under the *Administrative privileges* group to *View*, *Modify*, *Add*, and *Delete*.
- 4 Fine tune the user privileges by changing the individual privilege settings if necessary. Keep in mind that if your user has a parent user group, the privilege inheritance rules apply.
 - **Allow:** Grant the privilege to the user. You cannot select this option if the privilege is denied to the parent user group.
 - **Deny:** Deny the privilege to the user.
 - **Undefined:** Inherit this privilege from the parent user group. If there is not parent user group, this privilege is denied.
 - 5 If necessary, configure the privilege exceptions for each partition the user has access to.

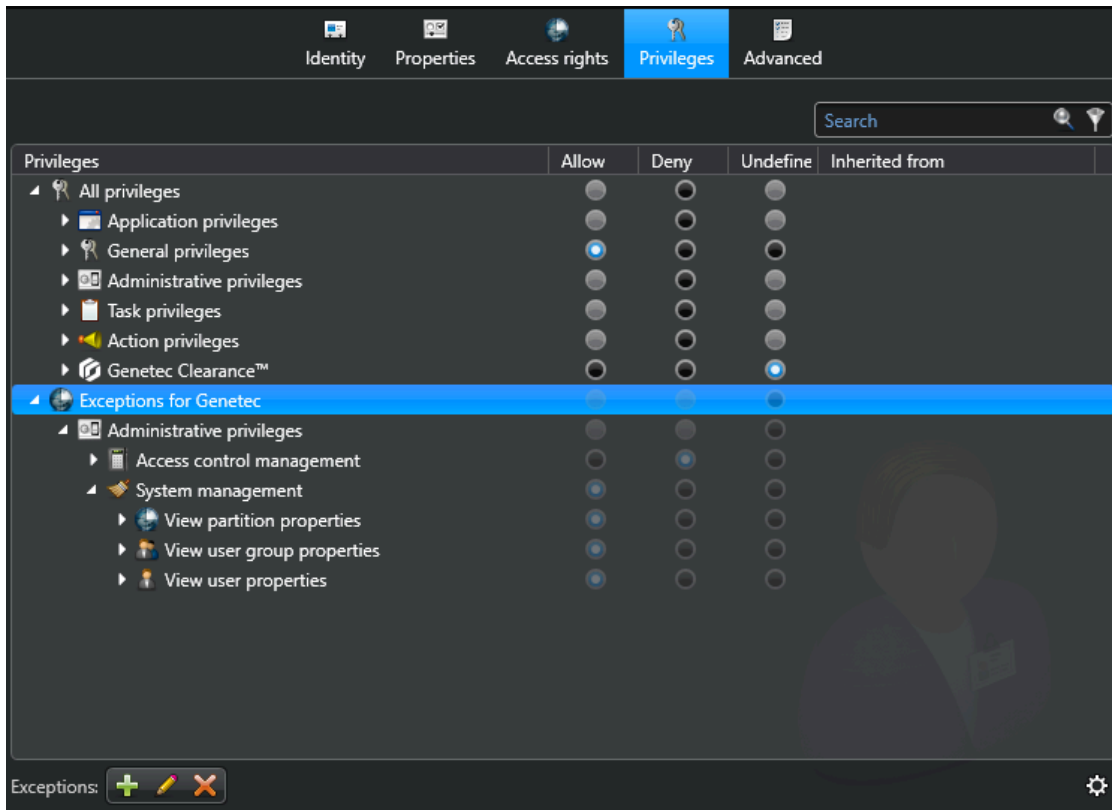
When a user is given access to a partition, their basic privileges are applied by default to the partition. As a system administrator, you can overwrite the privileges a user has over a specific partition. For example, a user can be allowed to configure alarms in partition A, but not in partition B. This means that a user

can have a different set of privileges for each partition they have access to. Only *Administrative* and *Action* privileges, plus the privileges over public tasks, can be overwritten at the partition level.

- a) At the bottom of the page, click **Exceptions** (+).
- The *Privilege exception* dialog box opens.
- b) In the **Create an exception for** drop-down list, select a partition.
- c) Change the user's basic privileges as required.



- d) Click **Create**.
- The privilege exceptions are added at the bottom of the privilege list.



6 Click **Apply**.

7 (Optional) Allow the user to move entities from one partition to another to which they have access.

To allow a user to move entities from one partition to another to which they have access, you must grant them the associated *Add/Delete <entities>* pair of privileges for each entity type you allow them to move between partitions.

If you do not want to grant the full *Add* and *Delete* privileges to the user but still want to allow them to move entities between partitions, enable the *Manage partition memberships* option as follows.

a) Click the **Advanced** tab.

b) Enable the **Manage partition memberships** option.

If necessary, switch **Inherit from parent** to **Override** to change this setting.

c) Click **Apply**.

NOTE: When you grant *All privileges* to a user, the *Manage partition memberships* option is also enabled. However, if you disable the **Manage partition memberships** option, it does not affect the other privileges the user has.

Restricting client application connections to a specific Directory (Advanced)

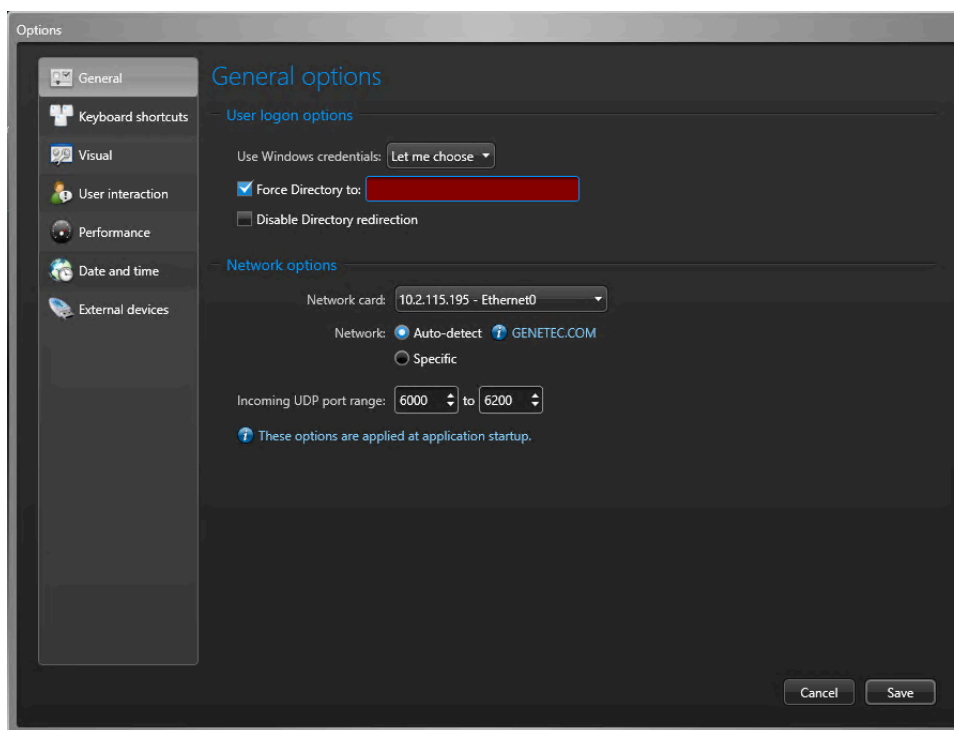
In addition to user access management, you can restrict Config Tool and Security Desk from connecting to a specific Directory.

To restrict client applications from connecting to a specific Directory:

- 1 From the Config Tool or Security Desk home page, click the *Options* tab and then click **General**.
- 2 In the *User logon options* section, select **Force Directory to**, and type the name of the Directory.

With this option enabled, users cannot choose the Directory to which they want to connect; the **Directory** field is not displayed in their *Logon* window. However, they can automatically be redirected to another Directory with load balancing.

NOTE: If there is a mistake in the Directory name, such as a typo, users will not be able to connect the next time they try to log on.



- 3 Click **Save**.

System

This section includes the following topics:

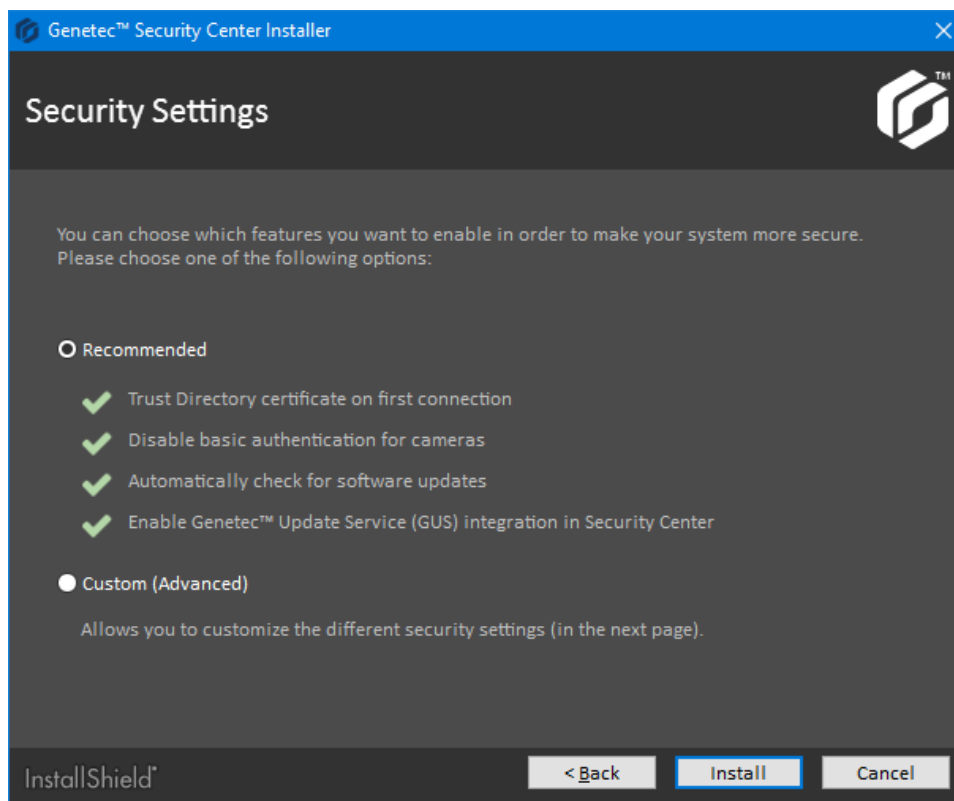
- ["Using the recommended security settings in InstallShield \(Basic\)"](#) on page 27
- ["Reviewing which data is collected for the Product Improvement Program \(Basic\)"](#) on page 28
- ["Using trusted certificates on Security Center servers \(Advanced\)"](#) on page 30
- ["Controlling access to your resources using partitions \(Advanced\)"](#) on page 32
- ["Disabling backward compatibility \(Advanced\)"](#) on page 33
- ["Disabling backward compatibility for the Map Manager role \(Advanced\)"](#) on page 34
- ["Deactivating unused roles \(Advanced\)"](#) on page 35
- ["Using a Directory gateway for external access to Security Center \(Basic\)"](#) on page 36
- ["Running macros with limited access rights \(Advanced\)"](#) on page 38

Using the recommended security settings in InstallShield (Basic)

InstallShield offers recommended security settings by default. Upon first connection, client applications trust the server certificates, and warn the user if certificates change upon subsequent connections.

What you should know

The certificates in the recommended security settings for Security Center are used to establish a Transport Layer Security (TLS) connection between the Directory and clients (Security Desk and Config Tool), and between Genetec™ Servers.



To use the recommended security settings in InstallShield:

- 1 On the *Security Settings* page of the Security Center installation wizard, select **Recommended**.
- 2 Click **Install**.

Reviewing which data is collected for the Product Improvement Program (Basic)

The Product Improvement Program collects system usage data to help us improve our products.

What you should know

Sharing system data might cause privacy concerns for some customers.

Make sure the option you choose is in accordance with your privacy policy. This option is chosen during installation and can be modified in Genetec™ Server Admin tool.

To modify the data collected for the Product Improvement Program:

- 1 Open Genetec™ Server Admin.
- 2 From the **Servers** list, select your server.

- In the *Directory* section, under **Indicate how you want your system data to be collected**, select your desired method of data collection from the list.

Directory

Database server: (local)\SQLEXPRESS Status: OK

Database name: Directory

Keep incidents: Indefinitely For 90 days

Keep audit and activity trails: Indefinitely For 90 days

Keep alarms: Indefinitely For 90 days

Maximum journal size: 1024 MB

Enable cache

Auto ack alarms after 72 hours

Run macros with limited access rights

Indicate how you want your system data to be collected.

Do not collect data ct improvement.

- Do not collect data
- Collect data anonymously
- Collect and link data to your system ID

- Click **Save**.

Using trusted certificates on Security Center servers (Advanced)

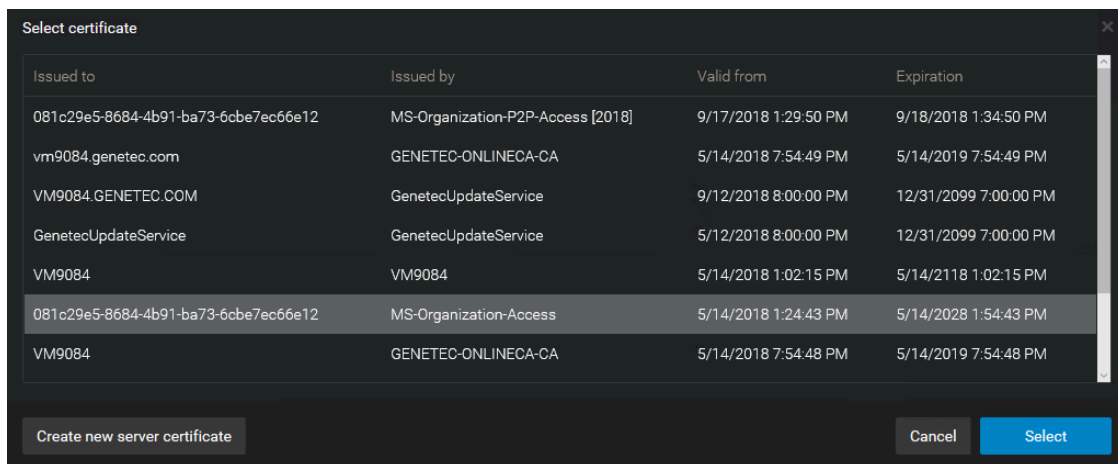
To strengthen the security of your system, you can replace the self-signed certificate on the main server with one issued by a trusted certificate authority (CA). Alternatively, you can import the certificate into the trusted root store of all machines that connect to the Directory.

Before you begin

When installing Security Center, on the *Security Settings* page of the InstallShield, select **Always validate the Directory certificate**.

To modify a trusted certificate on your Security Center server:

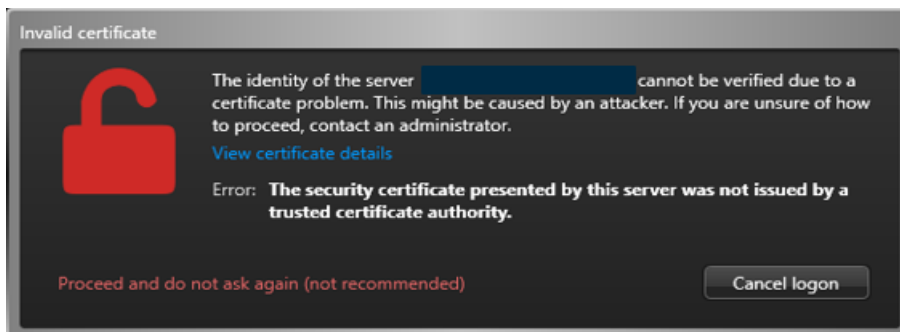
- 1 Open Genetec™ Server Admin.
- 2 From the **Servers** list, select your server.
- 3 In the *Secure communication* section, click **Select certificate**.
- 4 Choose a certificate and click **Select**.



5 Click **Save**.

IMPORTANT: If the selected certificate is not trusted by client machines, users are presented with a dialog box when they attempt to log on, informing them of the untrusted connection and providing the following options:

- **Proceed and do not ask again (not recommended)**
- **Cancel logon**



There is also a link to **View certificate details** to help understand why the certificate is not trusted.

We recommend using a certificate that is trusted by all client machines. If the *Invalid certificate* warning is unexpected, ensure that you understand why the certificate is not trusted before proceeding.

Controlling access to your resources using partitions (Advanced)

To organize and manage access to system resources in Security Center, you can use a container called a partition to group related assets, such as buildings, equipment, cameras, imported data collected in the fields, and so on.

What you should know

It is considered a best practice to create a special partition for low-privileged operators that only need to view video. To strictly control access rights, assign camera entities to that partition without assigning their associated video unit entities. You can then control which users or user groups can access each partition.

To create a partition:

- 1 From the Config Tool home page, do one of the following:
 - Open the *User management* task, click **Add an entity** (+), and then click **Partition**.
 - Open any administration task, click **Add an entity** > **Show all** > **Partition**, or click **More** (▾) beside the **Add** (+) button, and then click **Partition**.
- 2 If a partition is selected in the entity tree before you click **Add**, then the new partition is immediately created under the selected partition.
 - a) Enter the name of the **New partition**.
 - b) In the **Identity** tab, enter the partition description.
- 3 If no partition was selected in the entity tree before you click **Add**, then the *Create partition* wizard opens.
 - a) On the *Basic information* page, enter the name and description of the new partition.
 - b) From the **Partition** drop-down list, select the parent partition that this new partition should belong to. The new partition is created.
- 4 If you already have entities ready to be added to the new partition, add them.
- 5 If users and user groups are already created in your system, grant access rights for the new partition to those who need it.

Disabling backward compatibility (Advanced)

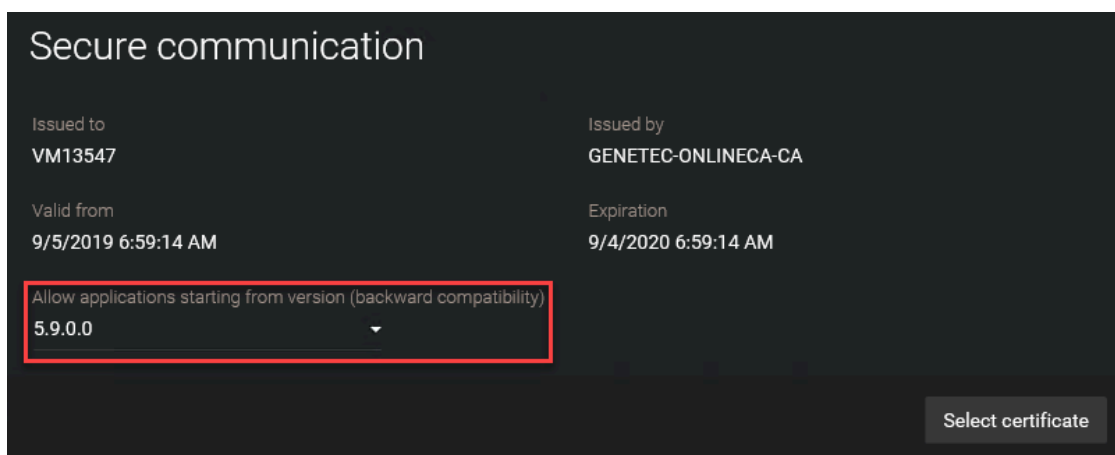
If your system is backward compatible with older versions of Security Center that do not support the Transport Layer Security (TLS) protocol (5.4 and earlier), your system will be more vulnerable to network attacks.

What you should know

Mobile Server 4.0 does not support Transport Layer Security (TLS) protocol. Disabling backward compatibility means that the Mobile apps and the Web Clients 4.0 can no longer connect to Security Center. Expansion servers that have not been upgraded to version 5.5 or later will also stop working. Both Web Client 4.1 and the role-based Web Client 5.6 and later support TLS.

To disable backward compatibility:

- 1 Connect to the Server Admin of your main server with a web browser.
- 2 Click the main server (🌐) in the server list.
- 3 In the *Secure communication* section, select your current version of Security Center version from the **Allow applications starting from version (backward compatibility)** drop-down.



- 4 Click **Save**.

IMPORTANT: The next time someone tries to connect to your system with an older Security Center version, they will get the *Client-server versions are incompatible* error.

Disabling backward compatibility for the Map Manager role (Advanced)

For enhanced security, disable backward compatibility for the Map Manager role after upgrading all client applications from Security Center 5.8 and earlier.

What you should know

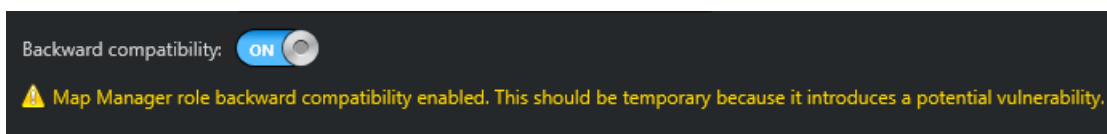
Starting with Security Center 5.9, Map Manager requires all clients that request image maps to pass authentication. To ensure legacy clients can view the background images of image maps after upgrading the server, Map Manager roles upgraded from 5.8 and earlier run in backward compatibility mode by default.

When in backward compatibility mode, Map Manager grants access to image maps without authentication. This mode is intended to temporarily maintain map functionality during a staged upgrade where some clients remain at an older version for a limited time.

BEST PRACTICE: Disable backward compatibility for the Map Manager role after all client applications have been upgraded.

To disable backward compatibility for the Map Manager role:

- 1 From the Config Tool home page, open the *System* task, and click the **Roles** view.
- 2 Select the Map Manager role, and click the **Properties** tab.
- 3 Switch **Backward compatibility OFF**.



- 4 Click **Apply**.

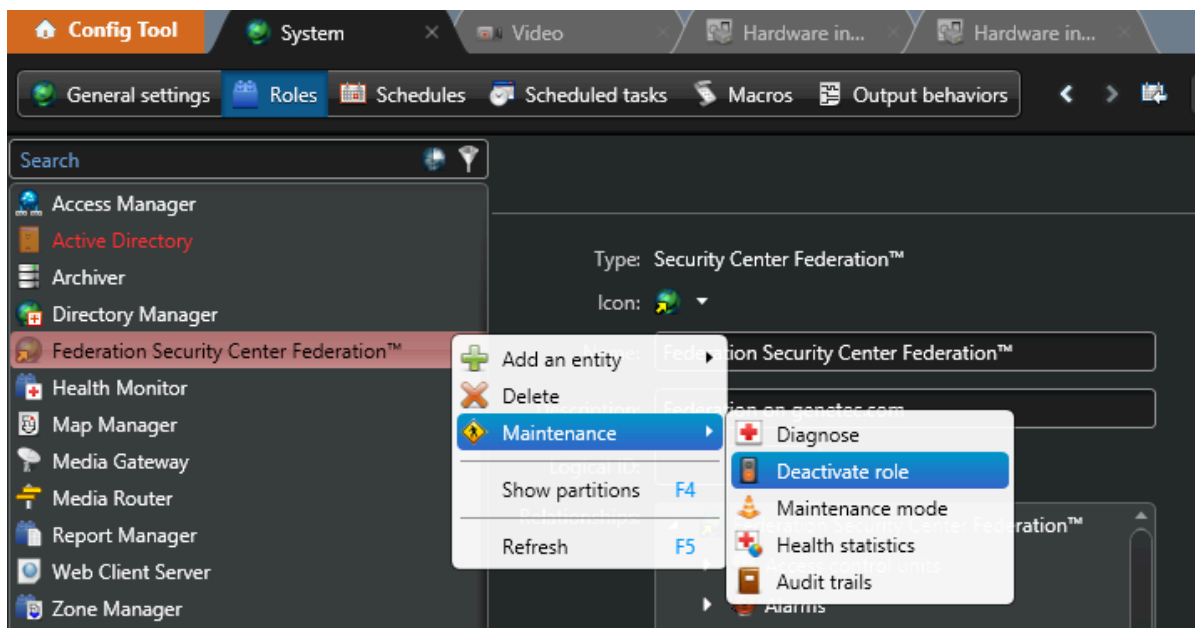
Backward compatibility for the Map Manager role is disabled. Client applications that do not authenticate are unable to view the background images of image maps.

Deactivating unused roles (Advanced)

To reduce your surface of attack with a defense-in-depth strategy, you can disable unused roles. Some roles are activated by default and might not be needed by all users, or might be left activated after a configuration change even if they are not used anymore.

To deactivate an unused role:

- 1 From the Config Tool home page, open the *System* task, and click on the **Roles** view.
- 2 Right-click the role, then click **Maintenance > Deactivate role**.



- 3 Click **Continue**.

Using a Directory gateway for external access to Security Center (Basic)

Directory gateways allow Security Center applications on non-secured networks to connect to the main server that is behind a firewall.

What you should know

A Directory gateway is a Security Center server that acts as a proxy for the main server. A server cannot be both a Directory server and a Directory gateway; the Directory server must connect to the Directory database and, for security reasons, the Directory gateway must not.

To create Directory gateways:

- 1 From the Config Tool home page, open the *System* task, and click the **Roles** view.
- 2 Select the **Directory Manager** (🌐) role, and then click the **Directory servers** tab.
- 3 At the bottom of the server list, click **Advanced** (⚙️).
An extra column, **Gateway**, opens in the list.
- 4 At the bottom of the list, click **Add an item** (+).
- 5 In the dialog box that opens, select the server you want to add, and click **Add**.
- 6 Add more servers to the list if necessary.

- 7 Select the **Gateway** option on servers you want to use as Directory gateways.

A Directory gateway must be located on the non-secured network. It does not need to access the Directory database, but it needs to connect to the main server. The following example shows a system with two Directory servers, one of which is the main server, and two Directory gateways.

NOTE:

- *Load balancing* only occurs between Directory servers. A user trying to connect to a Directory gateway will not be redirected to a Directory server, and vice versa.
- The **Disaster recovery** option only applies to Directory servers, not to Gateways.

Identity | **Directory servers** | Database failover

List of Directory servers (for failover and load balancing) and Directory gateways (for redirection):

Server	Gateway	Disaster recovery
P-DC	<input type="checkbox"/>	<input type="checkbox"/>
F-DC	<input type="checkbox"/>	<input type="checkbox"/>
P-DMZ	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F-DMZ	<input checked="" type="checkbox"/>	<input type="checkbox"/>

⚠ Adding, modifying, or removing Directory servers forces the servers to restart.

ⓘ Adding a server in the list will require a license update

- 8 [Update your license](#) to include the servers that you have just promoted to Directory gateways.
- 9 Click **Apply**.

Running macros with limited access rights (Advanced)

Starting in Security Center 5.8, you can run macros with limited access rights. This eliminates the risk of a user running a macro to create a new admin user and gain greater access to the system.

What you should know

Macros have limited access rights by default in fresh installations. Systems upgrading to Security Center 5.8 run macros with administrative rights by default. If you are upgrading to Security Center 5.8, review this setting and make sure it is activated.

To run macros with limited access rights:

- 1 Open Genetec™ Server Admin and click the *Servers* page.
- 2 Click the Directory that you want to run macros on.
- 3 In the *Directory* section, select **Run macros with limited access rights**.

The screenshot shows the 'Directory' configuration page. At the top, the 'Database server' is set to '(local)\SQLEXPRESS' and the 'Status' is 'OK'. The 'Database name' is set to 'Directory'. Below these are several icons: a plus sign, a close sign, a list icon, a menu icon, and a refresh icon. The 'Keep incidents' section has 'Indefinitely' and 'For 90 days' options, with 'For 90 days' selected. The 'Keep audit and activity trails' section also has 'Indefinitely' and 'For 90 days' options, with 'For 90 days' selected. The 'Keep alarms' section has 'Indefinitely' and 'For 90 days' options, with 'For 90 days' selected. The 'Maximum journal size' is set to '1024 MB'. There is an 'Enable cache' checkbox which is unchecked. The 'Auto ack alarms after 72 hours' checkbox is checked. At the bottom, the 'Run macros with limited access rights' checkbox is checked and highlighted with a red box.

- 4 Click **Save**.

Genetec™ Update Service (GUS)

This section includes the following topics:

- ["About keeping Security Center updated with Genetec™ Update Service \(Basic\)"](#) on page 40
- ["Connecting to Genetec™ Update Service with Server Admin credentials \(Basic\)"](#) on page 41
- ["Using a proxy server to connect Genetec™ Update Service to the internet \(Basic\)"](#) on page 42

About keeping Security Center updated with Genetec™ Update Service (Basic)

Genetec™ Update Service (GUS) automatically keeps your version of Security Center up-to-date with the latest security fixes and improvements.

Internet access is required for GUS to work. Otherwise, Security Center can be manually updated by downloading the latest version from [GTAP](#).

For more information on GUS, consult the *Genetec™ Update Service User Guide*.

Connecting to Genetec™ Update Service with Server Admin credentials (Basic)

To be notified when a unit's firmware (such as Axis or Access Control units) contains security issues, connect Genetec™ Update Service (GUS) to Security Center using your Server Admin credentials.

To modify Security Center Directory GUS credentials:

- 1 From the Config Tool home page, open the *System* task.
- 2 Click the **General settings** view, and click the *Updates* page.
- 3 Click on the **Settings** tab.
- 4 In the *Advanced* section, under **Credentials**, click **Security Center Directory**.
- 5 In the **Security Center Directory** dialog box, enable **Modify credential of Server Admin** and enter a password.
- 6 Click **Apply**.

Security Center Directory

Directory name or IP: localhost

Sever Admin REST port: 443

Modify credential of

Server Admin

Password:

Close Apply

- 7 Click **Save configuration**.

Using a proxy server to connect Genetec™ Update Service to the internet (Basic)

Genetec™ Update Service (GUS) requires an internet connection. However, to reduce the potential impact of a compromised system, it is best if the machine that hosts the Directory role is not the machine accessing the Internet.

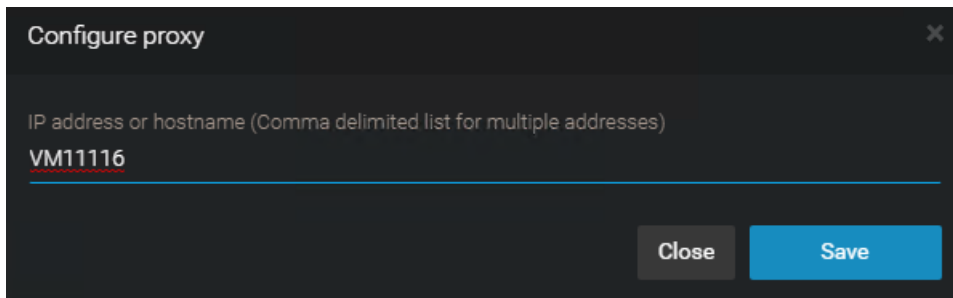
What you should know

Any Genetec™ Server on which GUS is configured can act as a proxy for a different GUS within the system.

In this scenario, a proxy is required by the GUS installed on the main server to communicate with the machine that has Internet access.

To use a proxy to connect Genetec™ Update Service to the internet:

- 1 From the Config Tool home page, open the *System* task.
- 2 Click the **General settings** view, and click the *Updates* page.
- 3 Click on the **Settings** tab.
- 4 In the *Download and Internet Proxy* section, click the edit button (✎).
- 5 In the **Configure proxy** dialog box, enter the IP address or host name of a valid Internet-enabled machine.



- 6 Click **Add**.
- 7 Click **Save configuration**.

Video

This section includes the following topics:

- ["Refusing basic authentication \(Basic\)"](#) on page 44
- ["Enabling secure communication in the Media Router \(Basic\)"](#) on page 46
- ["Upgrading video unit firmware \(Basic\)"](#) on page 47
- ["Ensuring that your cameras have strong administrator passwords \(Basic\)"](#) on page 49
- ["Rotating your camera passwords periodically \(Advanced\)"](#) on page 50
- ["Connecting to cameras through HTTPS \(Advanced\)"](#) on page 51
- ["Encrypting data in transit and at rest with fusion stream encryption \(Advanced\)"](#) on page 52
- ["Deactivating unused services on video units \(Advanced\)"](#) on page 54

Refusing basic authentication (Basic)

Basic authentication sends camera passwords over the network in clear text equivalent (encoded in base64). Therefore, an attacker can passively listen to capture the passwords. Basic authentication should therefore be disabled while installing cameras.

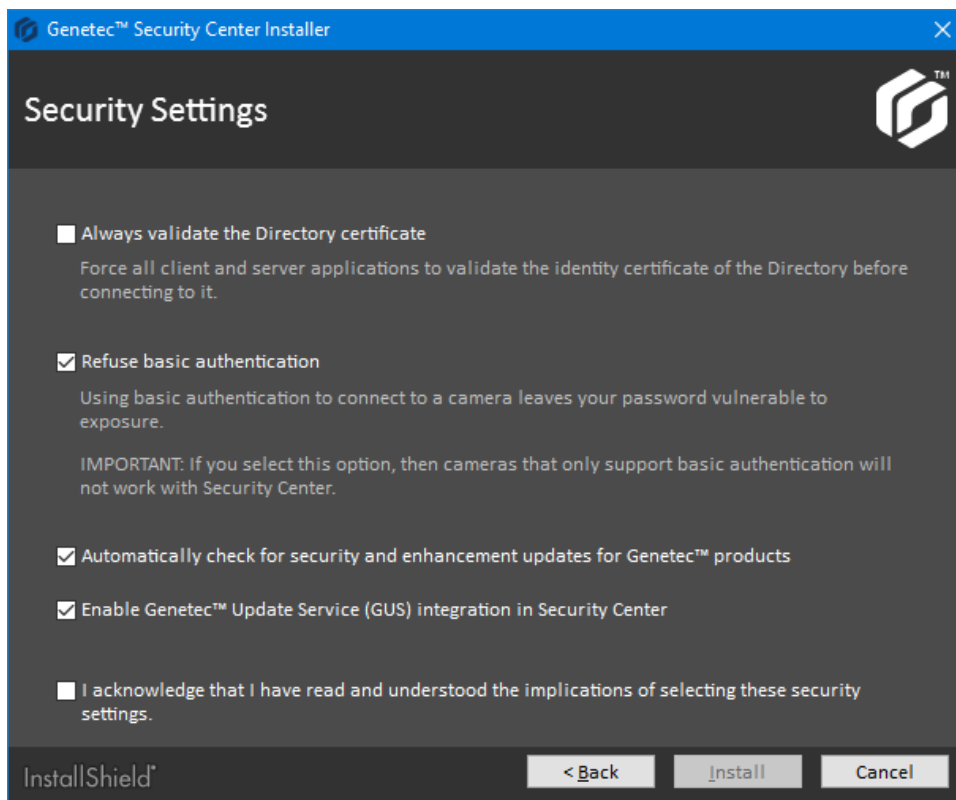
What you should know

Some camera manufacturers only support basic authentication, so disabling this authentication might prevent Security Center from connecting to some cameras.

Basic authentication is disabled by default when the recommended security settings are selected. If you want to enable basic authentication, adjust your settings on the *Advanced* page in InstallShield.

To enable basic authentication:

- 1 On the *Security Settings* page of the Security Center InstallShield, select **Custom (Advanced)**.
- 2 Click **Next**.
- 3 Select **Refuse basic authentication**.
- 4 Click **Install**.



Enabling basic authentication (Basic)

If basic authentication is disabled, you can enable it using the Config Tool.

To revert to the basic authentication scheme on a specific video unit:

- 1 From Config Tool, open the *Hardware inventory* task.
- 2 Run the report on the video units that are inactive (in red) in your system.
You might need to scroll horizontally to the right to see the **Authentication scheme** column.

- 3 In the report pane, select the video units that are inactive and click **Reset authentication scheme**.
The **Authentication scheme** changes to **Anonymous**. After the Archiver successfully connects to the video unit, the exact authentication scheme is displayed.

To revert to the basic authentication scheme for a specific manufacturer:

- 1 From Config Tool, open the *Video* task.
- 2 Select the Archiver role that controls your cameras and click **Extensions**.
- 3 Select the manufacturer you want and set **Refuse basic authentication** to **OFF**.
- 4 Click **Apply**.

Enabling secure communication in the Media Router (Basic)

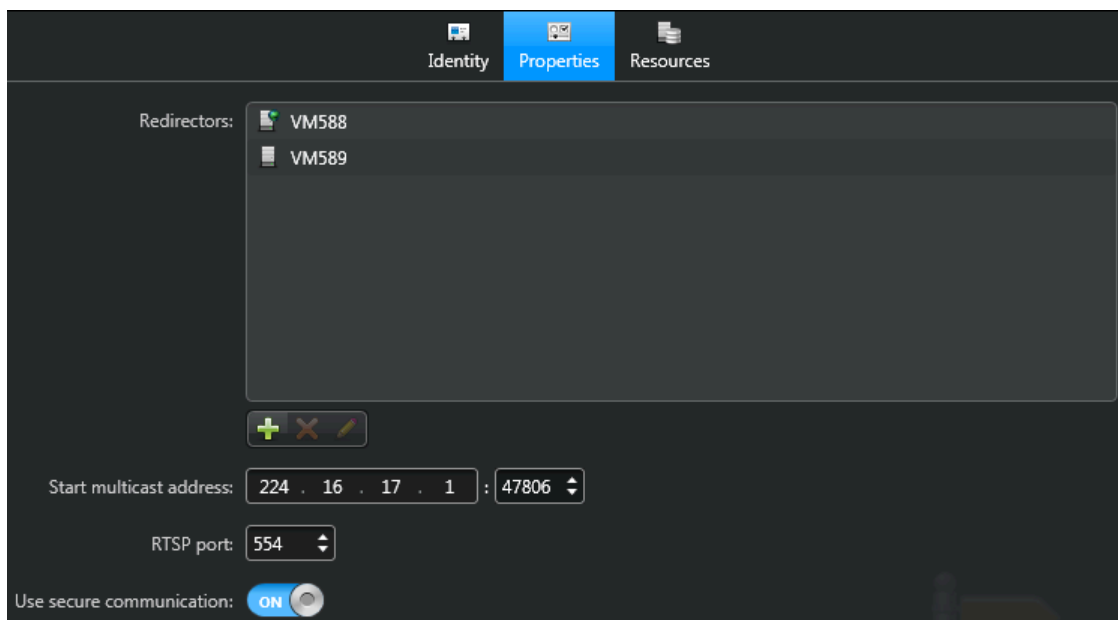
Starting in Security Center 5.5, when Security Desk requests a video sequence, the connection is secured using authentication and encryption with the Transport Layer Security (TLS) protocol.

What you should know

This feature is enabled by default.

To activate secure communication on the Media Router:

- 1 From the Config Tool home page, open the *Video* task.
- 2 Select the **Media Router** role from the entity browser.
- 3 In the **Properties** tab, set the **Use secure communication** slider to **ON**.



- 4 Click **Apply**.

Upgrading video unit firmware (Basic)

Camera manufacturers frequently upgrade their products and fix security vulnerabilities within new firmware. So, it is best practice to upgrade video units with the latest firmware certified by Genetec Inc.

Before you begin

- If *Genetec™ Update Service (GUS)* is running, the status of the firmware upgrade is indicated in the unit's *Identity* page and in the **Proposed firmware description** column of the *Hardware inventory* report:
 - **Up to date:** No firmware upgrade is necessary.
 - **Optional:** The firmware upgrade is not urgent.
 - **Recommended:** The firmware upgrade is recommended.
 - **Security vulnerability:** The firmware upgrade fixes a security vulnerability issue and is highly recommended.
- Download the recommended firmware from the manufacturer's website. If GUS is not running, you can find the recommended firmware for your unit from our [Supported Device List](#).

NOTE: For certain video unit models, GUS can download for you the recommended firmware so you don't have to do it yourself. When the download option is available, the recommended firmware version is indicated in the *Upgrade firmware* dialog box. The downloaded firmwares are kept in a central storage managed by GUS, called the *Firmware Vault*, for seven days.

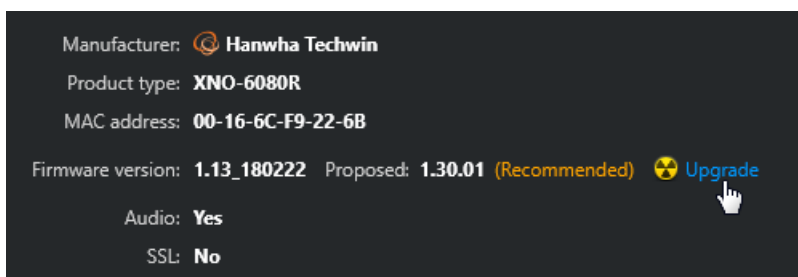
- Take note of the unit's configuration settings. For some manufacturers, the unit is reset to its default settings after the firmware upgrade.

What you should know

For some manufacturers, you cannot upgrade the unit's firmware from Config Tool. For manufacturer-specific information, see the manufacturer's documentation.

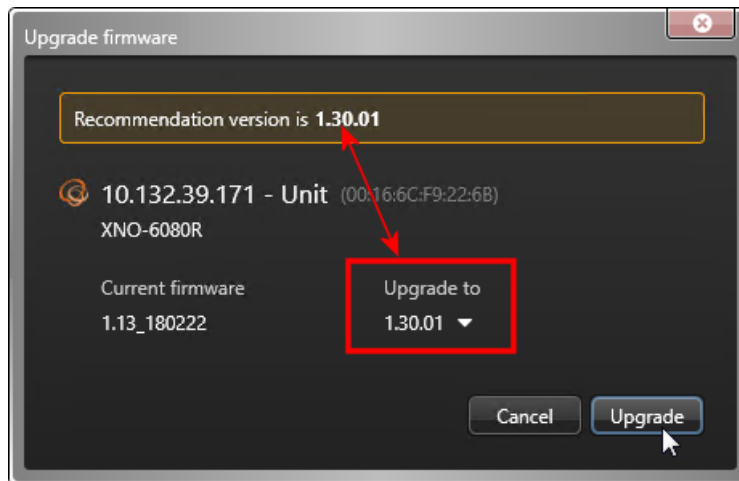
To upgrade the firmware of a single video unit:

- 1 From the Config Tool home page, open the *Video* task.
- 2 Select the video unit to upgrade, and click the **Identity** tab.
- 3 Click **Upgrade** (☠).

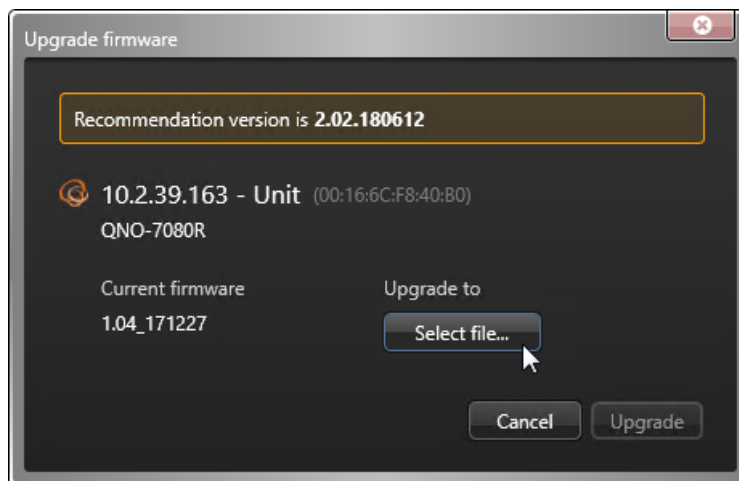


4 In the *Upgrade firmware* dialog box that opens, do one of the following:

- If the recommended firmware is shown under the label **Upgrade to**, it means that GUS can download the firmware for you. Click **Upgrade** to start the upgrade.



- If the **Select file** button is displayed instead, click that button and browse to the firmware file you downloaded yourself, and click **Open > Upgrade**.



A message is displayed in the notification tray telling you that the firmware upgrade has started.



When the firmware upgrade completes, the unit restarts.

After you finish

Reconfigure the units if they were reset to default settings during the upgrade.

Ensuring that your cameras have strong administrator passwords (Basic)

It is recommended that you change your cameras' default administrator passwords before you add them to Security Center.

What you should know

Some cameras are shipped with default administrative passwords, which can be weak or known to others.

The most secure way to change passwords is to set up a separate network (ideally over HTTPS). The camera can then be mounted at the desired location, and added to the CCTV network.

To view the password strength of cameras:

- 1 From the Config Tool home page, open the *Hardware Inventory* task.
- 2 Select an Archiver in the entity browser and click **Generate report**.

The report indicates the password strength of each video unit connected to the Archiver role.

Unit	Unit type	Product type	Firmware version	Password strength	Password	Last password update	Authentication
10.132.218.106	Video	AXIS M3016	9.50.1	Very weak	*****	2/19/2020 6:15:23 PM	Digest

- 3 Change the password on each video unit that lacks a *Strong* password.

For instructions on how to change video unit passwords, refer to "Changing video unit passwords" in the *Security Center Administrator Guide*.

NOTE: Passwords can be manually entered or system generated. We recommend using system-generated passwords because they are more secure. The system always uses the highest password complexity supported by the manufacturers.

Rotating your camera passwords periodically (Advanced)

For maximum security, we recommend changing your camera administrator passwords on a regular basis.

What you should know


Changing passwords periodically helps to protect vulnerable cameras from unauthorized access due to leaked passwords, brute force attacks, and so on.

Security Center can automatically update passwords for supported cameras using the highest possible password complexity for each manufacturer. When using Security Center to manage passwords, we recommend rotating camera passwords annually using a scheduled task.

NOTE: Only certain models of video units support the password update feature from Config Tool. For the list of manufacturers that support this feature, see "Manufacturers that support password update" in the Security Center Video Unit Configuration Guide.

If you manage passwords manually, or use an external tool that does not ensure maximum password complexity, we recommend changing passwords every 3 months or earlier.

To enable annual password rotation for supported cameras in Security Center:

- 1 From the Config Tool home page, open **System > Scheduled tasks**.
- 2 Click **Scheduled task** .
- A new scheduled task is added to the entity list.
- 3 Enter a name for the new scheduled task.
- 4 Click the **Properties** tab for the scheduled task, and switch **Status** to **Active**.
- 5 For **Recurrence**, select **Yearly** and specify a day and time to run the task.
- 6 For **Action**, select **Update unit password**.
- 7 For **Entities**, select one or more supported video units.
- 8 Click **Apply**.

If supported, the selected video units will automatically be updated with a new random, generated password every year.

NOTE: This task will be skipped if it cannot be executed at the scheduled time because the main server is offline, an entity is unavailable, and so on.

Connecting to cameras through HTTPS (Advanced)

For maximum security, it is recommended that you connect Security Center to cameras using HTTPS.

What you should know

The Archiver supports HTTPS connections with compatible cameras.

A certificate trusted by the Archiver must be installed on the cameras.

To enable HTTPS connections on cameras:

- 1 From the Config Tool home page, open the *Video* task.
- 2 Click **Add an entity** > **Video unit**.
- 3 Enter the required camera information.
- 4 For **Authentication**, select **Specific**.
- 5 Switch the **Use HTTPS** slider to **ON**.

Manual add

Manufacturer: Axis

Product type: Other

IP address: 10 . 2 . 18 . 222 + Hostname IPv6

HTTP port: 80 +

Authentication: Default logon Specific

Username: root

Password: ••••

Use HTTPS: ON Port: 443

Location: VM11306

Add Close Add and close

- 6 Click **Add and close**.

Encrypting data in transit and at rest with fusion stream encryption (Advanced)

You can enable fusion stream encryption to protect your multimedia streams (video, audio, and so on) in transit and at rest.

What you should know

Data in transit is data that is actively moving from one location to another. Data at rest is data that is stored or archived.

When fusion stream encryption is enabled, unencrypted data streams from your cameras are encrypted by the Archiver role. On request, encrypted data is sent to the requesting client where it is decrypted for presentation. If your video units support encryption, and are connected to the Archiver using HTTPS, then the video is encrypted end-to-end.

To set up fusion stream encryption

- 1 [Request and install the encryption certificates](#) on the client machines that are authorized to access your company's private data.
- 2 [Enable encryption on your Archiver or individual cameras.](#)

After you finish

For more information, refer to "What is fusion stream encryption?" in the *Security Center Administrator Guide*.

Requesting and installing encryption certificates (Advanced)

To authorize a client machine to view encrypted data, you must request an encryption certificate from the client machine. You then install the certificate with the private key locally, and transfer the public portion of the certificate to the Archiver responsible for encryption.

Before you begin

There are many ways to request and manage [digital certificates](#). Before you proceed, consult your IT department about your company's policies and standard procedures.

What you should know

The encryption certificate contains a pair of public and private keys. The public key is used by the Archiver to encrypt the private data for a specific client machine. The private key is used by the client machine to decrypt the private data.

BEST PRACTICE: The private key should never leave the machine on which it is needed.

To request and install an encryption certificate on a client machine:

- 1 Log on as a local administrator of the client machine.
- 2 [Add the Certificates snap-in to your local computer account.](#)
Installing the certificates in the local computer store gives you more control over the management of private keys.
- 3 Follow your company's procedure for requesting and installing the certificate.
- 4 If the client is supposed to have access to encrypted data for a limited time, set the certificate's expiry date accordingly.

- 5 If you do not plan to run Config Tool from this computer, [export the certificate with only the public key to a certificate \(.cer\) file](#).
Save the certificate file to a location that can be accessed from the workstation from which you plan to run Config Tool.

After you finish

[Enable encryption on your Archiver or individual cameras.](#)

Enabling fusion stream encryption (Advanced)

To protect the privacy of your data, you can enable fusion stream encryption.

Before you begin

[Request and install the encryption certificates](#) on the client machines authorized to access your company's private data.

What you should know

Only the public portion of the certificate must be installed on the Archiver.

Encryption certificates are applied through Config Tool. It is not necessary to install certificates on the Archiver server. To apply certificates, Config Tool must have access to the required certificates in the certificate store on the local machine, or exported certificate (.cer) files.

IMPORTANT: To enable encryption, you must add at least one certificate to the Archiver.

To enable fusion stream encryption:

- 1 From the Config Tool home page, open the *Video* task, and click the **Roles and units** view.
 - 2 Do one of the following:
 - To enable encryption for all cameras connected to an Archiver, select an Archiver role to configure, and click the **Camera default settings** tab.
 - To enable encryption for a specific a camera, select the camera, click the **Recording** tab, and then ensure **Recording settings** is set to **Custom settings**.
 - 3 Click **Show advanced settings** and set **Encryption** to **In transit and at rest**.
 - 4 Under the *Certificates* table, click **Add an item** (+).
- The *Select certificate* dialog box opens.
- 5 If the encryption certificates are already installed to the certificate store on the local machine, select them from the *Installed certificates* table, and click **OK**.
 - 6 If the encryption certificates are not installed, find and install them:
 - a) Select **Browse certificate file**, and click **Browse certificate file** (...).

The *Open* dialog box opens.

 - b) Navigate to the folder where the certificates files are saved.
The browser looks for **X.509 Certificates** files by default. If you do not find the required files, set it to look for **Personal Information Exchange** files instead.
 - c) Select the certificates to install, and click **Open**.
 - d) If a certificate file is password-protected, click the advanced show icon (⊕) and enter the password.
 - e) (Optional) Click **Validate file** to make sure the selected file contains a public key.
 - f) Click **OK**.
 - 7 Click **Apply**.

The Archivers start encrypting all data streamed from the selected cameras. Only client workstations with one or more of the configured certificates are able to view the encrypted streams from now on.

Deactivating unused services on video units (Advanced)

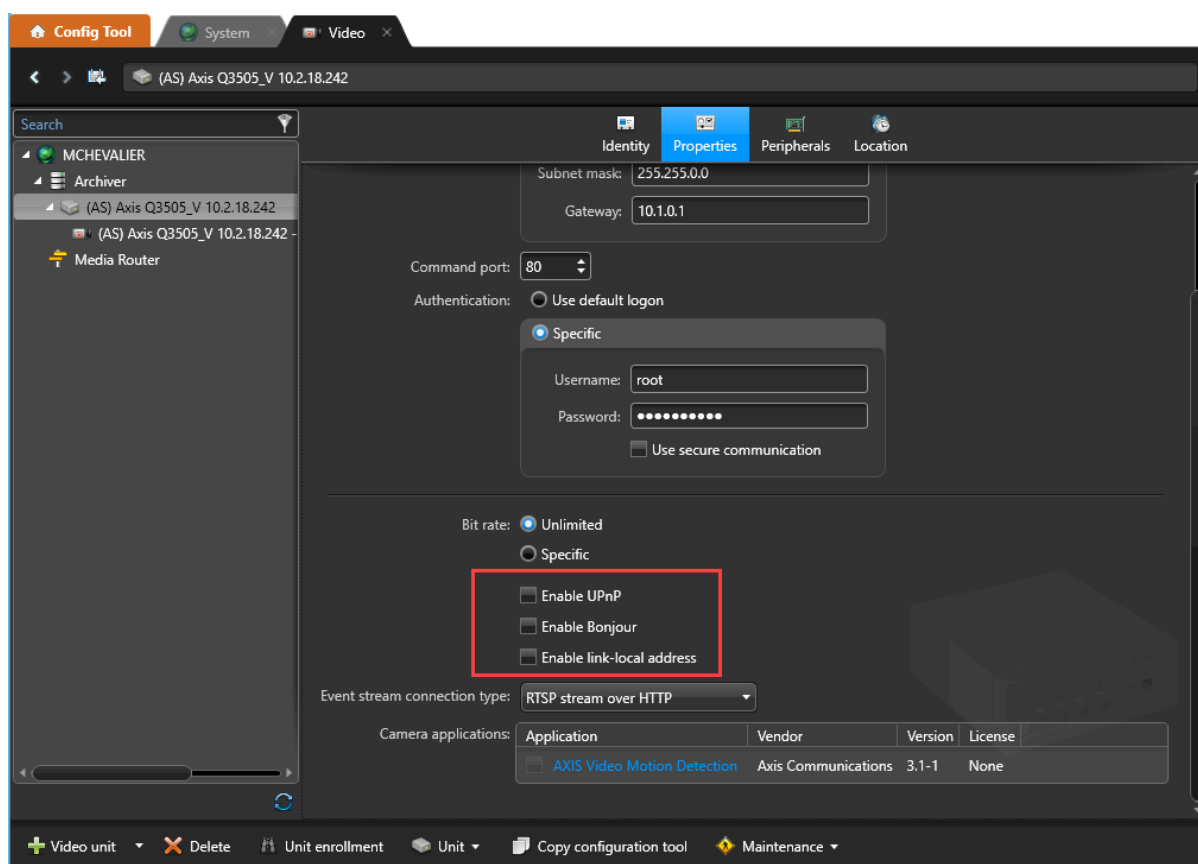
As a defense-in-depth strategy, you can deactivate any unused services and roles to reduce this risk. This reduces the number of active services in your system, and therefore the attack surface.

To deactivate unused services on video units:

- 1 From the Config Tool home page, open the *Video* task.
- 2 Select a video unit from the entity browser.
- 3 In the **Properties** tab, clear the unused services.
- 4 Click **Apply**.

Example

For an Axis Q3505-V network camera, the services that should be disabled are UPnP, Bonjour, and link-local address.



Access Control

This section includes the following topics:

- ["Using dedicated users with restricted privileges for connecting to Global Cardholder Synchronizer role \(Basic\)" on page 56](#)
- ["Enabling Secure mode on HID units \(Basic\)" on page 57](#)
- ["Using strong passwords on access control units \(Basic\)" on page 58](#)
- ["Applying critical firmware updates to access control equipment \(Basic\)" on page 59](#)
- ["Applying the latest cumulative security rollup available for Synergis™ units \(Basic\)" on page 60](#)
- ["Using trusted certificates on Synergis™ units \(Advanced\)" on page 61](#)
- ["Disabling the ability to drive output relays from the Synergis™ unit web interface \(Basic\)" on page 64](#)
- ["Using secure reader connections \(Basic\)" on page 65](#)
- ["Deactivating peer-to-peer and global antipassback for the Access Manager role \(Basic\)" on page 66](#)

Using dedicated users with restricted privileges for connecting to Global Cardholder Synchronizer role (Basic)

The Global Cardholder Synchronizer role ensures the two-way synchronization of shared cardholders and their related entities between the local system (sharing guest) where it resides and the central system (sharing host).

The GCS role on a sharing guest system requires a dedicated user on the sharing host system to connect. The dedicated user should not be an administrator of the entire system. Instead, grant minimum required privileges and access rights to the sharing guest.

Enabling Secure mode on HID units (Basic)

Secure mode is available for HID units that support it. When it is enabled, Telnet, FTP, and SSH protocols are disabled, and communication between the HID access control unit and the Access Manager role is encrypted.

Before you begin

The HID Admin password is required to enable Secure mode.

What you should know

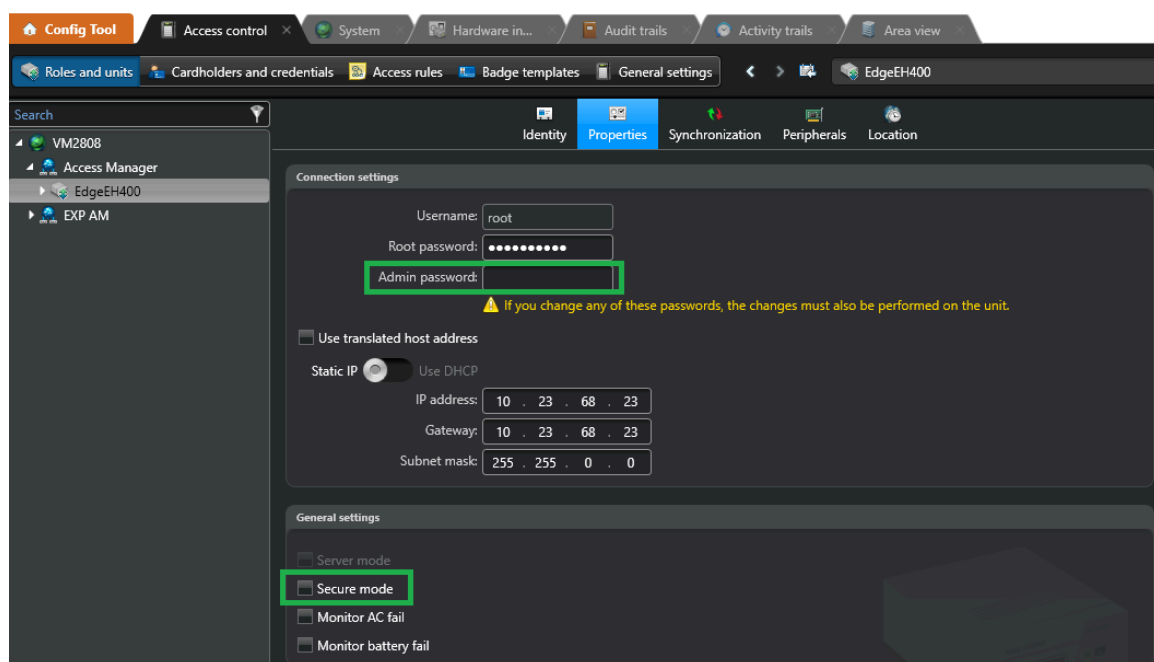
- It is best practice to enable Secure mode on HID access control units because it protects against packet sniffing, replay attacks, and injection attacks.

For supported firmware versions, refer to the *Security Center Release Notes*.

- You can enable Secure mode on HID units when enrolling them in Security Center or after they are enrolled. For more information about how to enroll an HID unit in Secure mode, see "Adding HID access control units" in the *Security Center Administrator Guide*.

To enable Secure mode on enrolled HID units:

- From the Config Tool home page, open the *Access control* task, and click the **Roles and units** view.
- From the entity browser, select an access control unit, and click the **Properties** tab.
- In the *Connection settings* section, enter the **Admin password**.
- In the *General settings* section, select **Secure mode**.



- Click **Apply**.

Using strong passwords on access control units (Basic)

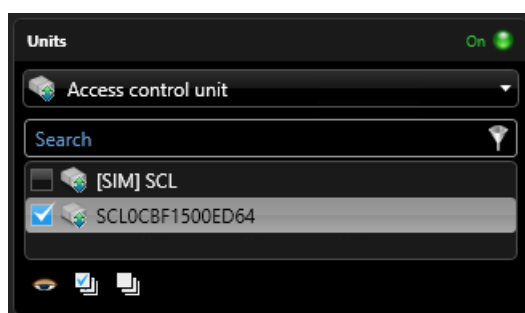
For security purposes, you must change the default passwords on your access control units to strong administrator passwords.

What you should know

A valid administrator password can include all printable ASCII characters from 32-126 (decimal). See <http://www.asciitable.com> for more guidelines.

To use strong passwords on an access control unit:

- 1 Generate a *Hardware inventory* report for the access control unit:
 - a) From the Config Tool home page, open the *Hardware inventory* task.
 - b) Turn on the **Units** filter, and filter by **Access control unit**.
 - c) From the list, select the access control units for which you want to verify the password strength.



- d) Click **Generate report**.
- 2 In the report pane, verify the **Password strength** column.

Unit	Unit type	Manufacturer	Product type	Role	Password strength
SCL0CBF150...	Access control	Genetec	Synergis Cloud Link	Access Manager	Weak

NOTE: Password strength for Synergis™ Cloud Link units is only available with Synergis™ Softwire 11.1 and later.

- 3 Change the password for each unit that does not have a **Strong** password.
 - For Synergis™ units, use one of the following:
 - Synergis™ Appliance Portal
For more information, see "Changing the default administrator password for the Synergis™ unit" in the *Synergis™ Appliance Configuration Guide*.
 - Config Tool
For more information, see "Changing Synergis™ unit passwords in Config Tool" in the *Security Center Administrator Guide*.
 - For third-party controllers, see the documentation provided by the manufacturer.

Applying critical firmware updates to access control equipment (Basic)

To ensure that you have the latest security fixes and improvements, apply critical firmware updates to your access control units and interface modules.

You can upgrade the firmware on your access control units and interface modules in one of the following ways:

- Upgrade your access control units and interface modules in batches in Config Tool.

NOTE: Access control units or interface modules must be of the same product type to be upgraded at the same time.

For more information, see "Upgrading access control unit firmware and platform, and interface module firmware" in the *Security Center Administrator Guide*.

- Upgrade your Synergis™ units and interface modules from the Synergis™ Appliance Portal.

For more information, see "Upgrading Synergis™ Softwire on the Synergis™ appliance" and "Upgrading interface module firmware through the Synergis™ Appliance Portal" in the *Synergis™ Appliance Configuration Guide*.

Applying the latest cumulative security rollup available for Synergis™ units (Basic)

Synergis™ Cloud Link supports the latest security updates in the field with cumulative security rollups. You can apply the latest fixes or patches to security vulnerabilities as they are discovered, using either Config Tool or the Synergis™ Appliance Portal.

You can apply the cumulative security rollup to your Synergis™ units by doing one of the following:

- Apply the cumulative security rollup to one or more Synergis™ appliances at the same time in Config Tool.

For more information, see "Upgrading access control unit firmware and platform, and interface module firmware" in the *Security Center Administrator Guide*.

- Apply the cumulative security rollup to Synergis™ appliances one at a time in Config Tool.

For more information, see "Applying a cumulative security rollup to a Synergis™ appliance through Config Tool" in the *Synergis™ Appliance Configuration Guide*.

- Apply the cumulative security rollup to a Synergis™ appliance from the Synergis™ Appliance Portal.

For more information, see "Applying a cumulative security rollup to a Synergis™ appliance through Synergis™ Appliance Portal" in the *Synergis™ Appliance Configuration Guide*.

Using trusted certificates on Synergis™ units (Advanced)

The authenticity of the self-signed certificate that comes with the unit by default is not enforced as usual with the Public Key Infrastructure. To be more secure, you can use a fully trusted certificate signed by a certificate authority instead.

What you should know

- Using certificates signed by a certificate authority is better for setups where multiple computers and browsers access the Synergis™ unit because you do not need to configure each browser to recognize these trusted certificates.
- Starting in Synergis™ Softwire 10.7, the Synergis™ Cloud Link unit comes with an ECDSA certificate by default. When you try to enroll a new Synergis™ Cloud Link unit on a system running an operating system that lacks support for ECDSA, the enrollment fails because no compatible cipher is available.

If the enrollment fails, upgrade your operating system to one that supports ECDSA or generate a new RSA certificate on the unit and then try enrolling the unit again.

To use certificates signed by a certificate authority:

- 1 Log on to the Synergis™ unit.
- 2 Click **Configuration** > **Certificates**.

- 3 In the *Certificate management* section, complete the identification fields.

The **Common name** field contains the Synergis™ unit's hostname by default. The **Subject alternative name** field also contains the hostname by default, but can be edited to a comma-separated DNS list.

NOTE: The **Common name**, **Subject alternative name**, and **Country** fields are mandatory.

Certificate management

⚠ Changes to the certificate settings on this page will cause the unit to appear offline in Security Center until the trusted certificate is reset in Config Tool.

Common name
SCL0CBF15006D8E

Organization
Genetec

Organization unit
Tech doc

Locality
Montreal

State or province
QC

Country
CA

Subject alternative name
SCL0CBF15006D8E

Certificate type
ECDSA 256 bits

Period of validity
50

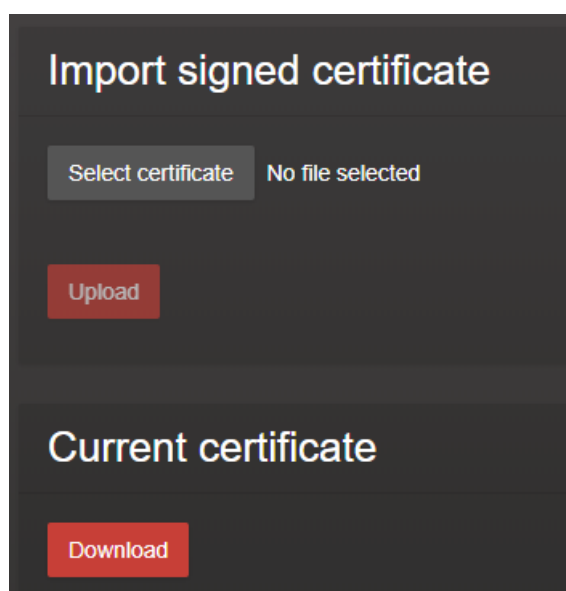
Generate new self-signed certificate

Create certificate signing request

- 4 From the **Certificate type** list, select one of the following algorithms and key lengths:

- ECDSA 256 bits
- ECDSA 384 bits
- RSA 2048 bits
- RSA 3072 bits
- RSA 4096 bits

- 5 Click **Create certificate signing request**.
A *.req* file is generated, containing the public portion of the certificate. The file does not contain the private key and is therefore not confidential.
 - 6 In Windows File Explorer, navigate to your Downloads folder.
 - 7 Copy the signing request *.req* file and send it to a certificate authority.
After verification, the certificate authority signs the public portion of the certificate with its own private key.
 - 8 When you receive the certificates from the certificate authority, log onto the Synergis™ unit and click **Configuration > Certificates**.
 - 9 In the *Import signed certificate* section, click **Select certificate** and browse to the folder with the certificates.
 - 10 Select the first certificate and click **Upload**. Repeat for the remaining certificates.
- NOTE:** Each certificate in the certificate chain must be uploaded individually, or in one operation if you received a *.p7b* collection file. If you received the collection file, you can omit uploading the root certificate.



Your Synergis™ unit will no longer show a security error in the address bar when connecting using hostname.

After you finish

If the Synergis™ unit was already enrolled in Security Center, the Access Manager will not trust the new certificate or connect to the unit, and you must reset the trusted certificate in Config Tool.

For more information, see "Resetting the trusted certificate" in the *Security Center Administrator Guide*.

Disabling the ability to drive output relays from the Synergis™ unit web interface (Basic)

To prevent doors from being unlocked through Synergis™ Appliance Portal, disable the control of output states.

You must change the settings in the Synergis™ Appliance Portal.

NOTE: Your Synergis™ Cloud Link appliance must be running Synergis™ Software 11.0 or later to disable output controls.

For more information about how to do this, see "Disabling output controls in Synergis™ Software" in the *Synergis™ Appliance Configuration Guide*.

Using secure reader connections (Basic)

The protocols used to communicate with readers must be secured because the communication with a reader can be listened to and manipulated by an attacker.

What you should know

Some communication protocols are more secure than others. Follow the recommendations to ensure your reader connections are secure:

- Avoid using the Wiegand protocol
- Use the OSDP v2 protocol with the secure channel mode enabled

NOTE: The reader must be online for the connection settings to be taken into account in the security score.

To use secure reader connections:

- 1 From the Config Tool home page, open the *Access control* task, and click the **Roles and units** view.
- 2 From the entity browser, select an access control unit, and click the **Hardware** tab.
- 3 Click the tabs for your integrations, and change the reader settings follow the recommendations, as required:
 - **Reader type:** The connection is not secure if the reader is **Wiegand** or **Clock and data**.
 - **OSDP:** For OSDP readers, the connection is not secure if the **Reader type** is set to **Raw card reader** and the **Connection settings** are set to either **Unencrypted** or **Encrypted** with a **Default key**.
- 4 Click **Apply**.

Deactivating peer-to-peer and global antipassback for the Access Manager role (Basic)

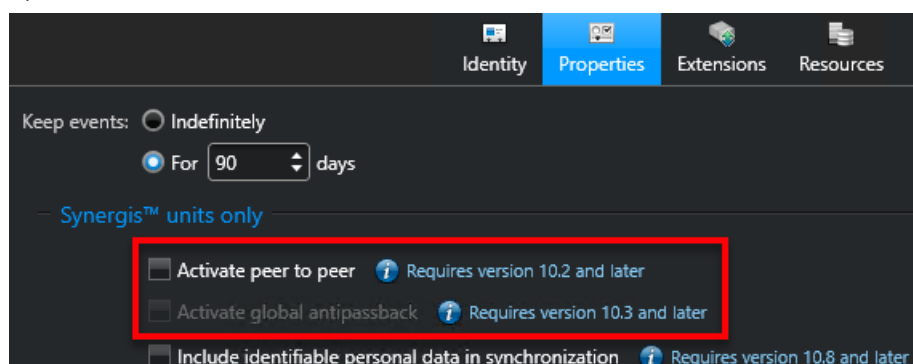
If global antipassback or I/O zones are not used, peer-to-peer and global antipassback should not be activated.

What you should know

Peer-to-peer and global antipassback are deactivated by default.

To deactivate peer-to-peer and global antipassback:

- 1 From the Config Tool home page, open the *Access Control* task and click the **Roles and units** view.
- 2 Select the Access Manager role, and then click the **Properties** tab.
- 3 In the *Synergis™ units only* section, clear the **Activate peer to peer** and **Activate global antipassback** options.



- 4 Click **Apply**.

Logging

This section includes the following topics:

- ["Logging Activity trails for security-related events \(Basic\)"](#) on page 68

Logging Activity trails for security-related events (Basic)

It is considered a best practice to log all security-related events, so they are recorded in the database and available for reporting in the *Activity trails* task.

To log activity trails:

- 1 From the Config Tool home page, open the *System* task, and click the *General settings* view.
- 2 Click the **Activity trails** tab.
- 3 In the *Activity trails* page, select the following options:
 - **Connected to remote Security Desk**
 - **Disconnected from remote Security Desk**
 - **User logged off**
 - **User logged on**
 - **User logon failed**
 - **Trusted certificate reset**
- 4 Click **Apply**.

Web Server

This section includes the following topics:

- ["Changing default Web Server ports \(Basic\)"](#) on page 70
- ["Disabling unlimited session time in Security Center Web Server \(Basic\)"](#) on page 71
- ["Installing a valid certificate on the Security Center Web Server \(Advanced\)"](#) on page 72

Changing default Web Server ports (Basic)

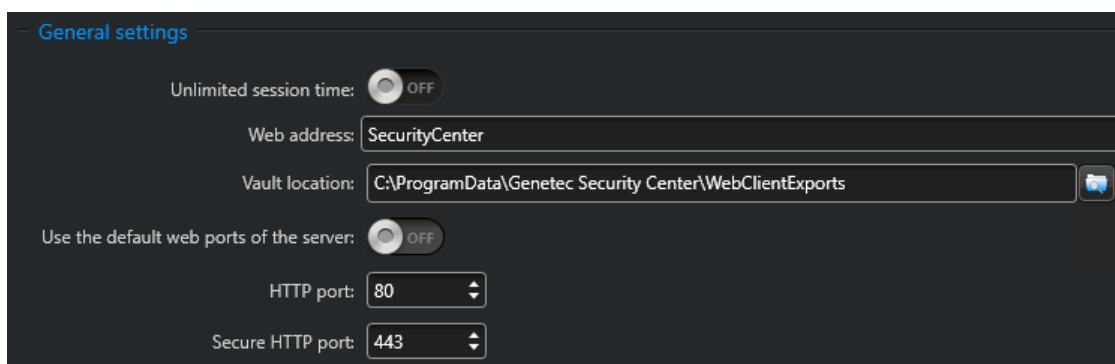
If you do not want to expose your Security Center servers publicly, you can override those ports so that only the mobile role is accessible.

What you should know

By default, the Mobile Server role uses ports 80 and 443.

To restrict your Web Server ports:

- 1 From the Config Tool home page, open the *System* task and click the **Roles** view.
- 2 Open the *Web Server* page from the entity browser and click on the **Properties** tab.
- 3 In the *General settings* section, move the **Use the default secure web ports of the server** slider to **OFF**.
- 4 Enter a new number for your **HTTP port** and **Secure HTTP port**.



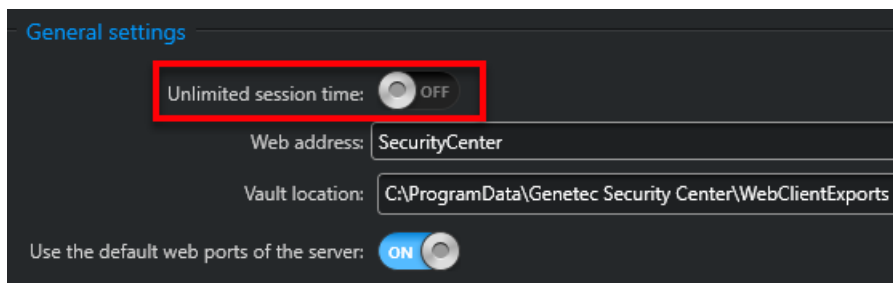
- 5 Click **Apply**.

Disabling unlimited session time in Security Center Web Server (Basic)

In the Security Center Web Server, you can disable **Unlimited session time** to automatically log off users after 12 hours of inactivity.

To disable unlimited session time in Security Center web server:

- 1 From the Config Tool home page, open the *System* task and click the *Roles* view.
- 2 In the entity browser, click **Web Server**.
- 3 In the *General settings* section of the **Properties** tab, move the **Unlimited session time** slider to **OFF**.



- 4 Click **Apply**.

Installing a valid certificate on the Security Center Web Server (Advanced)

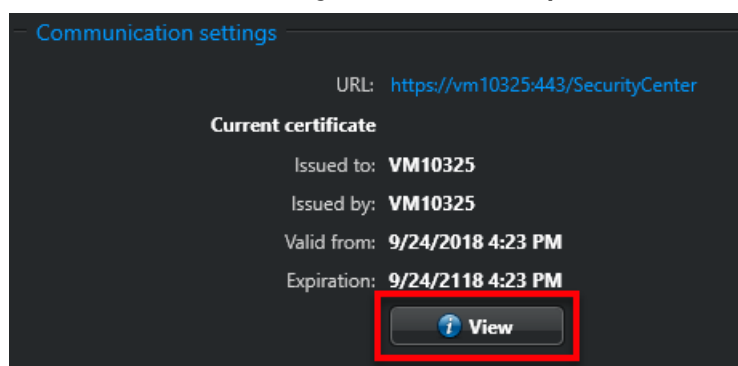
The Web Server role uses the certificate of the Genetec™ Server on which it is running. By default, this is a self-signed certificate. We recommend that you change the self-signed certificate to a certificate signed by a trusted certificate authority.

Before you begin

To change the certificate, you must access Server Admin.

To install a valid certificate on the Security Center Web Server:

- 1 From the Config Tool home page, open the *System* task and select the **Roles** view.
- 2 From the entity browser, open the *Web Server* page.
- 3 In the *Communication settings* section of the **Properties** tab, click **View**.



- 4 In the **General** tab of the *Certificate* window, click **Install Certificate** and follow the *Certificate Import Wizard*.

Genetec™ Mobile

This section includes the following topics:

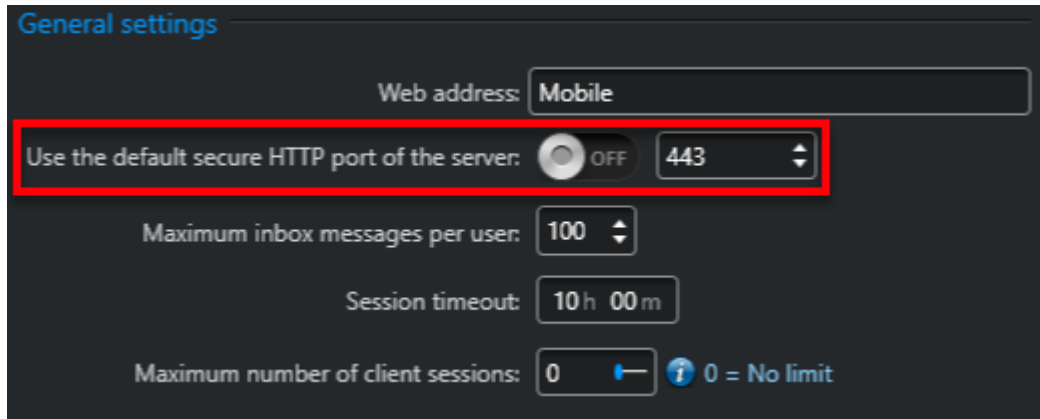
- ["Changing the default Mobile Server port \(Basic\)"](#) on page 74
- ["Always use trusted connections by enforcing certificate validity \(Advanced\)"](#) on page 75
- ["Verifying the list of mobile devices connected to Security Center \(Advanced\)"](#) on page 76

Changing the default Mobile Server port (Basic)

By default, the Mobile Server role uses port 443, which is the same port used by Security Center servers. If you do not want to expose your Security Center servers publicly, you can override those ports so that only the mobile role is accessible.

To change your Mobile Server port:

- 1 From the Config Tool home page, open the *System* task and click the **Roles** view.
- 2 Open the *Mobile Server* page from the entity browser and click on the **Properties** tab.
- 3 In the *General settings* section, move the **Use the default secure HTTP port of the server** slider to **OFF** and enter a new **Secure HTTP port** number.



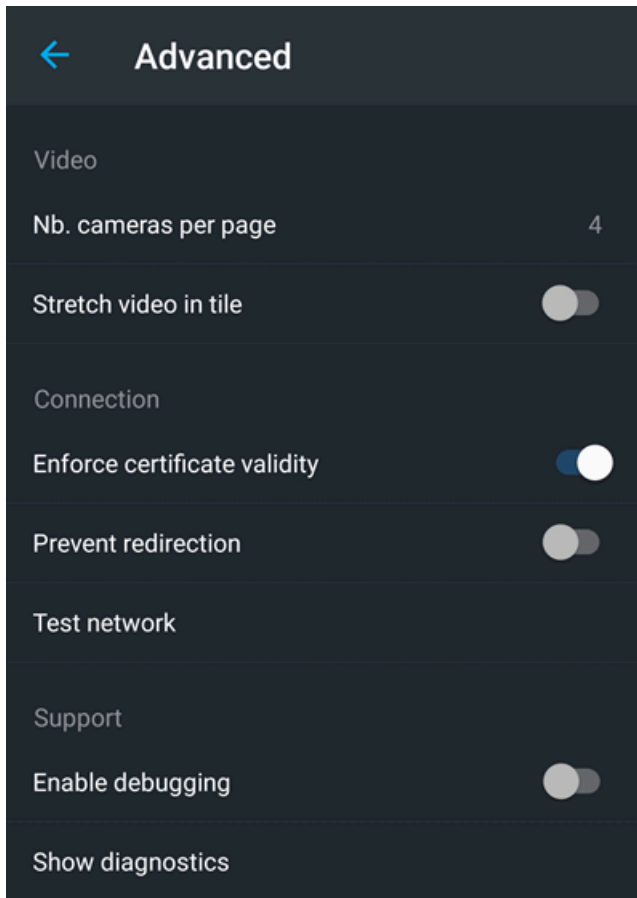
- 4 Click **Apply**.

Always use trusted connections by enforcing certificate validity (Advanced)

For security purposes, the Genetec™ Mobile application should always enforce certificate validity when authenticating a server.

When **Enforce certificate validity** is enabled, the application can only log on to servers that have trusted certificates.

When **Enforce certificate validity** is disabled, the application automatically trusts the certificate when it first connects to a server. If the server certificate changes, you will receive a message when you log on that provides detailed information of the certificate and requests that you to trust this server.

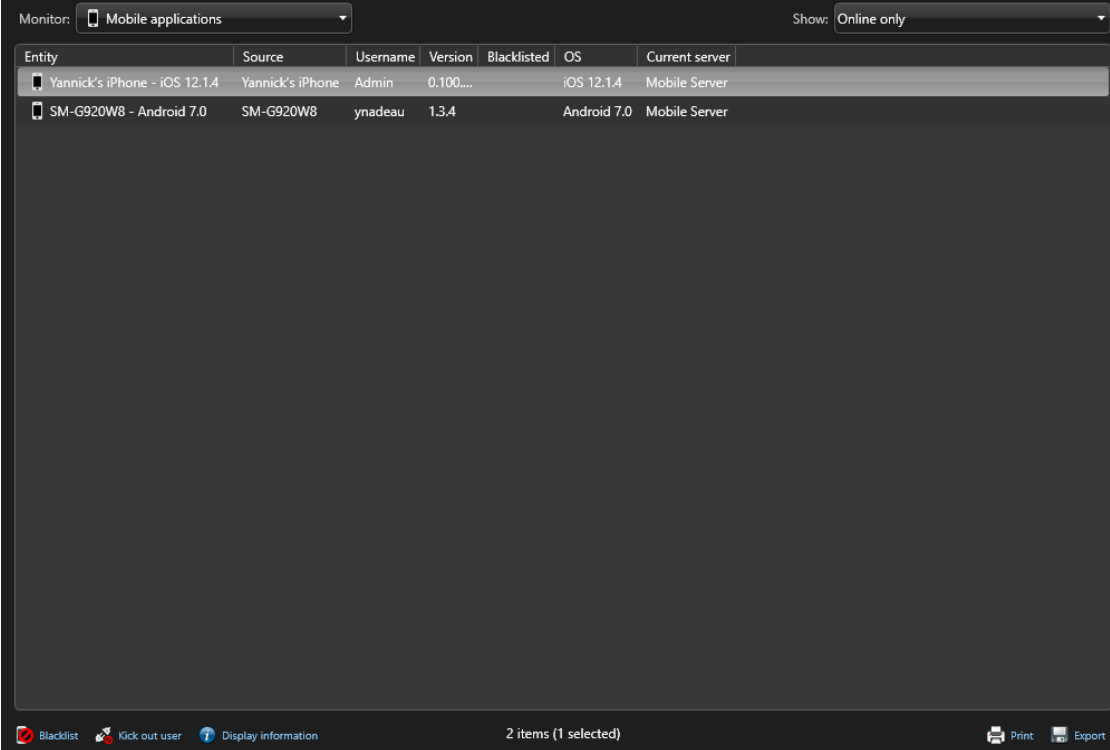


Verifying the list of mobile devices connected to Security Center (Advanced)

Security Center can display which devices are connected to the system. If a mobile device is stolen or lost, you can remove it from the system.

To verify the list of mobile devices connected to Security Center:

- 1 From the Config Tool home page, open the *System status* task.
- 2 From the **Monitor** list, select **Mobile applications**.
- 3 From the **Show** list, select **All entities**.
- 4 If a mobile device from the list must to be removed, do the following:
 - a. Select the entity that you would like to remove.
 - b. Click the blacklist icon (🚫).
 - c. In the pop-up window, click **Yes**.



Entity	Source	Username	Version	Blacklisted	OS	Current server
Yannick's iPhone - iOS 12.1.4	Yannick's iPhone	Admin	0.100...		iOS 12.1.4	Mobile Server
SM-G920W8 - Android 7.0	SM-G920W8	ynadeau	1.3.4		Android 7.0	Mobile Server

License Plate Recognition

This section includes the following topics:

- ["Changing the default administrator password on a SharpV camera \(Basic\)"](#) on page 78
- ["Encrypting the connection to the SharpV web portal \(Basic\)"](#) on page 79
- ["Using the LPM protocol to connect SharpV cameras with Security Center \(Basic\)"](#) on page 83
- ["Changing the default password of a SharpX unit \(Basic\)"](#) on page 85
- ["Encrypting the connection to the SharpX web portal \(Basic\)"](#) on page 86
- ["Restricting access to the AutoVu™ root folder \(Basic\)"](#) on page 87
- ["Using a network location for the AutoVu™ root folder \(Advanced\)"](#) on page 88
- ["Encrypting communication between Genetec Patroller™ and Security Center \(Basic\)"](#) on page 89
- ["Encrypting the Genetec Patroller™ database \(Advanced\)"](#) on page 91
- ["Restricting access to the Genetec Patroller™ workstation \(Basic\)"](#) on page 92
- ["Selecting a Genetec Patroller™ logon type \(Basic\)"](#) on page 93
- ["Disabling Simple Host functionality in Genetec Patroller™ \(6.5 SR1 and later\) \(Basic\)"](#) on page 94

Changing the default administrator password on a SharpV camera (Basic)

When setting up a new SharpV camera, the default password should be changed to a long, random and unique password that is not shared with any other users. The password should contain uppercase and lowercase letters, numbers and non-alphanumeric characters.

What you should know

The SharpV Portal will indicate if the password is considered weak, strong or very strong. It is recommended to set a strong or very strong password as defined on the webpage.

To change the default password of a SharpV unit:

- 1 In the Sharp Portal, open the *Security* page from the **Configuration** menu.
- 2 In the **Access** section, click **Modify password**.
- 3 Enter your old password, then enter and confirm your new password.
- 4 Click **Apply**.

Encrypting the connection to the SharpV web portal (Basic)

If you are using SharpOS 12.6 or earlier, it is recommended that you use an HTTPS connection while connecting to the Sharp Portal. This requires a certificate that is either self-signed or issued by a trusted certificate authority (CA) to be installed on the SharpV camera. SharpOS 12.7 GA and later cannot operate without HTTPS and require the use of a certificate. A self-signed certificate will be automatically created for the unit that did not already have one.

- In the *AutoVu™ SharpV Deployment Guide* guide, read about why the connection to the SharpV web portal should be encrypted.

IMPORTANT: To add the SharpV to the Archiver using HTTPS with a self-signed certificate, you must modify the Archiver's HTTPS options using the instructions in [KBA-01405](#).

- If you are adding the SharpV to the Archiver using HTTPS, configure the camera's network configuration to use a static IP address before you install a certificate.
- The first time you log on to the SharpV web portal, the system logs you on using HTTP mode (no certificate). Your organization's security policy might require that you configure either a self-signed certificate or a signed certificate from a trusted certificate authority.
- You must install the certificate on all machines that communicate with the SharpV camera, which includes the ALPR Manager, the Archiver, and all machines that connect to the web portal
- You can install multiple certificates on a SharpV camera and then select a certificate to activate.

IMPORTANT: If the current certificate is a signed certificate, deleting the certificate signing request prevents the certificate from being reinstalled.

Encrypting the connection to the SharpV web portal using a self-signed certificate (Basic)

To connect to the SharpV web portal using an HTTPS connection, you must obtain a certificate that is either self-signed or issued by a trusted certificate authority (CA) and install it on the SharpV camera.

What you should know

SharpOS 12.7 GA and later cannot operate without HTTPS and requires the use of a certificate. A self-signed certificate will be automatically created for the unit that did not already had one.

To encrypt connection to the Sharp Portal using a self-signed certificate:

- 1 On the machine where you want to register the certificate, log on as an Administrator.
- 2 Log on to the Sharp Portal.
- 3 From the **Configuration** menu, select the *Security* page.
- 4 From the **Certificate** section, select **+ Self-signed**.
- 5 Enter the required information for the certificate and click **OK**.
 - The **Country** field requires a two-letter country code.
 - If you are also using the certificate to connect to the Archiver, the **Sharp's common name** (Sharp's IP address if connecting to the Archiver) defined in the certificate must be the Sharp unit's IP address, not the Sharp name.

The message *Operation succeeded* is displayed and the signing request is added to the certificate list.

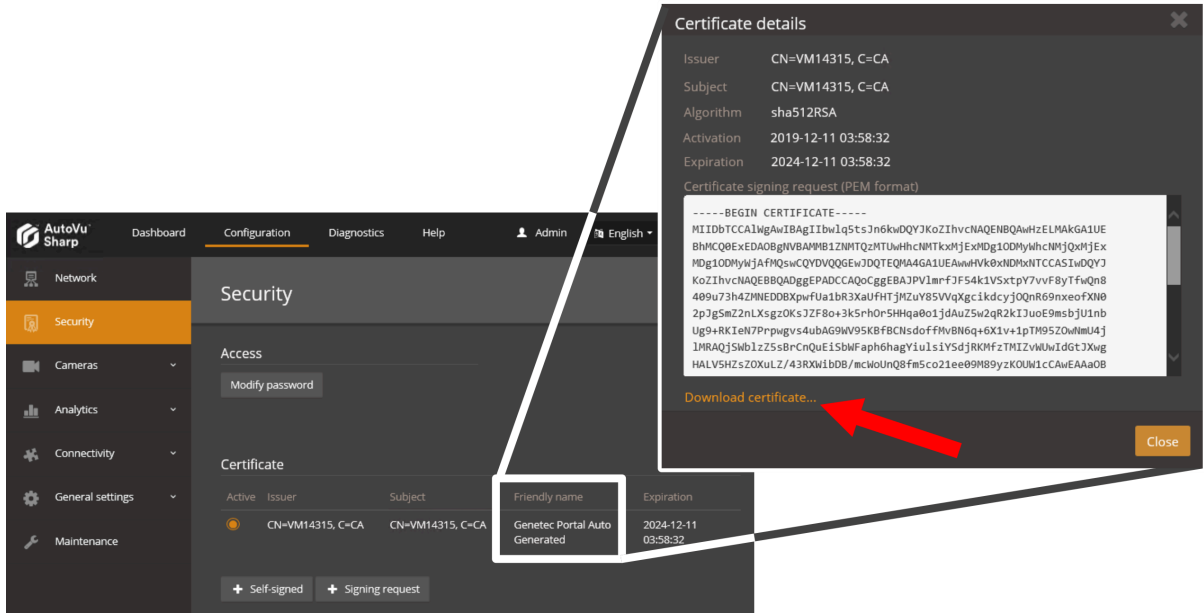
- 6 Click the **Active** button for the certificate.
- 7 Click **Save and reboot** and click **OK** to confirm the reboot.

NOTE: Depending on the browser you are using, you might receive warnings because the certificate is not signed by a trusted certificate authority.

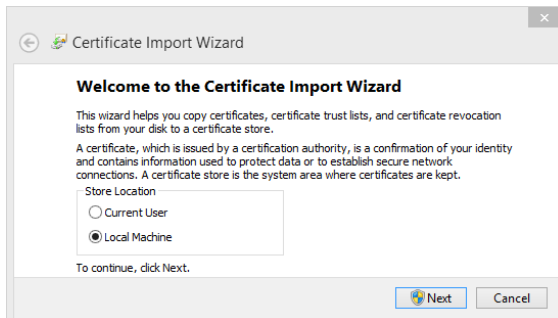
To install the certificate on a workstation:

- 1 Click on the certificate to display the *Certificate details*.

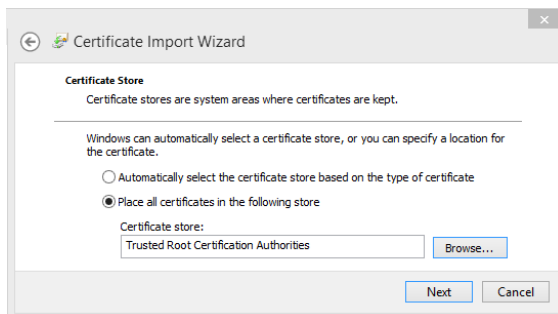
- Click **Download certificate** and save the certificate file as prompted by your browser.



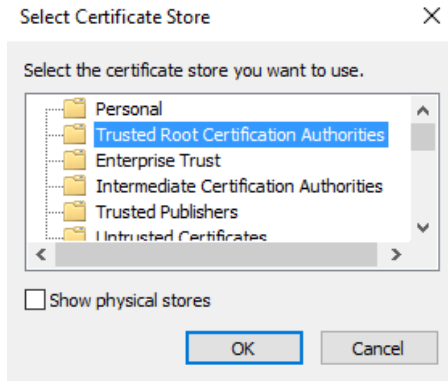
- Double-click the *certificate.cer* file and click **Install Certificate**.
- The *Certificate Import Wizard* prompts you to select a store location. Select **Local Machine** and click **Next**.




- The wizard prompts you to select the certificate store you want to use. Select **Place all certificates in the following store** and click **Browse**.



- From the **Select Certificate Store** window, select **Trusted root certification Authorities** and click **OK**.



- Click **Next** to continue, and click **Finish** to close the wizard.
The system displays the message: *The import was successful.*
- Close all web browsers and open the Windows Task Manager to ensure that no browser processes are running in the background.
- Log on to the Sharp Portal. You are automatically logged on in HTTPS mode.
A lock icon () in the browser's address bar indicates that you are now logged on to the camera with a secure connection.

Encrypting the connection to the SharpV web portal using a certificate issued by a trusted certificate authority (CA) (Basic)

To connect the SharpV web portal using an HTTPS connection, you must obtain a certificate that is either self-signed or issued by a trusted certificate authority (CA) and install it on the SharpV camera.

What you should know

SharpOS 12.7 GA and later cannot operate without HTTPS and requires the use of a certificate. A self-signed certificate will be automatically created for the unit that did not already have one.

To encrypt the connection to the Sharp Portal using a signed certificate:

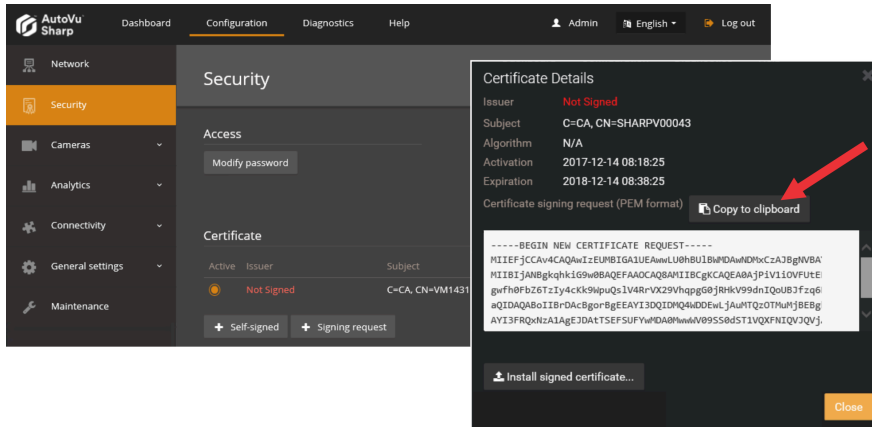
- On the machine where you want to register the certificate, log on as an Administrator.
- Log on to the Sharp Portal.
- From the **Configuration** menu, select the *Security* page.
- Click + **Signing request**.
- Enter the required information for the certificate signing request and click **OK**.

NOTE:

- The **Country** field requires a two-letter country code.
- If you are also using the certificate to connect to the Archiver, the **Sharp's common name** (Sharp's IP address if connecting to the Archiver) defined in the certificate must be the Sharp unit's IP address, not the Sharp name.

The message *Operation succeeded* is displayed and the signing request is added to the certificate list with *not signed* displayed for the **Issuer**.

- Click on the certificate to display the *Certificate details*.

7 Click **Copy to clipboard**.

8 Send the certificate signing request to a certificate authority.

IMPORTANT: Do not delete the signing request if it has been used to request a certificate.

You will receive an SSL certificate signed by the certificate authority.


9 In the *Certificate Details* window, click **Install signed certificate** then browse to the certificate location and click **Open**.10 Click **Save**.

The system displays the message: *Installed signed certificate... successful*.

11 Refresh the browser (F5).

The certificate is displayed in the **Certificate** list.

12 Click the **Active** button for the certificate.13 Click **Save and reboot** and click **OK** to confirm the reboot.

When the system comes back online, notice that the URL displays that you are in HTTPS mode. A lock icon () in the browser's address bar indicates that you are now logged on to the camera with a secure connection.

Using the LPM protocol to connect SharpV cameras with Security Center (Basic)

The License Plate Management (LPM) protocol provides a Sharp camera with a secure and reliable connection to Security Center. When the LPM protocol is enabled on a Sharp camera, the protocol manages the camera's connection to the ALPR Manager role.


Before you begin

- Minimum SharpOS version: 12.7
NOTE: If your camera was shipped with SharpOS 12.7 or later, the LPM protocol is automatically enabled when adding the camera to the ALPR role.
- Minimum Security Center version: 5.8

What you should know

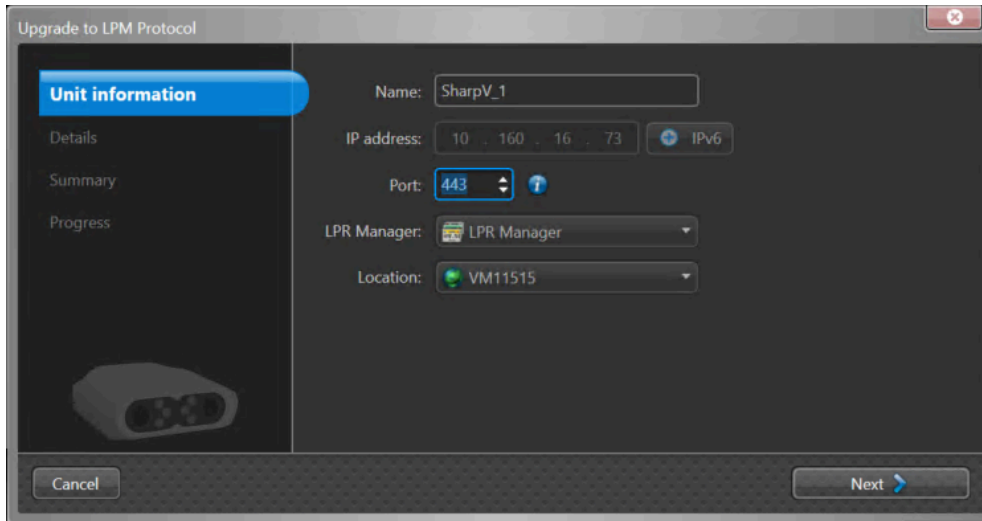
- In addition to upgrading an existing camera to SharpOS 12.7 or later, this procedure updates the Directory database to allow Sharp units to use the LPM protocol.
- If the LPM protocol is enabled on the camera, Security Center can only connect to the camera using the LPM protocol.
- If a camera uses the LPM protocol to connect to Security Center, its extension type in the **Sharp Portal > Configuration > Connectivity > Extension** will be **Security Center (LPM Protocol)**.
- The LPM protocol can be disabled, but you can not revert to the WCF protocol.

To upgrade a SharpV camera to use the LPM protocol:

- 1 From the Config Tool home page, click the *ALPR* task and select **Roles and units**.
- 2 Select the **ALPR Manager** role from the drop-down list.
- 3 Expand the list of cameras under the ALPR Manager and select the SharpV camera.
- 4 At the bottom of the screen, click **Unit** and select **Upgrade to LPM protocol** .
The *Upgrade to LPM Protocol* window opens.
- 5 Enter a **Name** for the camera.
- 6 Enter the IPv4 or IPv6 **IP address** of the camera.
- 7 Enter the **Port** of the camera. Use port 443 for HTTPS communication.

NOTE: Avoid entering port 8001, as it refers to the legacy connectivity port. Connecting to this port will prevent Sharp units from using the LPM protocol and will cause them to fall back to less secure legacy protocol.

8 From the **Location** list, assign the camera to an area entity.

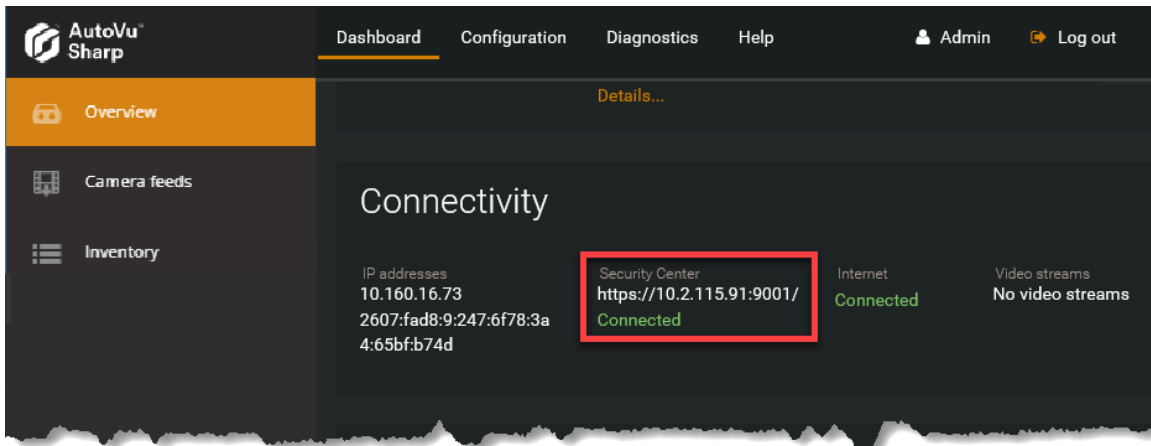


9 Click **Next**.

10 Enter the **Username** and **Password** used to log onto the Sharp Portal and click **Next**.

11 Review the settings and click **Create**.

- The new camera is added under the selected ALPR Manager.
- The Sharp Portal shows that the camera is connected to Security Center.



Changing the default password of a SharpX unit (Basic)

All SharpX units ship with the same default factory password. During its configuration, it is recommended that you replace the default password with a long, unique and random password.

To change the default password on a SharpX unit:

- 1 Open the Sharp Portal and select the *Status* page.
- 2 In the **Actions** section, click **Change password**.

The screenshot displays the Genetec Sharp Portal interface for a SharpX unit. The interface includes a navigation bar with 'Status', 'Configuration', 'Live feed', and 'Diagnostics' tabs. The 'Status' page is active, showing various system information and actions.

Properties:

- Name: SHARPX0527
- IP address: 10.160.80.10
- MAC address: 00-19-0F-14-DC-DD
- Serial number: G2369510061430014
- Type: Sharp X - X2S
- Version: N/A
- Inputs: 4
- Relays: 4
- GPS: Not supported
- Video port: 80

Actions:

- Reboot Sharp
- File versions...
- Change password... (highlighted with a red box)
- Free space on the disk
- Configure the other unit...

System resources:

CPU	Usage (%)	Memory	Free Space (MB)	Total Space (MB)	Used (%)
0	46.71	RAM	1,544	2,135	27.66
1	38.95	D:\	336	839	59.93
2	28.27	E:\	2,468	2,603	5.18

Other Status:

- License: Valid
- Diagnostics: Export settings..., Import settings...
- Remote assistance: Activate
- GPS coordinates: Longitude: ?, Latitude: ?
- Clock: Remote clock is synchronized
- Firmware: Firmware is up to date

- 3 Enter and confirm your new password.
- 4 Click **OK**.

Encrypting the connection to the SharpX web portal (Basic)

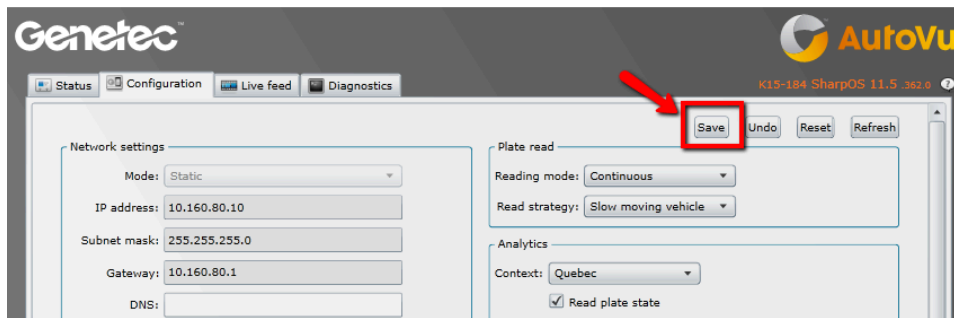
It is recommended that you use an HTTPS connection while connecting to the Sharp Portal. This requires a certificate that is either self-signed or issued by a trusted certificate authority (CA) to be installed on the SharpX camera.

Encrypting the connection to the SharpX portal using a self-signed certificate (Basic)

To connect to the SharpX web portal using an HTTPS connection, you must obtain a certificate that is either self-signed or issued by a trusted certificate authority (CA) and install it on the SharpX camera.

To configure an HTTPS connection to the Sharp Portal using a self-signed certificate:

- 1 Open the Sharp Portal and select the *Configuration* page.
- 2 In the **Security settings** section, select **Use HTTPS**, then click on **Show Settings**.
- 3 In the **Security Settings** dialog box, click on **Create self-signed certificate**.
- 4 In the **Create a certificate signing request** dialog box, enter the required information and click **OK**.
- 5 In the **Security Settings** dialog box, click **OK**.
- 6 On the *Configuration* page of the Sharp Portal, click **Save** to complete the installation.



Encrypting the connection to the SharpX portal using a certificate from a certificate authority (Basic)

To connect the SharpX web portal using an HTTPS connection, you must obtain a certificate that is either self-signed or issued by a trusted certificate authority (CA) and install it on the SharpV camera.

To configure an HTTPS connection to the Sharp Portal using a signed certificate:

- 1 Open the Sharp Portal and select the *Configuration* page.
- 2 In the **Security settings** section, select **Use HTTPS**, then click on **Show Settings**.
- 3 In the **Security Settings** dialog box, click on **Create a certificate signing request**.
- 4 In the **Create a certificate signing request** dialog box, enter the required information and click **OK**.
- 5 In the **Security Settings** dialog box, click **Install certificate**.
- 6 Navigate to the signed certificate and click **Open**.
- 7 When the installation is complete, click **OK** on the **Installation Complete** dialog box and **OK** on the **Security Settings** dialog box.
- 8 On the *Configuration* page of the Sharp Portal, click **Save** to complete the installation.

Restricting access to the AutoVu™ root folder (Basic)

The AutoVu™ root folder should be secured and have restricted access as it contains encrypted hotlist and permit files with personally identifiable information.

What you should know

Multiple strategies can be used to restrict access to the folder:

- Set up access permissions to the root folder. The access can be restricted to a specific Windows user used for that sole purpose.
- Restrict physical access to the root folder.
- Encrypt the root folder. Windows BitLocker or equivalent technology can be used for this.

The AutoVu™ root folder is usually found at *C:\Genetec\AutoVu\Rootfolder*.

Using a network location for the AutoVu™ root folder (Advanced)

By moving the AutoVu™ root folder to a network location, you can keep it behind a secure username and password. This can limit exposure and control access of this folder by keeping files in separate locations.

Before you begin

In Windows Explorer, add a root folder to the network location of your choice.

To use a network location for the AutoVu™ root folder

- 1 From the Security Center Config Tool home page, open the *ALPR* task, and click **Roles and units**.
- 2 Select the ALPR Manager you want to configure, then click **Properties**.
- 3 In the **Root folder** section, delete the existing root folder location and enter the network location where added the root folder.

The network drive must begin with \\.

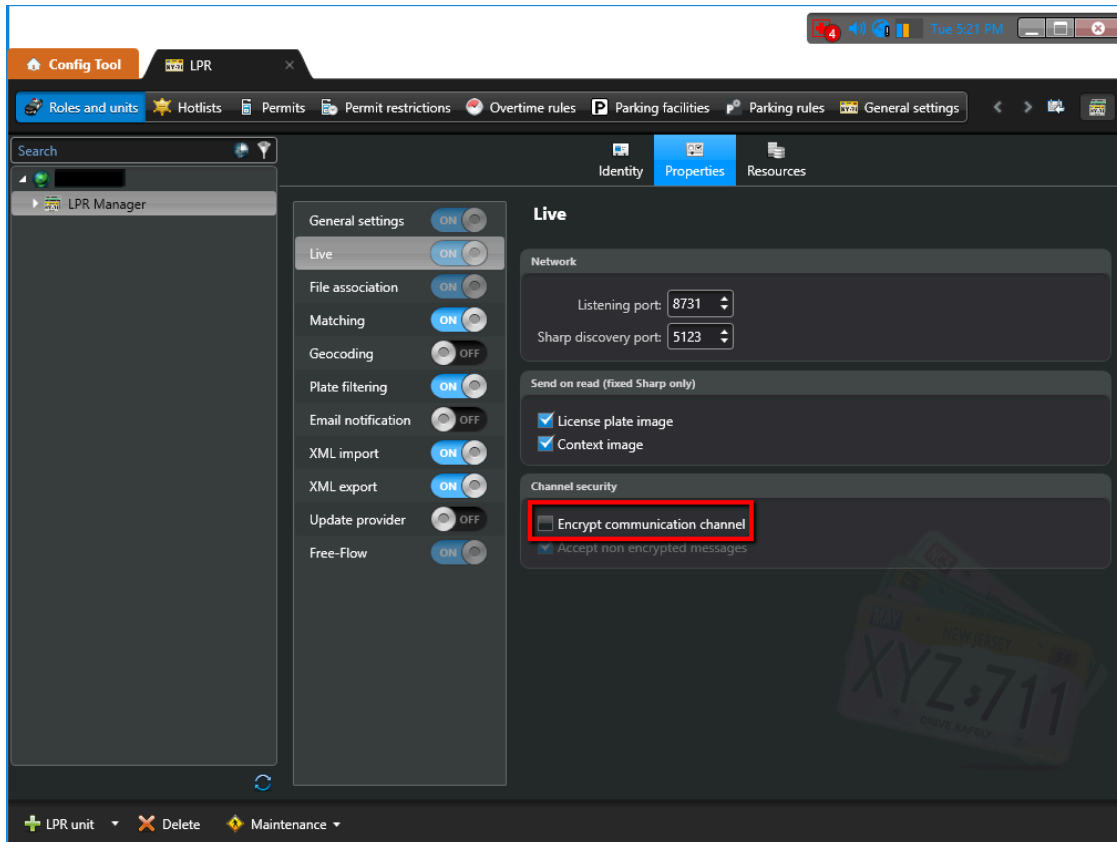
- 4 Enter the **Username** and **Password** to access the network drive.
- 5 Confirm the password and click **Apply**.

Encrypting communication between Genetec Patroller™ and Security Center (Basic)

Enabling encryption between Genetec Patroller™ and Security Center protects the data transferred between the two entities.

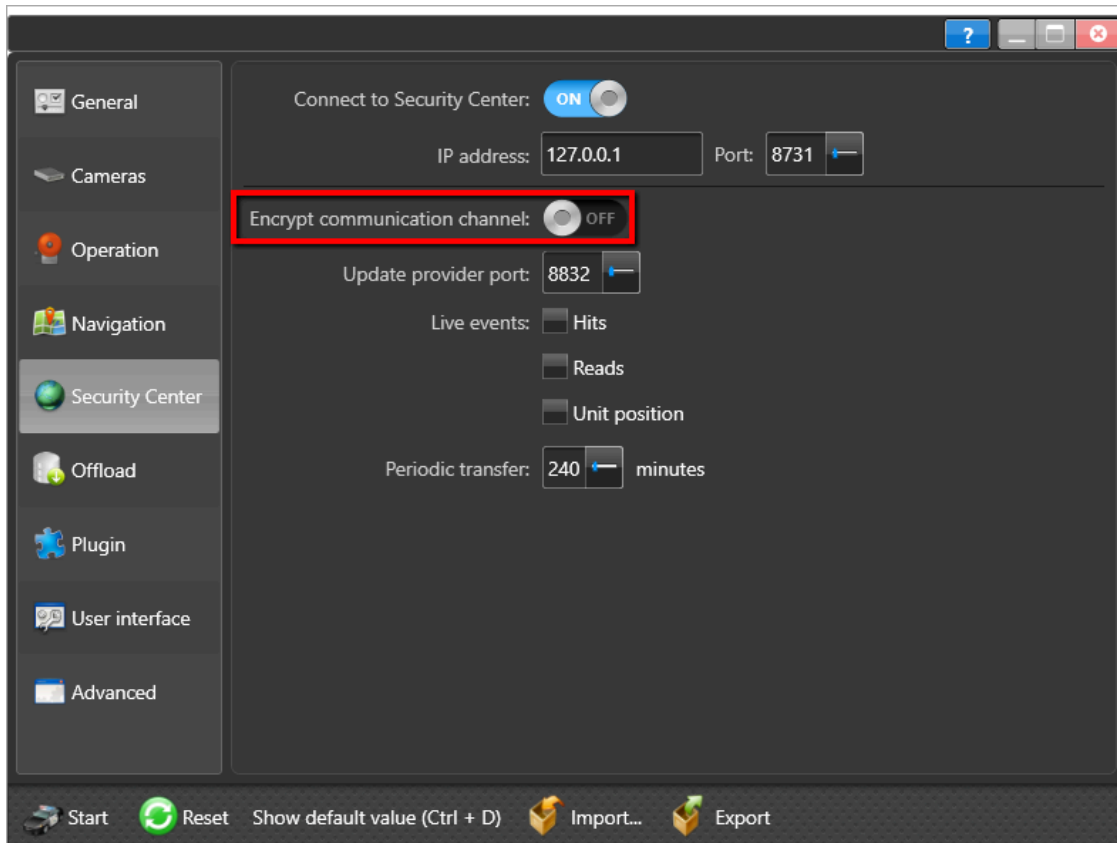
To encrypt communication between Genetec Patroller™ and Security Center:

- 1 From the Security Center Config Tool home page, click the *ALPR* task and select **Roles and units**.
- 2 In the Channel security section of the *Properties* page, select **Encrypt communication channel** and click **Apply**.



- 3 From the Genetec Patroller™ Config Tool home page, open the *Security Center* page.

- 4 Turn on **Encrypt communication channel** and click **Apply**.



Encrypting the Genetec Patroller™ database (Advanced)

Genetec Patroller™ uses a local database and stores some files on disk. To protect the Genetec Patroller™ database, configure Transparent Data Encryption (TDE) in SQL Server.

NOTE: The version of SQL Server that is provided with Genetec Patroller™ does not support Transparent Data Encryption (TDE).

Restricting access to the Genetec Patroller™ workstation (Basic)

The easiest way to protect the Genetec Patroller™ folder and files is to prevent physical access to the machine. Make sure the Genetec Patroller™ laptop is locked in its docking station at all times. If it removed, it should be stored in a secure location.

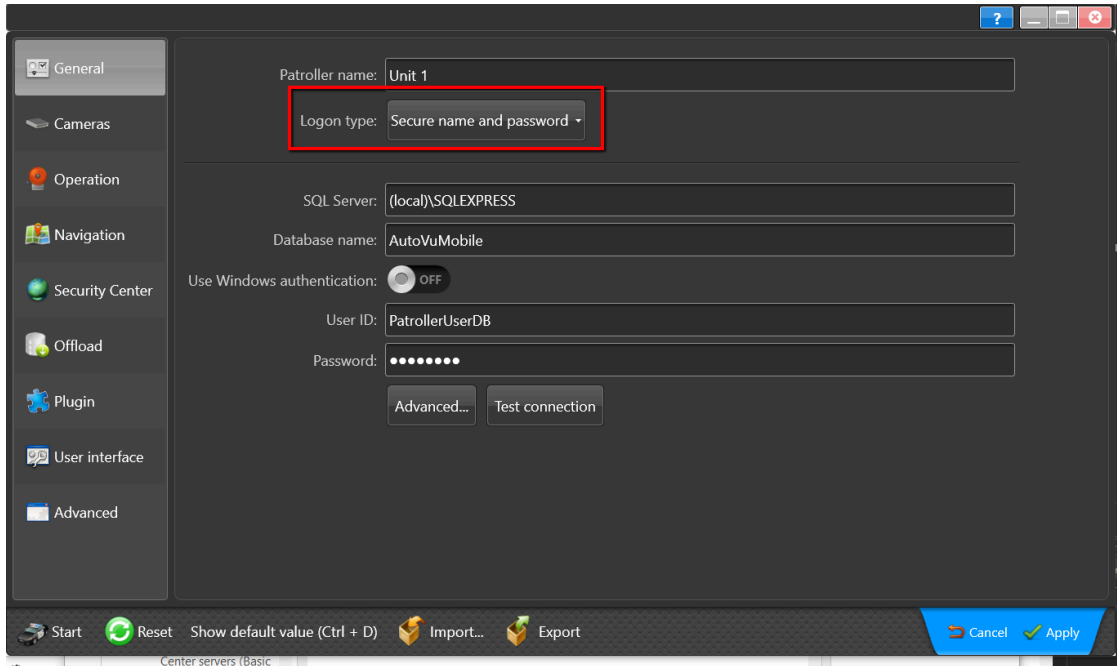
Genetec Patroller™ should be run using a non-privileged Windows account.

Selecting a Genetec Patroller™ logon type (Basic)

By using the Secure username and password logon type in Genetec Patroller™, only authorized users can access the application.

To select your Genetec Patroller™ logon type:

- 1 From the Genetec Patroller™ Config Tool home page, open the *General* page.
- 2 From the **Logon type** list, select **Secure name and password**.



- 3 Click **Apply**.

Disabling Simple Host functionality in Genetec Patroller™ (6.5 SR1 and later) (Basic)

In Genetec Patroller™, SimpleHost is disabled by default. If enabled, communication protocols are not sent securely. Therefore, it is recommended to avoid enabling SimpleHost functionality in Genetec Patroller™ unless it is necessary.

To disable Simple Host functionality in Genetec Patroller™:

- 1 From the Genetec Patroller™ Config Tool home page, open the *Advanced* page.
- 2 Under **Simple Host**, turn off **Use service**.
- 3 Click **Apply**.

Database

This section includes the following topics:

- ["About connecting to SQL Server with an account that has administrative privileges \(Basic\)"](#) on page 96
- ["About the encryption of communication between databases and Genetec™ services \(Basic\)"](#) on page 99
- ["About the encryption of database files \(Advanced\)"](#) on page 100
- ["Authenticating database connections \(Advanced\)"](#) on page 101
- ["Revoke permission to execute certain stored procedures \(Advanced\)"](#) on page 103

About connecting to SQL Server with an account that has administrative privileges (Basic)

Security Center does not require the SQL Sysadmin server role on the database server. Each role requires a different set of permissions.

Server-level roles

A broader set of permissions is necessary during the first execution of Security Center for the creation of the Security Center role databases. Therefore, it is possible to restrict the permission set after the first execution. You can also start with the restricted permission set by creating the required databases outside of Security Center. Refer to the table below for more information.

The Directory role requires the *View server state* permission to work properly. This is mandatory when Directory failover is configured. This permission should always be enabled.

The public server-level role allows the execution of some stored procedure created by default in SQL Server. It is recommended to revoke the execute permission of the *xp_dirtree* stored procedure.

Server-level roles

Roles	public	dbCreator	processAdmin
Access Manager	X	X ¹	X
ALPR Manager	X	X ¹	X
Archiver	X	X ¹	X
Auxiliary Archiver	X	X ¹	X
Directory	X	X ²	X
Health Monitor	X	X ¹	X
Intrusion Manager	X	X ¹	X
Media Router	X	X ¹	X
Mobile Credential Manager	X	X ¹	X
Mobile Server	X	X ¹	X
Plugin: KiwiVision Manager	X	X ¹	X
Point of Sale	X	X ¹	X
Record Caching Service	X	X ¹	X
Unit Assistant	X	X ¹	X
Zone Manager	X	X ¹	X

¹ dbCreator is only necessary if you want Security Center to create the databases for you; and only for the first system execution. You should remove it after the first execution. You also have the option to create empty databases yourself. When the system runs for the first time, the service user creates the tables in the empty databases and therefore the dbCreator role is not needed.

² dbCreator is necessary when using Directory database failover through backup and restore. If database failover through backup and restore is not used, dbCreator is only necessary for the first system execution, and only if you are letting the system create the Directory database.

Database-level roles

Databases are created during the first execution of a Security Center role.

The db_owner role is automatically created on the databases of Security Center roles after their creation. However, they only need the following database-level roles during normal operations:

Database-level roles

Roles	public	db_data reader	db_data writer	db_backup operator	db_ddl admin
Access Manager	X	X	X	X	X
ALPR Manager	X	X	X	X	X
Archiver	X	X	X	X	
Auxiliary Archiver	X	X	X	X	
Directory	X	X	X	X	X
Health Monitor	X	X	X	X	X
Intrusion Manager	X	X	X	X	
Media Router	X	X	X	X	
Mobile Credential Manager	X	X	X	X	X
Mobile Server	X	X	X	X	
Plugin: KiwiVision Manager	X	X	X	X	X
Point of Sale	X	X	X	X	X
Record Caching Service	X	X	X	X	X
Unit Assistant	X	X	X	X	
Zone Manager	X	X	X	X	X

NOTE: Security Center roles require the execute permission on the dbo schema. This permission can be granted by using the following T-SQL command on each database:

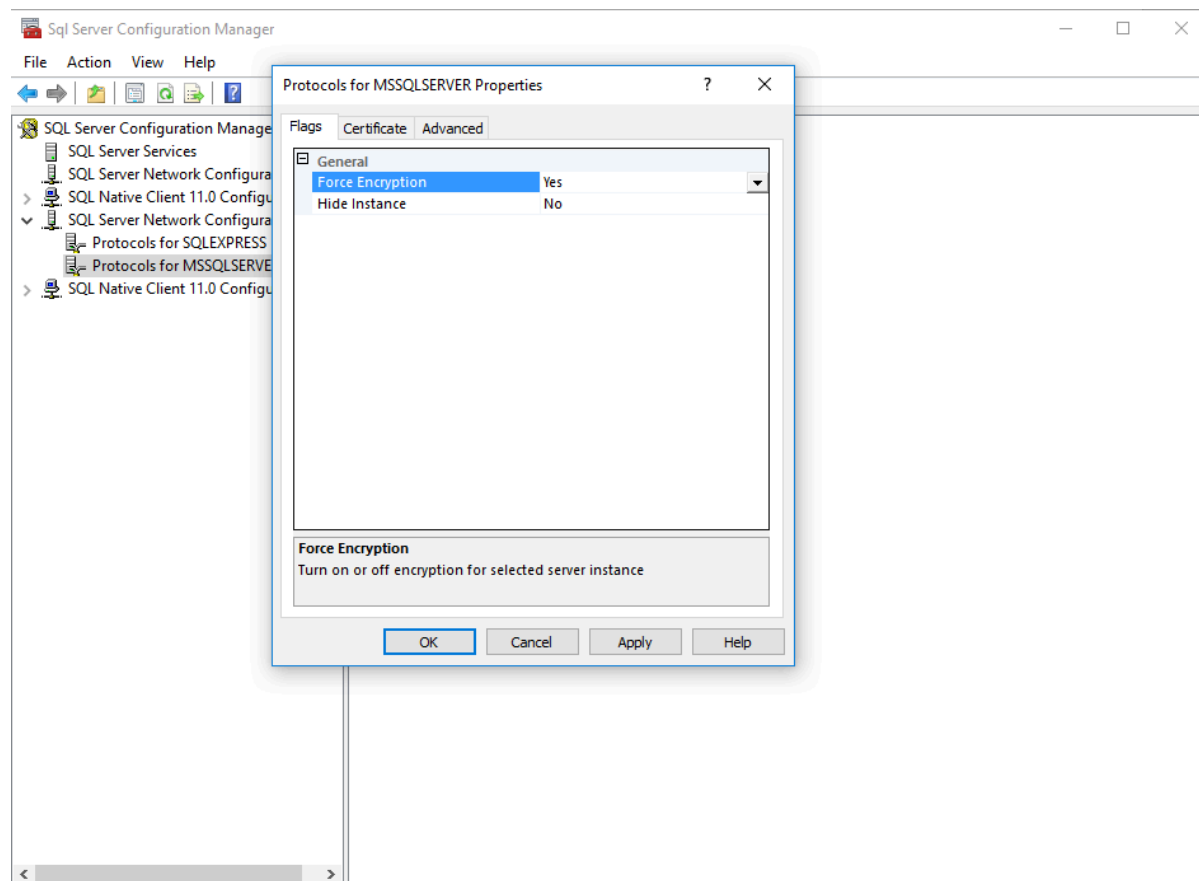
```
GRANT EXECUTE ON SCHEMA::[dbo] TO [ principal used by the Security Center role ]
```


About the encryption of communication between databases and Genetec™ services (Basic)

To protect data while it is in transit, you can configure the SQL service to force the encryption of communication between databases and Genetec™ services.

Encrypting communication can impact performance.

Encrypting communication is configured in the *SQL Server Configuration Manager*. For further information, refer to your SQL Server documentation.



About the encryption of database files (Advanced)

SQL Server offers the option to use Transparent Data Encryption (TDE) to encrypt database data files. This protects data while at rest.

CAUTION: If **Encrypting database data files** is enabled on your SQL server, the performance of your main Directory will decrease by 3% - 5%.

For information on how to encrypt data files, refer to your SQL Server documentation.

Authenticating database connections (Advanced)

To authenticate database connections, you must ensure that the SQL Server uses a Fully Qualified Domain Name (FQDN) certificate that is trusted by the machines that connect to the database.

What you should know

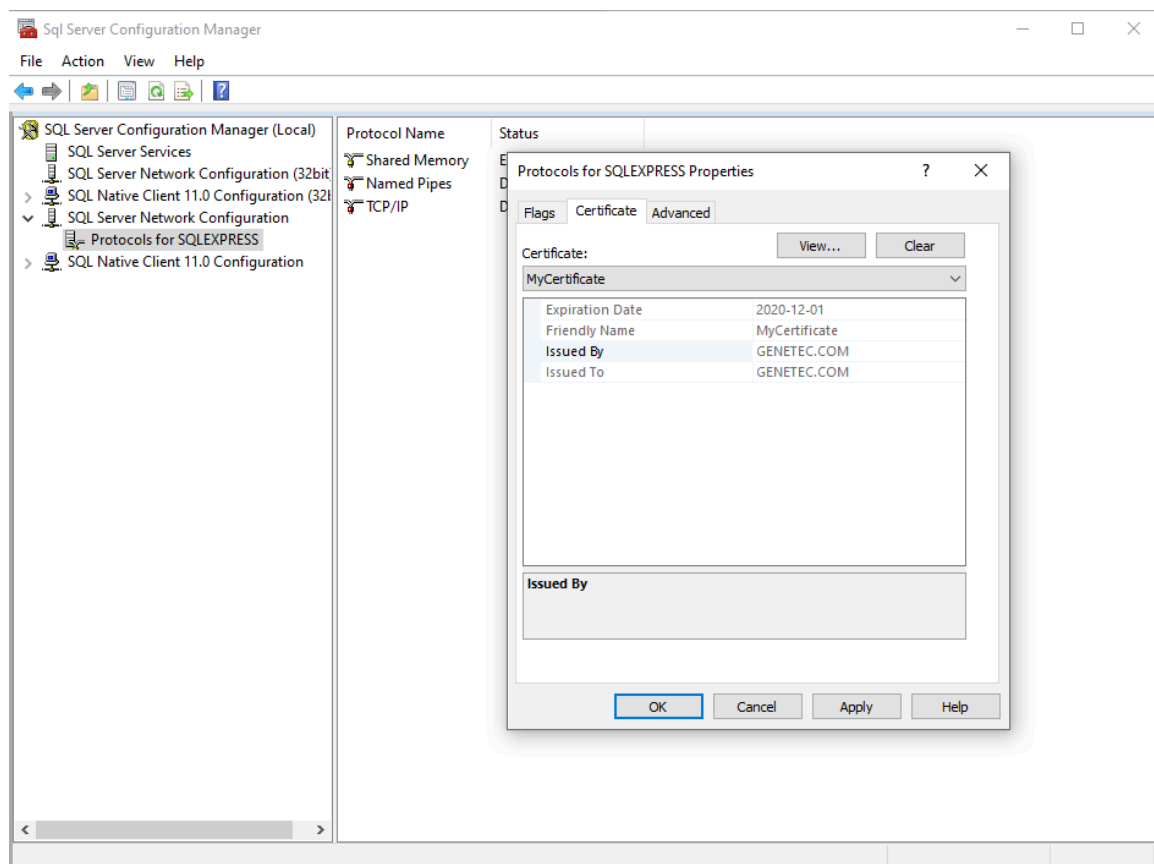
Security Center database connections are always encrypted, but not authenticated by default.

To authenticate database connections:

- 1 In *SQL Server Configuration Manager*, expand **SQL Server Network Configuration**, right-click **Protocols for <SQL_instance>**, and select **Properties**.

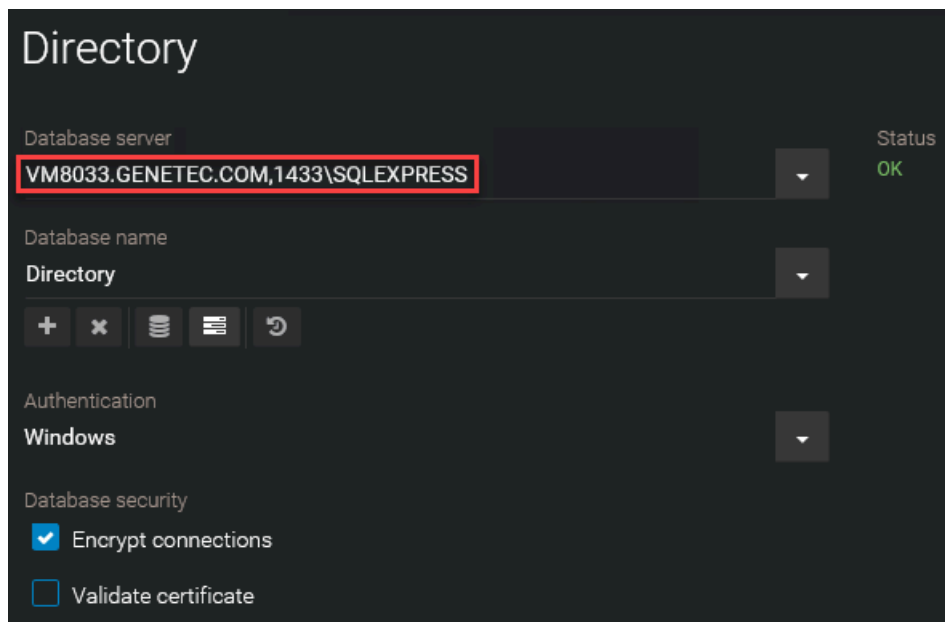
The *Protocols for <SQL_instance>* dialog box opens.

- 2 Under the **Certificate** tab, select the required certificate from the list and click **OK**.

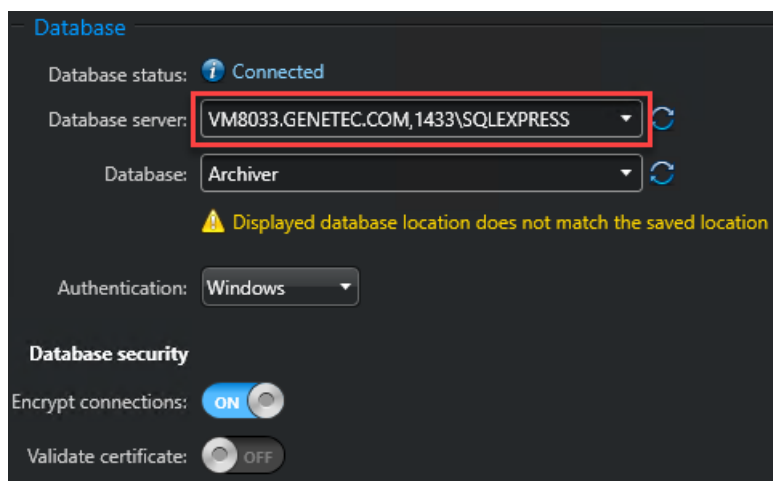


- 3 Under **Protocols for <SQL_instance>**, right-click **TCP/IP**, and select **Properties**.
The *TCP/IP Properties* dialog box opens.
- 4 Under the **Protocol** tab, set **Enabled** to **Yes**.
- 5 Under the **IP Addresses** tab, scroll down to *IPAll* and set **TCP Port** to an allowed value.
- 6 Click **OK**.
- 7 Restart the SQL Server service.

- 8 For the Directory role, do the following:
 - a) In Server Admin, open the main server.
 - b) Under *Directory*, update **Database server** with an FQDN and port.
The required format is: `<FQDN>,<PORT>\<SQL_instance>`



- c) Select **Validate certificate**.
 - d) Click **Save**.
The Directory is restarted before the changes take effect.
- 9 For all other roles that connect to the database, do the following:
 - a) In Config Tool, open **System** > **Roles** and select the role.
 - b) Click the **Resources** tab, and update **Database server** with an FQDN and port.
The required format is: `<FQDN>,<PORT>\<SQL_instance>`



- c) Turn on the **Validate certificate** option.
 - d) Click **Apply**.

After you finish

For more information, see [Enable Encrypted Connections to the Database Engine](#).

Revoke permission to execute certain stored procedures (Advanced)

For security purposes, it is recommended that you revoke permission to execute some of the stored procedures that are created by default in SQL server.

The following SQL command can be used to revoke permission:

```
REVOKE EXECUTE ON [stored procedure] FROM public;
```

The command will block the public server-level role from executing stored procedures. It should be used to block the following procedures:

- xp_availablemedia
- xp_dirtree
- xp_enumgroups
- xp_fixeddrives
- xp_regaddmultistring
- xp_regdeletekey
- xp_regdeletevalue
- xp_regenumvalues
- xp_regremovemultistring
- xp_regread
- xp_regwrite
- xp_servicecontrol
- xp_subdirs

NOTE: Some extended procedures are used by Security Center features, such as backups or health monitoring of the database sizes.

The following extended stored procedures are used by Security Center features, for items such as backups or health monitoring of database sizes:

- xp_dirtree
- xp_fixeddrives
- xp_getnetname

The execute permission on these procedures should be given to the account that is used by Security Center to connect to the database. To provide this permission, use the following command:

```
GRANT EXECUTE ON [stored procedure] TO [Security Center principal]
```

Windows

This section includes the following topics:

- ["Synchronizing all clocks within your system \(Advanced\)"](#) on page 105
- ["About running client applications without administrative privileges \(Basic\)"](#) on page 106
- ["About Windows security baselines \(Basic\)"](#) on page 107
- ["Using BitLocker full volume encryption \(Advanced\)"](#) on page 108
- ["Using safe TLS versions \(Advanced\)"](#) on page 109

Synchronizing all clocks within your system (Advanced)

It is considered best practice to synchronize the clocks on all machines running Genetec™ software using the Windows Time server (W32Time), which is based on the Simple Network Time Protocol (SNTP).

If your network doesn't have a domain controller, manual configurations need to be made. Following the configuration of the time server, it will synchronize the client clock periodically.

Synchronization does not always instantly change the time on the local machine. If the local clock time of the client is less than 3 minutes ahead of the time on the server, W32Time will quarter or halve the clock frequency for long enough to bring the clocks into sync. If the local clock time of the client is more than three minutes ahead of the time on the server, or behind the current time received from the server, W32Time will change the local clock time immediately.

Forcing the use of Active Directory on all client machines and servers running Security Center will enforce strict time synchronization between all users.

For more information about W32Time, see [How the Windows Time Service Works](#).

For more information about configuring W32Time, see [Windows Time Service Tools and Settings](#).

About running client applications without administrative privileges (Basic)

To reduce the damage caused by a compromised application, you can run client applications, such as Security Desk and Config Tool, under a nonadministrative account.

About Windows security baselines (Basic)

A security baseline is a vetted collection of security-focused configuration settings for Windows and other Microsoft products.

To maximize security with increased flexibility and reduced cost, Microsoft recommends deploying an industry-standard security configuration, such as one of their security baselines. For more information about these configurations, refer to [Microsoft Security Baselines](#).

We recommend using the Security Compliance Toolkit (SCT) to deploy the most recent security baseline for your version of Windows. The SCT is a set of tools provided by Microsoft to help deploy security baselines. For more information, refer to [Microsoft Security Compliance Toolkit 1.0](#).

Security baselines for supported versions of Windows and Windows Server:

- [Windows 8.1 and Windows Server 2012 R2](#)
- [Windows 10 and Windows Server 2019, version 2004](#)
- [Windows 10 version 1607 and Windows Server 2016](#)

SQL Server

Outside the security baselines, Microsoft has provided information and security guidance for SQL Server. For more information, refer to [Securing SQL Server](#).

Using BitLocker full volume encryption (Advanced)

BitLocker encryption is a security feature included with all supported versions of Microsoft® Windows and Windows Server. It protects the confidentiality of data at rest by transparently encrypting disk volumes, and is compatible with Security Center.

BEST PRACTICE: Use BitLocker to encrypt storage volumes holding Security Center data.

BitLocker encryption has a performance impact. The extent of the overhead depends on your setup, but BitLocker is generally predicted to have a single-digit percentage impact. For more information, see [BitLocker frequently asked questions \(FAQ\)](#).

For instructions on how to deploy BitLocker in a Windows Server environment, see [BitLocker: How to deploy on Windows Server 2012 and later](#).

For instructions on how to deploy BitLocker in a Windows environment, see [BitLocker basic deployment](#).

Using safe TLS versions (Advanced)

Security Center components use cryptographic protocols to communicate securely. All versions of Secure Sockets Layer (SSL), and early versions of Transport Layer Security (TLS) protocol are vulnerable, so we recommend disabling these protocols in Windows.

BEST PRACTICE: From 2019, disable SSL 3.0 and TLS 1.0. Only use TLS 1.1 if it is still required by other programs in your network.

Some vulnerable protocols might be disabled by default in your version of Windows. For more information on SSL and TLS support, see [Protocols in TLS/SSL \(Schannel SSP\)](#).

For instructions on how to disable cryptographic protocols in Windows, see "SSL 3.0", "TLS 1.0", and "TLS 1.1" in [Transport Layer Security \(TLS\) registry settings](#).

Glossary

action	An action is a user-programmable function that can be triggered as an automatic response to an event, such as door held open for too long or object left unattended, or that can be executed according to a specific time table.
Active Directory	Active Directory is a directory service created by Microsoft, and a type of role that imports users and cardholders from an Active Directory and keeps them synchronized.
Activity trails	The <i>Activity trails</i> task is a maintenance task that reports on the user activity related to video, access control, and ALPR functionality. This task can provide information such as who played back which video recordings, who used the Hotlist and permit editor, who enabled hotlist filtering, and much more.
Archiver	The Archiver role is responsible for the discovery, status polling, and control of video units. The Archiver also manages the video archive and performs motion detection if it is not done on the unit itself.
archive transfer	Archive transfer is the process of transferring your video data from one location to another. The video is recorded and stored on the video unit itself or on an Archiver storage disk, and then the recordings are transferred to another location.
Area activities	The <i>Area activities</i> task is an investigation task that reports on access control events pertaining to selected areas.
Auxiliary Archiver	The Auxiliary Archiver role supplements the video archive produced by the Archiver role. Unlike the Archiver role, the Auxiliary Archiver role is not bound to any particular <i>discovery port</i> , therefore, it can archive any camera in the system, including cameras federated from other Security Center systems. The Auxiliary Archiver role cannot operate independently; it requires the Archiver role to communicate with video units.
automatic license plate recognition	Automatic license plate recognition (ALPR) is an image processing technology used to read license plate numbers. ALPR converts license plate numbers cropped from camera images into a database searchable format.
automatic enrollment	Automatic enrollment is when new IP units on a network are automatically discovered by and added to Security Center. The role that is responsible for the units <i>broadcasts</i> a discovery request on a specific port, and the units listening on that port respond with a message that contains the connection

information about themselves. The role then uses the information to configure the connection to the unit and enable communication.

AutoVu™	The AutoVu™ automatic license plate recognition (ALPR) system automates license plate reading and identification, making it easier for law enforcement and for municipal and commercial organizations to locate vehicles of interest and enforce parking restrictions. Designed for both fixed and mobile installations, the AutoVu™ system is ideal for a variety of applications and entities, including law enforcement, municipal, and commercial organizations.
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.
certificate authority	A certificate authority or certification authority (CA) is an entity or organization that signs identity certificates and attests to the validity of their contents. The CA is a key component of the public-key infrastructure (PKI)
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.
digital certificate	A digital certificate, also known as <i>X.509 certificate</i> , is a digitally signed document that binds the identity of the certificate owner (a person, a computer, or an organization) to a pair of electronic encryption keys. Digital certificates are used for identity verification, asymmetric cryptography, data-in-transit security, and so on. Digital certificates are the basis for the HTTPS protocol.
Directory gateway	Directory gateways allow Security Center applications located on a non-secured network to connect to the main server that is behind a firewall. A Directory gateway is a Security Center server that acts as a proxy for the main server. A server cannot be both

a Directory server and a Directory gateway; the former must connect to the Directory database, while the latter must not, for security reasons.

Directory server	A Directory server is any one of the multiple servers simultaneously running the Directory role in a high availability configuration.
discovery port	A discovery port is a port used by certain Security Center roles (Access Manager, Archiver, ALPR Manager) to find the units they are responsible for on the LAN. No two discovery ports can be the same on one system.
encryption certificate	An encryption certificate, also known as a <i>digital certificate</i> or <i>public-key certificate</i> , is an electronic document that contains a public and private key pair used in Security Center for <i>fusion stream encryption</i> . Information encrypted with the <i>public key</i> can only be decrypted with the matching <i>private key</i> .
event	An event indicates the occurrence of an activity or incident, such as access denied to a cardholder or motion detected on a camera. Events are automatically logged in Security Center. Every event has an entity as its main focus, called the event source.
Federation™	The Federation™ feature joins multiple, independent Genetec™ IP security systems into a single virtual system. With this feature, users on the central Security Center system can view and control entities that belong to remote systems.
fusion stream encryption	Fusion stream encryption is a proprietary technology of Genetec Inc. used to protect the privacy of your video archives. The Archiver uses a two-level encryption strategy to ensure that only authorized client machines or users with the proper certificates on smart cards can access your private data.
Genetec™ Server	Genetec™ Server is the Windows service that is at the core of Security Center architecture, and that must be installed on every computer that is part of the Security Center's pool of servers. Every such server is a generic computing resource capable of taking on any role (set of functions) you assign to it.
Genetec™ Update Service	The Genetec™ Update Service (GUS) is automatically installed with most Genetec™ products and enables you to update products when a new release becomes available.
Global Cardholder Synchronizer	The Global Cardholder Synchronizer role ensures the two-way synchronization of shared cardholders and their related entities between the local system (sharing guest) where it resides and the central system (sharing host).
Hardware inventory	The <i>Hardware inventory</i> task is a maintenance task that reports on the characteristics (unit model, firmware version, IP address,

time zone, and so on) of access control, video, intrusion detection, and ALPR units in your system.

identity certificate	An identity certificate is a <i>digital certificate</i> used to authenticate one party to another in a secure communication over a public network. Identity certificates are generally issued by an authority that is trusted by both parties, called a <i>certificate authority (CA)</i> .
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.
LPM protocol	The License Plate Management (LPM) protocol provides a Sharp camera with a secure and reliable connection to Security Center. When The LPM protocol is enabled on a Sharp camera, the protocol manages the camera's connection to the ALPR Manager role.
load balancing	Load balancing is the distribution of workload across multiple computers.
macro	A macro is an entity that encapsulates a C# program that adds custom functionalities to Security Center.
main server	The main server is the only server in a Security Center system hosting the Directory role. All other servers on the system must connect to the main server to be part of the same system. In a high availability configuration where multiple servers host the Directory role, it is the only server that can write to the Directory database.
Map Manager	The Map Manager is the central role that manages all mapping resources in Security Center, including imported map files, external map providers, and KML objects. It acts as the map server for all client applications that require maps and as the <i>record provider</i> for all Security Center entities placed on georeferenced maps.
Media Router	The Media Router role is the central role that handles all stream requests (audio and video) in Security Center. It establishes streaming sessions between the stream source, such as a camera or an Archiver, and its requesters (client applications). Routing decisions are based on the location (IP address) and the transmission capabilities of all parties involved (source, destinations, networks, and servers).
Media Gateway	The Media Gateway role is used by Genetec™ Mobile and Web Client to get transcoded video from Security Center. The Media Gateway role supports the Real Time Streaming Protocol (RTSP), which external applications can use to request raw video streams from Security Center.

multi-factor authentication	Multi-factor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.
Genetec Mission Control™	Genetec Mission Control™ is a collaborative decision management system that provides organizations with new levels of situational intelligence, visualization, and complete incident management capabilities. It allows security personnel to make the right decision when faced with routine tasks or unanticipated situations by ensuring a timely flow of information. To learn more about Genetec Mission Control™, refer to the Genetec™ resource center .
Mobile Server	The Mobile Server role provides Security Center access on mobile devices.
Omnicast™	Security Center Omnicast™ is the IP video management system (VMS) that provides organizations of all sizes the ability to deploy a surveillance system adapted to their needs. Supporting a wide range of IP cameras, it addresses the growing demand for HD video and analytics, all the while protecting individual privacy.
partition	A partition is an entity in Security Center that defines a set of entities that are only visible to a specific group of users. For example, a partition could include all areas, doors, cameras, and zones in one building.
Plan Manager	(Obsolete) Plan Manager is a module of Security Center that provides interactive mapping functionality to better visualize your security environment. The Plan Manager module has been replaced by the Security Center role, Map Manager, since version 5.4 GA.
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.
private task	A private task is a saved task that is only visible to the user who created it.
task cycling	A task cycling is a Security Desk feature that automatically cycles through all tasks in the active task list following a fixed dwell time.
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.

recording mode

Recording mode is the criteria by which the system schedules the recording of video streams. There are four possible recording modes:

- **Continuous.** Records continuously.
- **On motion/Manual.** Records according to motion detection settings, and when a user or system action requests it.
- **Manual.** Records only when a user or system action requests it.
- **Off.** No recording is permitted.

restricted camera

Restricted cameras are cameras that Genetec Inc. has identified as cybersecurity risks.

Security Center Mobile

(Obsolete) See Mobile Server and Genetec™ Mobile.

self-signed certificate

A self-signed certificate is an *identity certificate* that is signed by the same entity whose identity it certifies, as opposed to a *certificate authority (CA)*. Self-signed certificates are easy to make and do not cost money. However, they do not provide all of the security properties that certificates signed by a CA aim to provide.

sharing guest

A sharing guest is a Security Center system that has been given the rights to view and modify entities owned by another Security Center system, called the sharing host. Sharing is done by placing the entities in a global partition.

sharing host

A sharing host is a Security Center system that gives the right to other Security Center systems to view and modify its entities by putting them up for sharing in a global partition.

SharpV

SharpV is a Sharp unit that is specialized for fixed installations and is ideally suited for a range of applications, from managing off-street parking lots and facilities to covering major city access points to detect wanted vehicles. SharpV combines two high-definition cameras (1.2MP) with onboard processing and illumination in a ruggedized, environmentally sealed unit. Both lenses are varifocal for ease of installation and the camera is powered via PoE+.

SharpX

SharpX is the camera component of the SharpX system. The SharpX camera unit integrates a pulsed LED illuminator that works in total darkness (0 lux), a monochrome ALPR camera (1024 x 946 @ 30 fps), and a color context camera (640 x 480 @ 30 fps). The ALPR data captured by the SharpX camera unit is processed by a separate hardware component called the AutoVu™ ALPR Processing Unit.

Sharp Portal	Sharp Portal is a web-based administration tool used to configure Sharp cameras for AutoVu™ systems. From a web browser, you log on to a specific IP address (or the Sharp name in certain cases) that corresponds to the Sharp you want to configure. When you log on, you can configure options such as selecting the ALPR context (for example, Alabama, Oregon, Quebec), selecting the read strategy (for example, fast moving or slow moving vehicles), viewing the Sharp's live video feed, and more.
Synergis™	Security Center Synergis™ is the IP access control system (ACS) that heightens your organization's physical security and increases your readiness to respond to threats. Synergis™ supports an ever-growing portfolio of third-party door control hardware and electronic locks. Using Synergis™, you can leverage your existing investment in network and security equipment.
Secure Socket Layer	The Secure Sockets Layer (SSL) is a computer networking protocol that manages server authentication, client authentication and encrypted communication between servers and clients.
Transport Layer Security	Transport Layer Security (TLS) is a protocol that provides communications privacy and data integrity between two applications communicating over a network. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).
user level	A user level is a numeric value assigned to users to restrict their ability to perform certain operations, such as controlling a camera PTZ, viewing the video feed from a camera, or staying logged on when a threat level is set. Level 1 is the highest user level, with the most privileges.
video analytics	Video analytics is the software technology that is used to analyze video for specific information about its content. Examples of video analytics include counting the number of people crossing a line, detection of unattended objects, or the direction of people walking or running.
video archive	A video archive is a collection of video, audio, and metadata streams managed by an Archiver or Auxilliary Archiver role. These collections are catalogued in the archive database that includes camera events linked to the recordings.
video sequence	A video sequence is any recorded video stream of a certain duration.
video unit	A video unit is a video encoding or decoding device that is capable of communicating over an IP network and that can incorporate one or more video encoders. The high-end

encoding models also include their own recording and video analytics capabilities. Cameras (IP or analog), video encoders, and video decoders are all examples of video units. In Security Center, a video unit refers to an entity that represents a video encoding or decoding device.

VSIP port

The VSIP port is the name given to the discovery port of Verint units. A given Archiver can be configured to listen to multiple VSIP ports.

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ TechDoc Hub:** The latest documentation is available on the TechDoc Hub. To access the TechDoc Hub, log on to [Genetec™ Portal](#) and click [TechDoc Hub](#). Can't find what you're looking for? Contact documentation@genetec.com.
- **Installation package:** The Installation Guide and Release Notes are available in the Documentation folder of the installation package. These documents also have a direct download link to the latest version of the document.
- **Help:** Security Center client and web-based applications include help, which explains how the product works and provide instructions on how to use the product features. To access the help, click **Help**, press F1, or tap the ? (question mark) in the different client applications.

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](#). Can't find what you're looking for? Contact documentation@genetec.com.

- **Genetec™ Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec™ Lifecycle Management (GLM) documents: [Genetec™ Assurance Description](#) and [Genetec™ Advantage Description](#).

Additional resources

If you require additional resources other than the Genetec™ Technical Assistance Center, the following is available to you:

- **Forum:** The Forum is an easy-to-use message board that allows clients and employees of Genetec Inc. to communicate with each other and discuss many topics, ranging from technical questions to technology tips. You can log on or sign up at <https://gtapforum.genetec.com>.
- **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>.

Licensing

- For license activations or resets, please contact GTAC at <https://portal.genetec.com/support>.
- For issues with license content or part numbers, or concerns about an order, please contact Genetec™ Customer Service at customerservice@genetec.com, or call 1-866-684-8006 (option #3).
- If you require a demo license or have questions regarding pricing, please contact Genetec™ Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Hardware product issues and defects

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