Genetec™ Security Center.

Security Center Hardening Guide 5.9

Click here for the most recent version of this document.

Document last updated: January 28, 2020

Genetec™

Legal notices

Document information

Document title: Security Center Hardening Guide 5.9

Original document number: EN.501.003-V5.9.0.0(2)

Document number: EN.501.003-V5.9.0.0(2)

Document update date: January 28, 2020

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.

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

Chapter 6: Access Control

Chapter 7: Logging

Chapter 8: Web Server

Chapter 9: Genetec Mobile

Chapter 10: License Plate Recognition

Chapter 11: Database

Chapter 12: Windows

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 5.9" 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.

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 5.9

With each release, new features, enhancements, or resolved issues are added to the product.

The Security Center Hardening Guide 5.9 includes the following new enhancements.

- **New topics:**

  - (User Management) Setting passwords for Media Gateway RTSP streaming
  - (System) Disabling backward compatibility for the Map Manager role
  - (Windows) Using BitLocker full volume encryption
  - (Windows) Using safe TLS versions

- **Updated topics:**

  - (Access Control) Applying a cumulative security rollup on a Synergis™ appliance
  - (Access Control) Applying a cumulative security rollup for a Synergis™ appliance through Config Tool
  - (Access Control) Updating firmware on Synergis™ appliances
  - (System) Disabling backward compatibility
  - (Database) About connecting to SQL Server with an account that has administrative privileges
  - (Database) Authenticating database connections

- **Removed topics:**

  - (Access Control) Enabling secure mode on a Synergis™ appliance running Synergis™ Softwire 10.4 or older

User Management

This section includes the following topics:

Changing the default administrator password in Security Center (Basic, Advanced)

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 (Basic, 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 must have a minimum length, complexity, and expiration period for each password.

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 that users receive a warning that their password is set expire.
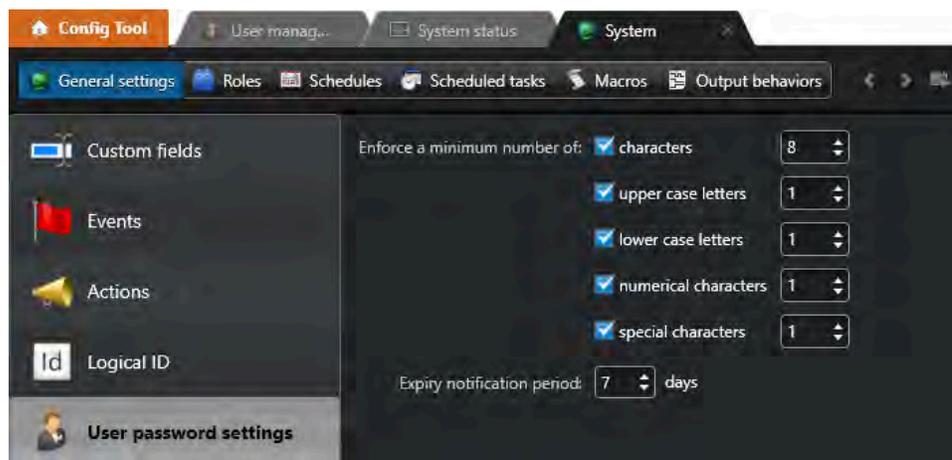
4 Click **Apply**.

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, Advanced)

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.

Before you begin

BEST PRACTICE: Enforce a strong password policy in Security Center.

What you should know

By default, Real Time Streaming Protocol (RTSP) streaming requires user authentication. Any Security Center user account can be used to request these video streams, but a separate Media Gateway password must be set for each RTSP user configured in the role.

Password complexity requirements are enforced for RTSP passwords.

To set a password for Media Gateway RTSP streaming:

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 Under the *Accessible to* list, click **Add an item (** ➕ **)** .
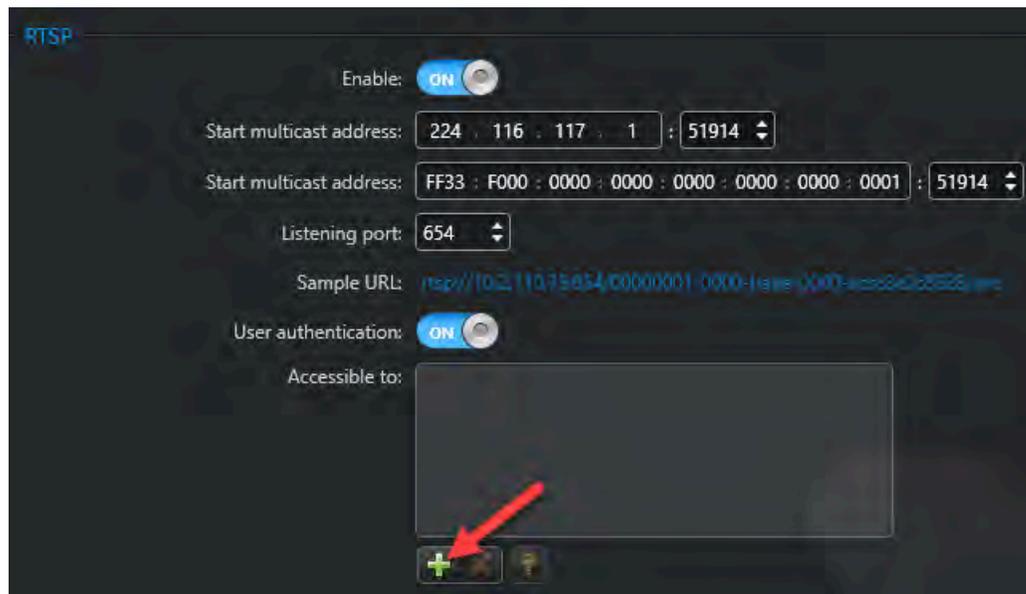
5   Select a Security Center user to grant RTSP access and click **Add**.

The *New password* dialog box opens.

6   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.

7   Click **Apply**.

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

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

What you should know

Only local privileges on the machines are required on you 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 is 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, Advanced)

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.

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.

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

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.
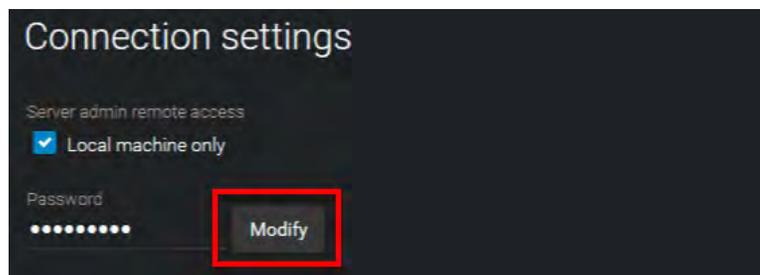
3 Enter your old password, then enter a new password and confirm it.
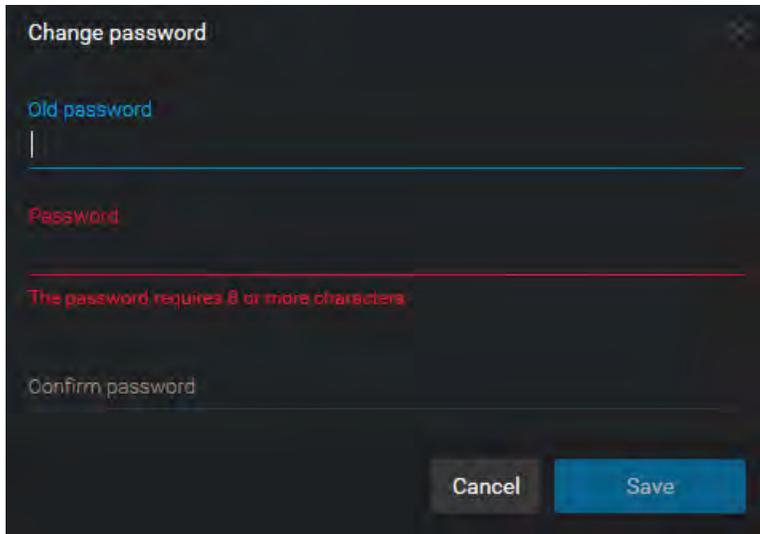
4 Click **Save**.

Activating auto lock on Security Desk workstations (Basic, Advanced)

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 **Overide**.
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, Advanced)

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 including a minimum password length, complexity, and expiration period 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.
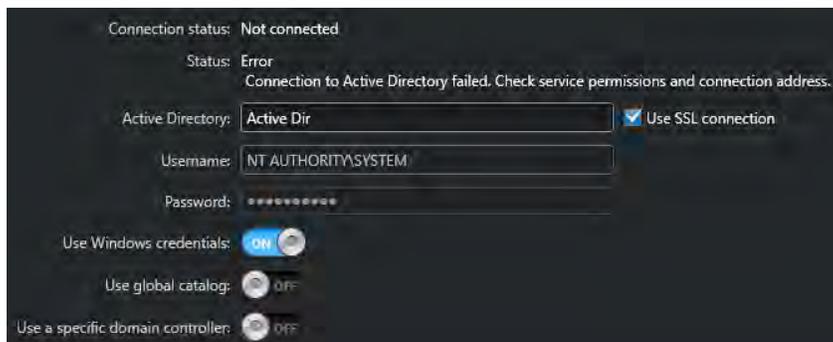
4 Click **Apply**.

Using Active Directory Federation Service (ADFS) to authenticate a Security Center user (Advanced)

Claims-based authentication allows external users to log on to Security Center if your organization's IT service cannot verify their identity.

Claims-based authentication can be enacted using an Active Directory Federation Service (ADFS).

For more information on claims-based authentication, consult the *Security Center Administration 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**.
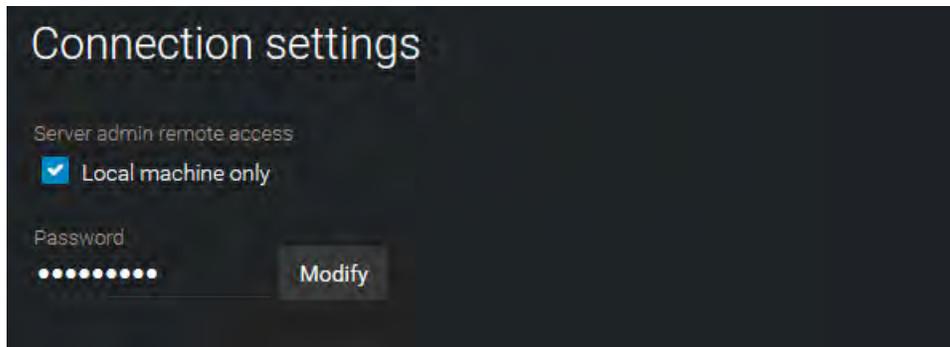
This option only allows the Server Admin to be accessed from the local machine.

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 grated 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.
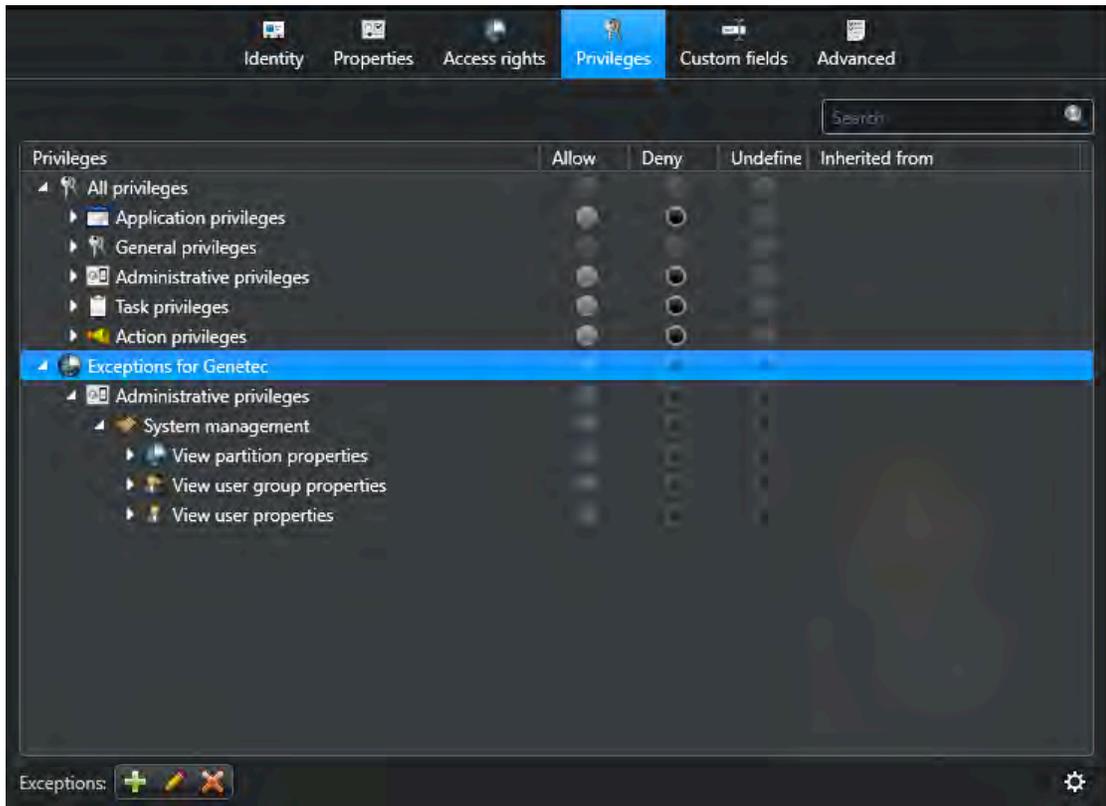
6   Click **Apply**.

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.
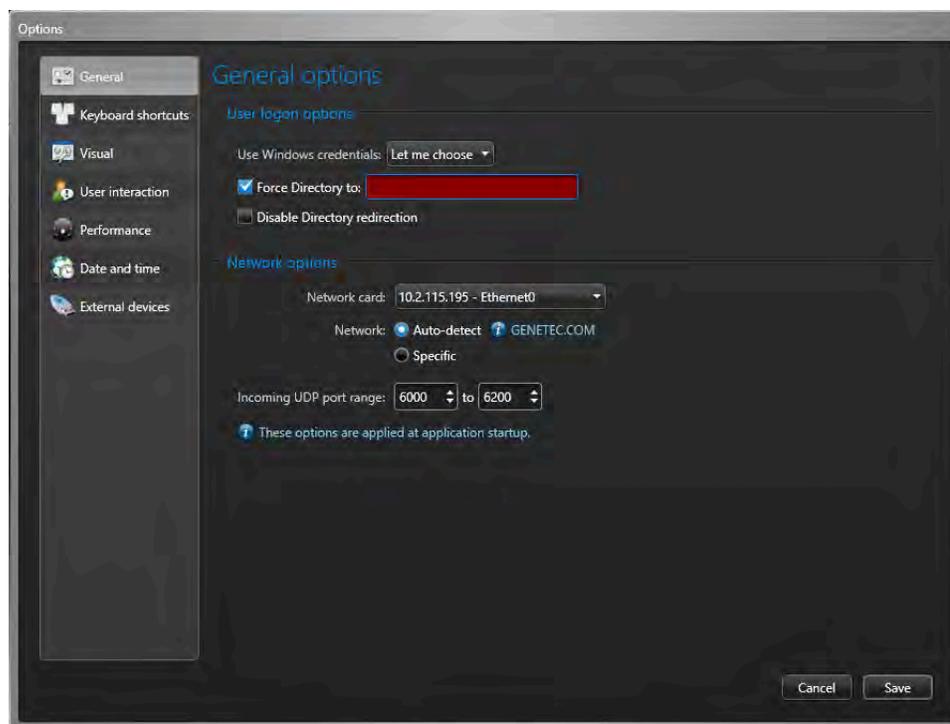
3   Click **Save**.

System

This section includes the following topics:

Using the recommended security settings in InstallShield (Basic, Advanced)

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.
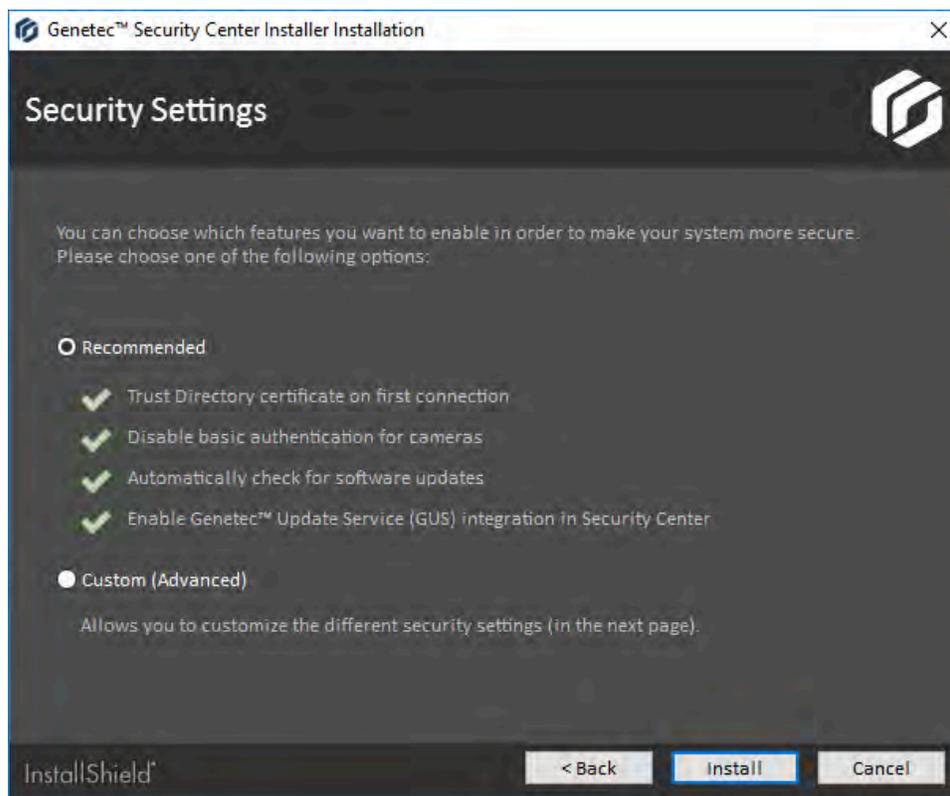
To use the recommended security settings in InstallShield:

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, Advanced)

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.

3 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.

4 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**.
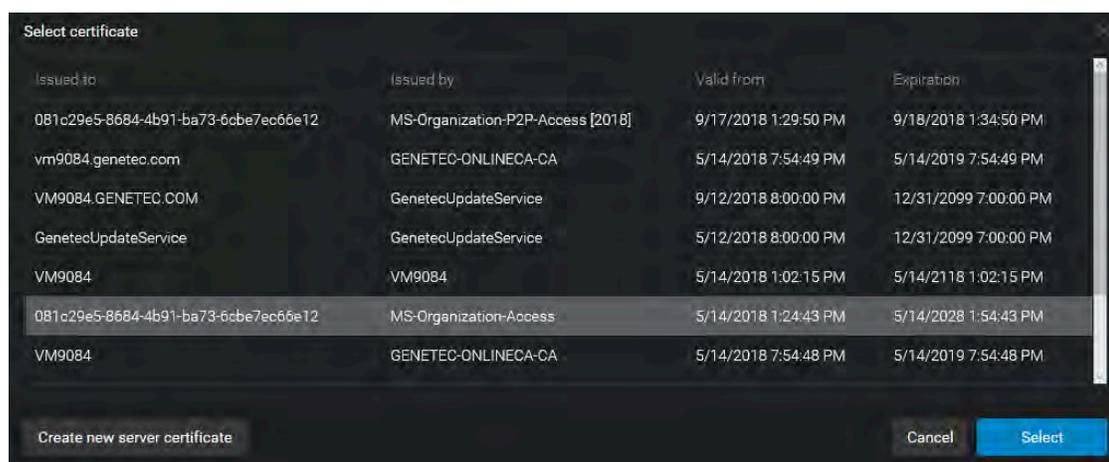
5   Click **Save**.

If you select a security certificate issued by a trusted certificate authority, a dialog box will inform you of the situation and provide you with can click one of three options:

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

Make sure that you are making the correct decision before you proceed.

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 now.

5   If users and user groups are already created in your system, grant access rights for the new partition to those who need it.

After you finish

For more information, refer to the *Partitions* chapter in the *Security Center Administrator Guide*.

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.
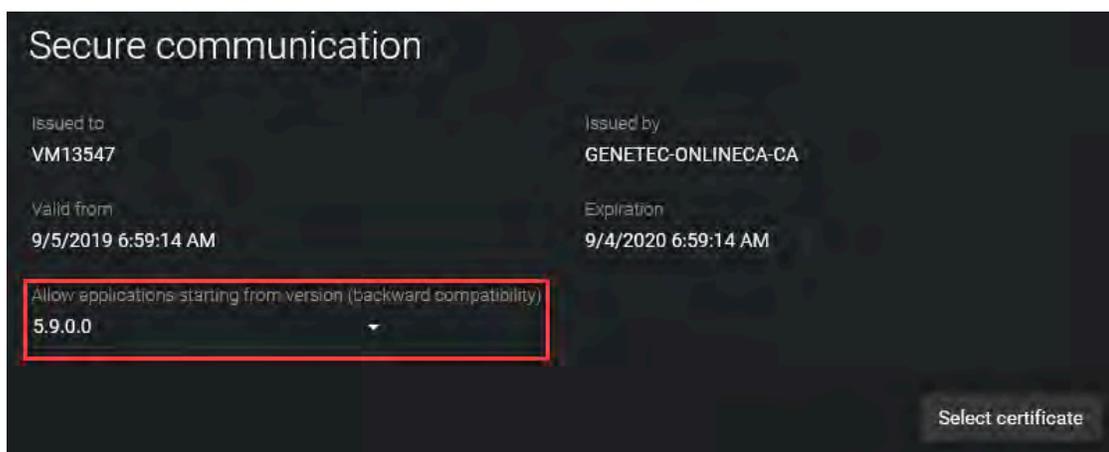
4 Click **Save**.

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 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**.
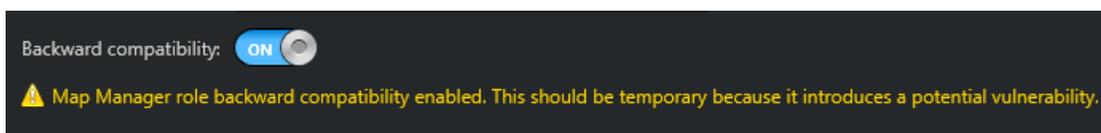
4 Click **Apply**.

Backward compatibility for the Map Manager role is disabled. Client applications that do not authenticate are unable to view 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**.
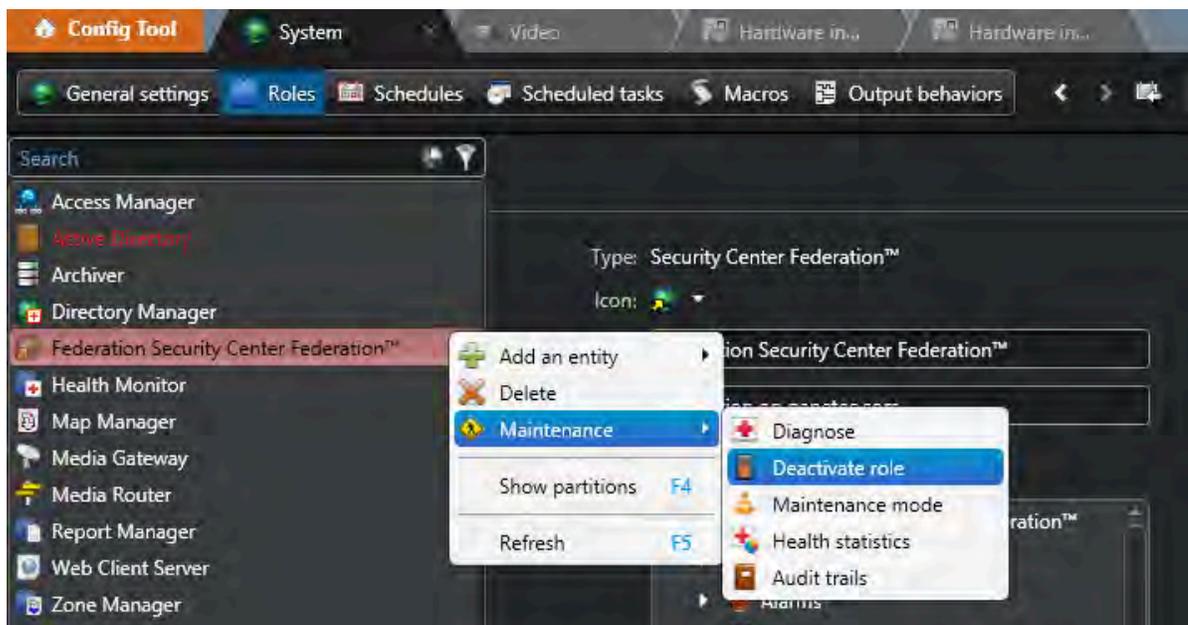
3 Click **Continue**.

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

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 servers of the same type. All Directory servers belong to one load balancing pool, and all Directory gateways belong to another. 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.
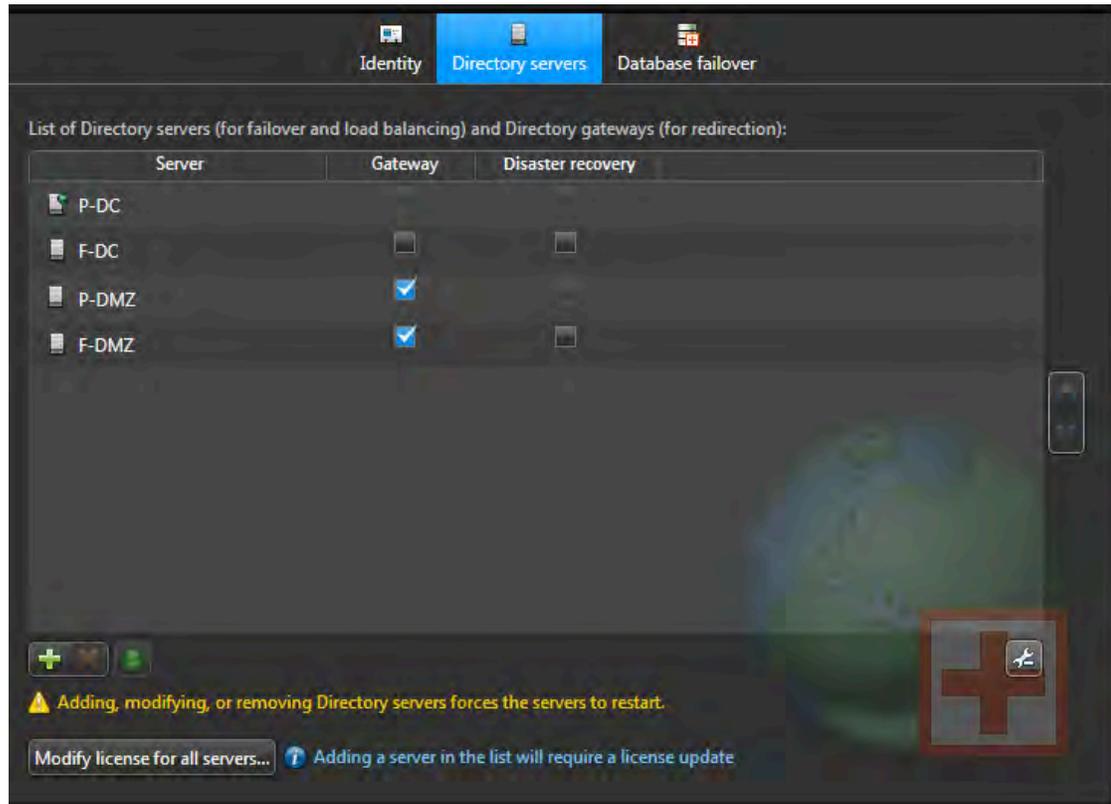
8   Update your license to include the servers that you have just promoted to Directory gateways.

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**.

4 Click **Save**.

4
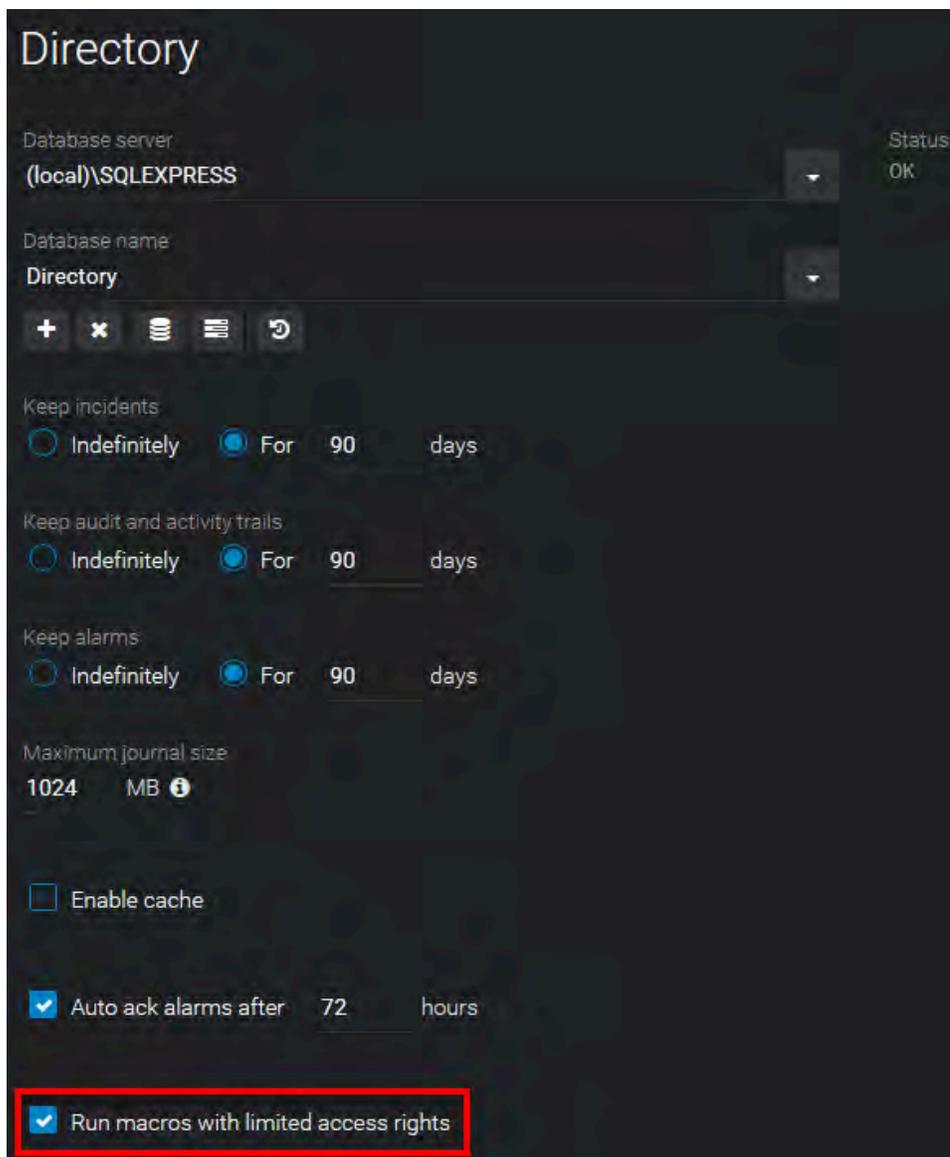
Genetec™ Update Service (GUS)

This section includes the following topics:

- "About keeping Security Center updated with Genetec Update Service (Basic, Advanced)" on page 36
- "Connecting to Genetec Update Service with Server Admin credentials (Basic, Advanced)" on page 37
- "Using a proxy server to connect Genetec Update Service to the internet (Basic, Advanced)" on page 38

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

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, Advanced)

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**.
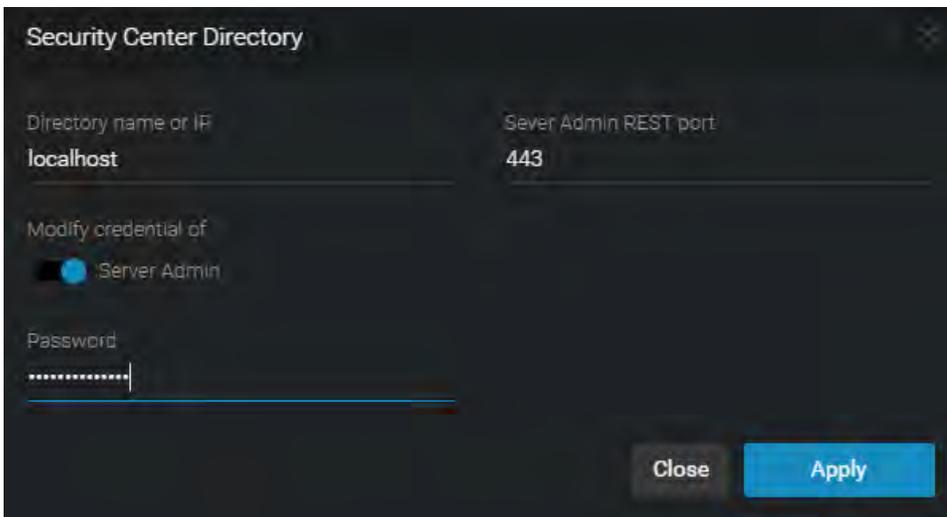
7 Click **Save configuration**.

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

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.
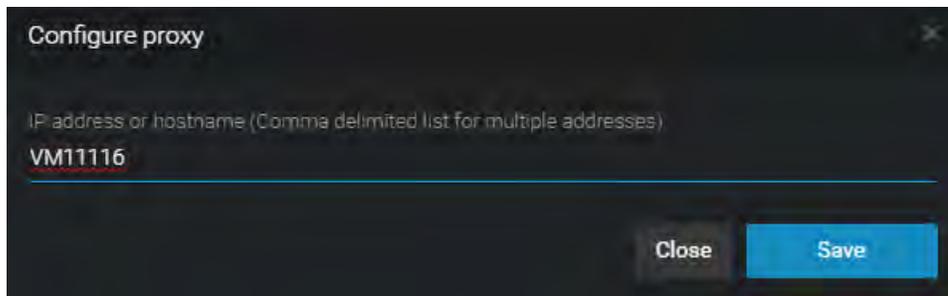
6   Click **Add**.

7   Click **Save configuration**.

Video

This section includes the following topics:

Refusing basic authentication (Basic, Advanced)

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 **Turn off basic authentication**.
4 Click **Install**.
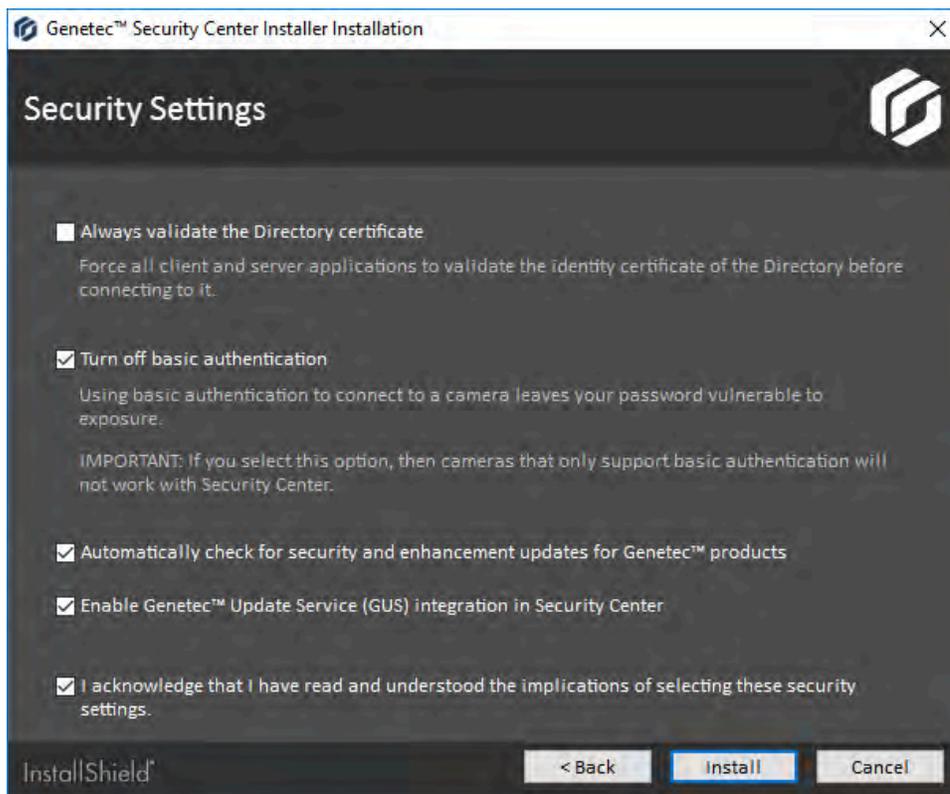
Enabling basic authentication (Basic, Advanced)

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, Advanced)

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**.
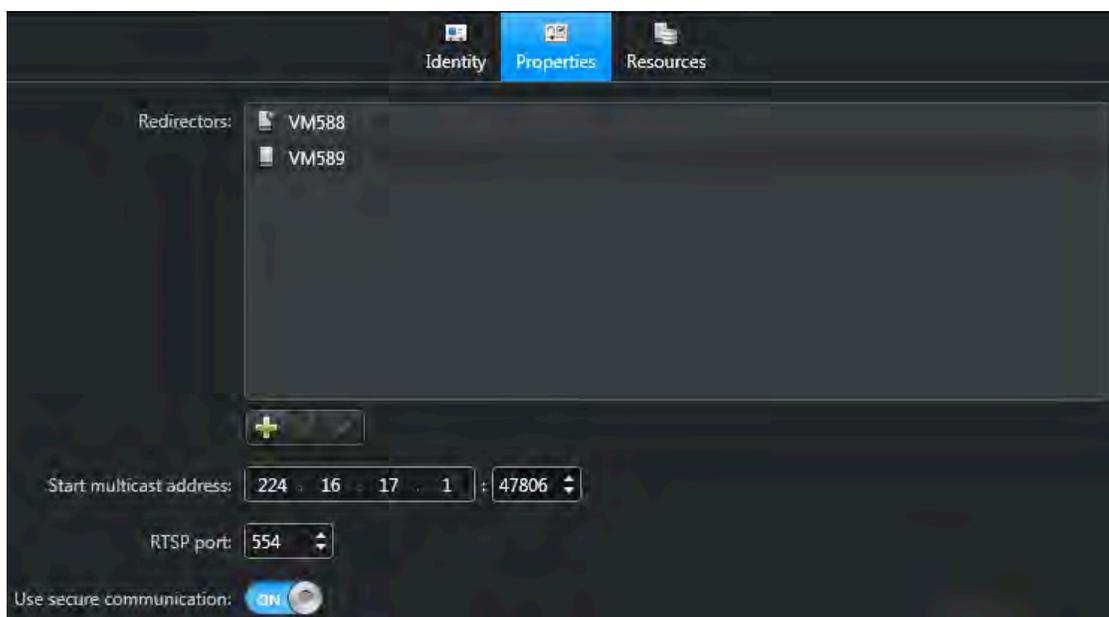
4   Click **Apply**.

Upgrading video unit firmware (Basic, Advanced)

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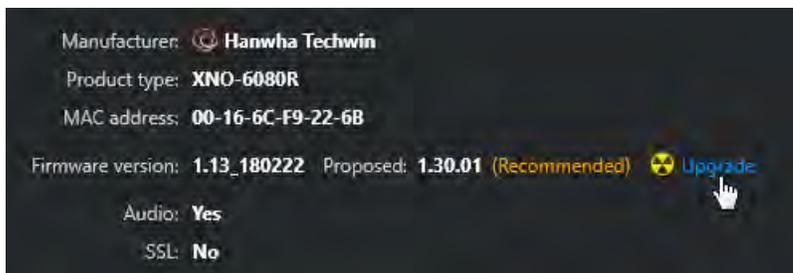
4   In the *Upgrade firmware* dialog box that opens, do one of the following:

- 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.
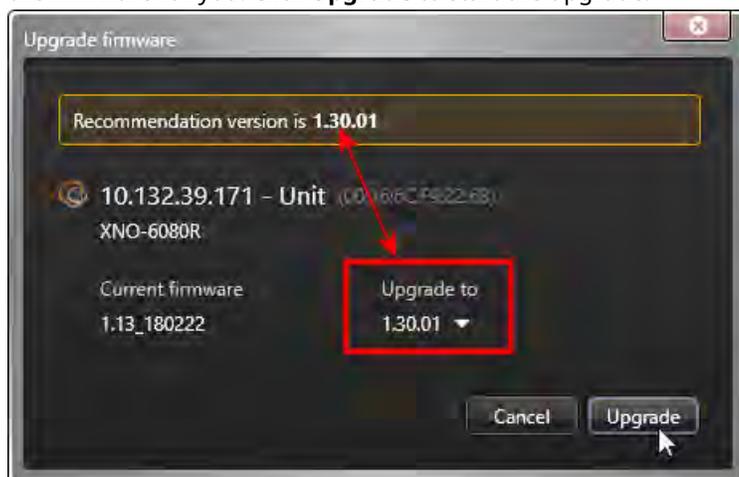
- If the **Select file** button is displayed instead, click that button and browse to the firmware file you downloaded yourself, and click **Open** > **Upgrade**.
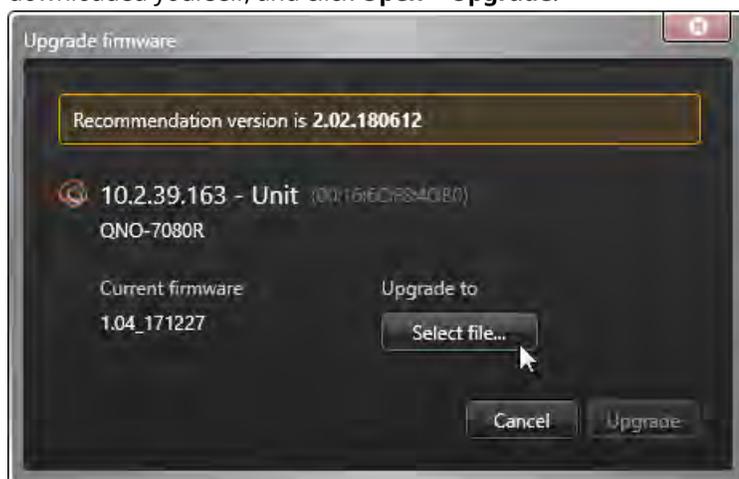
A message is displayed in the notification tray telling you that the firmware upgrade has started.

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, Advanced)

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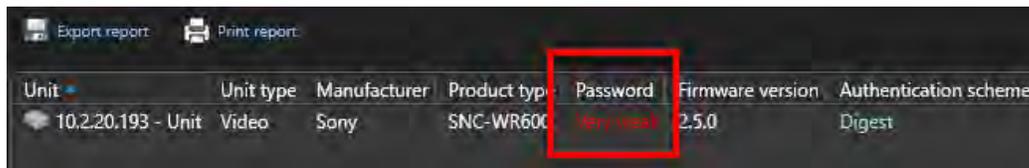
3 Change the password on each video unit that lacks a *Strong* password.

For instructions on how to change a camera's password, refer to the technical documentation provided by the manufacturer.

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: Axis, Bosch, Euklis, Extreme CCTV, Genetec™ Protocol, Intelbras, IONODES, ISD, March Networks, OTN Systems, SightLogix, Sony, and Verint.

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**.

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 stream (video, audio, and so on) both at rest and in transit.

What you should know

For a video stream, the Archiver role encrypts your video as soon as it receives it, and stores it in an encrypted file. The encrypted video data is sent over the network and can be decrypted only by the client.

To set up fusion stream encryption

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

After you finish

For more information, refer to the *Fusion stream encryption* chapter of the *Security Center Administrator Guide*.

Enabling fusion stream encryption (Advanced)

To protect the privacy of your data, you can enable fusion stream encryption either on the Archiver role or on individual cameras.

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 is required to be installed on the Archiver.

It is not necessary to install the certificates on the Archiver server. The encryption certificates are applied to the Archiver through Config Tool. For this reason, Config Tool must have access to the certificates, either from the certificate store of the local machine, or from 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.
2 Do one of the following:
   • To enable encryption on the Archiver, select the Archiver role to configure, and click the **Camera default settings** tab.
   • To enable encryption on a camera, select the camera to configure, click the **Recording** tab, and then click **Custom settings**.

3 Click **Show advanced settings** and set the **Encryption** slider to **ON**.
4 Under **Certificates**, click **Add an item** (➕).

   The *Select certificate* dialog box opens.

5 If the encryption certificates are installed on your local computer, select them from the **Installed certificates** list, and click **OK**.

6 If the encryption certificates are not installed on your local computer, find and install them:

a. Select **Browse certificate file**.

b. Click the browse icon (▦) and 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 files you want, look for Personal Information Exchange files instead.

c. Select the certificates you want, and click **Open**.

d. If the 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 Archiver starts encrypting all data streamed from the selected cameras. Only client workstations with one or more private key portions of certificates are able to view the data recorded from now on.

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.

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.

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:

About using Global Cardholder Synchronizer (Basic, Advanced)

Global Cardholder Synchronizer (GCS) is a role that synchronizes shared cardholders and other related entities between a local system (sharing guest) and a 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. To do this, configure the user as a partition administrator only for the shared partitions that the user will access from the sharing host system.

Enabling Secure mode on HID Units (Basic, Advanced)

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 Access Manager is encrypted.

Before you begin

The HID Admin password is required to enable Secure mode.

What you should know

It is considered a 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*.

To enable Secure Mode on HID units:

1 From the Config Tool home page, open the *Access Control* task and select the *Roles and units* view.
2 Select an access control unit from the entity browser and click the **Properties** tab.
3 In the *Connection settings* section, enter the **Admin password**.
4 In the *General settings* section, select **Secure mode**.
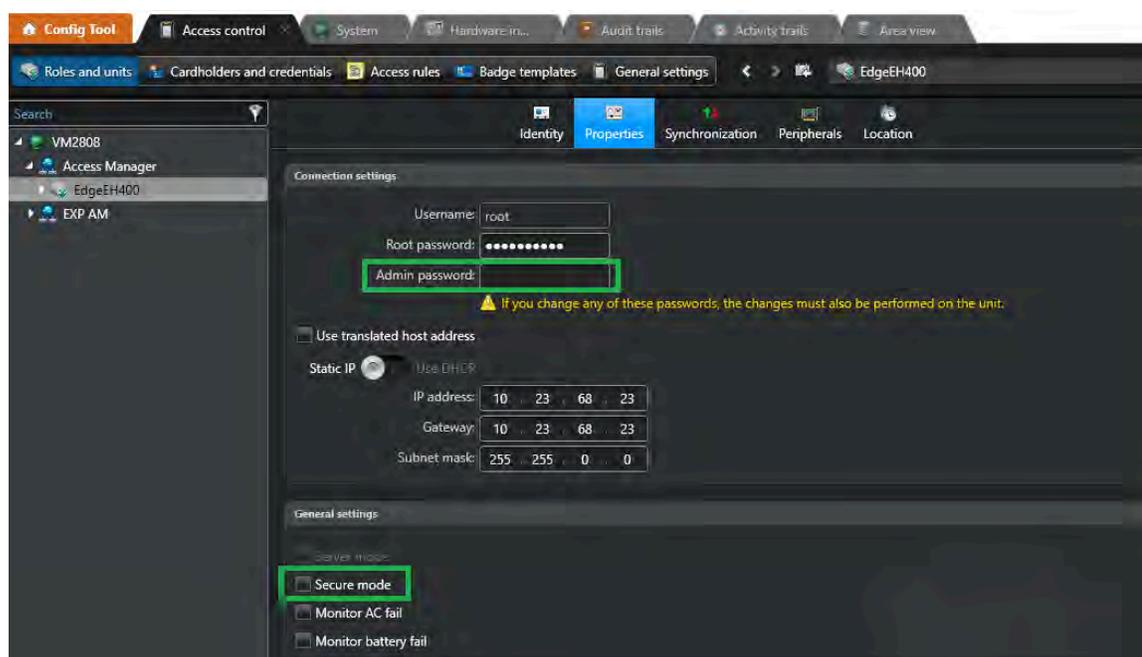
5 Click **Apply**.

Enabling Secure mode when enrolling HID Units (Basic, Advanced)

If secure mode is available on your HID units, you can enable it when enrolling them in Security Center.

What you should know

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

The HID Admin password is required to enable Secure mode.

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

To enable Secure Mode when enrolling an HID unit:

1   From the Config Tool home page, open the *Access Control* task.

2   Click 🟢 **Access Control Unit**.

3   In the *Network endpoint* section of the **Unit information** tab, enter the username and password of the Security Center administrator and select **Secure mode**.
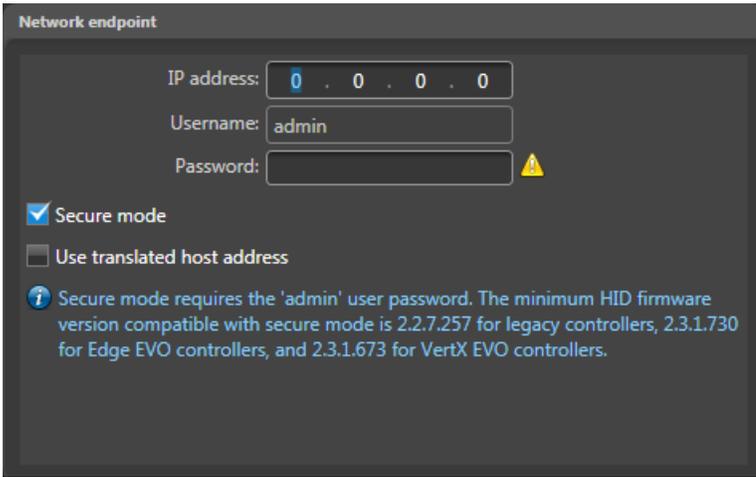
4   Click **Next**.

Analyzing the strength of administrator passwords on HID controllers (Basic, Advanced)

For security purposes, you must change the default passwords on your HID controllers with strong administrator passwords.

What you should know

A valid administrator password is between 6-10 characters in length, and can include all printable ASCII characters from 32-126 (decimal). See http://www.asciitable.com for more guidelines.

To analyze the password strength of your HID controllers:

1   From the Config Tool home page, open the *Hardware Inventory* task.

2   In the *Units* section, click on the drop-down and select **Access control unit**.

3   From the list, select your HID units.
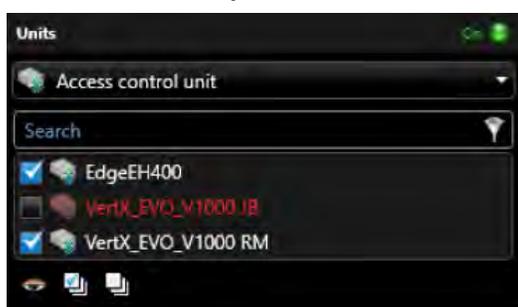
4   Click **Generate report**.

The report indicates the strength of each HID controller.

5   Change the password on each unit that doesn't have a Strong password.

For instructions on how to change the password of an HID controller, refer to the technical documentation provided by the manufacturer.

About updating the firmware on HID access units (Basic, Advanced)

To ensure you have the latest security fixes and improvements, keep the firmware of your HID access control unit up-to-date.

For more information, see HID EVO Unit Firmware Upgrade Procedure.

Updating firmware on Synergis™ appliances (Basic, Advanced)

To ensure that you have the latest security fixes and improvements, keep your Synergis™ appliance up-to-date with the latest Synergis™ Softwire firmware.

Before you begin

Download the latest version of the Synergis™ Softwire firmware from GTAP.

To check and upgrade the appliance firmware:

1 Log on to the Synergis™ unit.

2 Click **Maintenance** > **Softwire upgrade**.
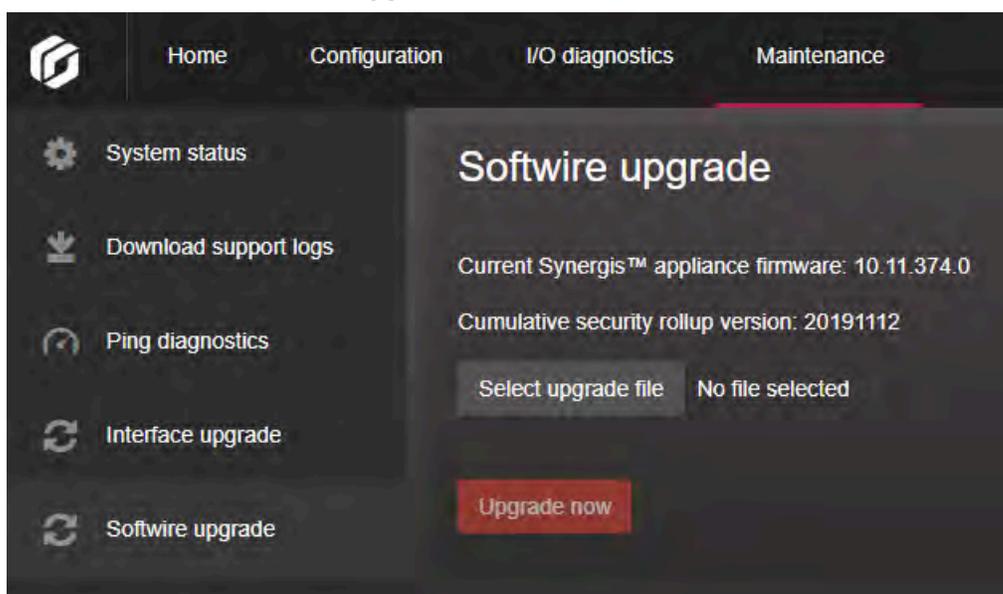
The current firmware version is indicated.

3 If an upgrade is necessary, click **Select upgrade file**.

4 In the file browser that opens, select the *.sfw* firmware file, and click **Open**.

The *.sfw* file must be located on your local drive.

5 Click **Upgrade now**.

Applying a cumulative security rollup for a Synergis™ appliance through Config Tool (Basic, Advanced)

Synergis™ Cloud Link supports security updates in the field. You can apply temporary fixes or patches to security vulnerabilities as they are discovered, either through Config Tool or through the Synergis™ Cloud Link portal.

Before you begin

Ensure that the firmware installed on the appliance is version 10.9 or later, and the appliance has at least 1.5 GB of available storage.

What you should know

It is recommended to perform the upgrade on a spare appliance and then replace the vulnerable unit in the field.

The upgrade takes about 30 minutes. During this time, you will experience a downtime between 5-15 minutes. It is recommended to schedule this update outside of core business hours.

To apply a cumulative security rollup for a Synergis™ appliance through Config Tool:

1 Log on to Config Tool.
2 Click the **Access Control** tab and select the roles and units view.
3 Select your Synergis™ unit from the entity browser and click the **Identity** tab.
4 Click **Upgrade** and select **Upgrade firmware**.
5 In the *New firmware* section of the *Upgrade firmware* dialog box, click the browse button ( ).
6 Select the firmware file: *SynergisSecurityrollupYYYYMMDD.sfw*.
   The .*sfw* file must be found on your local drive.
7 Click **Open** and then click**Upgrade** .
   Refer to the Hardware Inventory report to check for possible failure reasons.

Applying a cumulative security rollup on a Synergis™ appliance (Basic)

Using Synergis™ Cloud Link, you can apply temporary fixes or patches to security vulnerabilities as they are discovered.

Before you begin

Ensure that the firmware installed on the appliance is version 10.9 or later, and the appliance has at least 1.5 GB of available storage.

To apply a cumulative security rollup on a Synergis™ appliance:

1 Download the latest Synergis™ Cloud Link Cumulative Security Rollup from GTAP.
2 Log on to the Synergis™ unit.

3   Click **Maintenance** > **Softwire upgrade**.
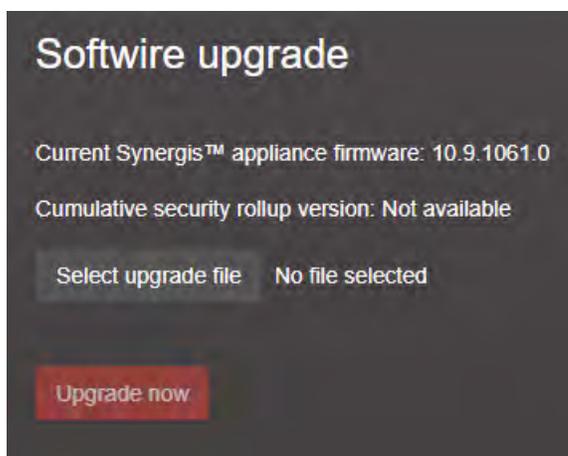
4   Click **Select upgrade file**, select the cumulative security rollup file, and click **Open**.

   NOTE: The *SynergisSecurityrollupYYYYMMDD.sfw* file must be on your local drive.

5   Click **Upgrade now**.
   The update is applied. It can take up to 20 minutes for the install to complete.

Changing the default administrator password for your Synergis™ appliance (Basic, Advanced)

Synergis™ appliances are shipped with a default administrator password. This should be changed when adding your Synergis™ appliance to Security Center, as it might be known to others.

What you should know

Replace the default administrator password with a password that is a long, unique, and random.

You can review the strength of your Synergis™ appliance password in the *Hardware inventory* task in Config Tool.

To change the default Admin password for your Synergis™ appliance

1　Log on to the Synergis™ unit.

2　Click on **Configuration** > **Users**.

3　From the *Users* page, select the **admin** user.

4　Enter the old password, then enter and confirm the new password and click **Save**.

The new password is applied immediately.

After you finish

If the unit was already connected to an Access Manager role, then change the logon password in the Config Tool to synchronize the Synergis™ unit with the Access Manager.

Synchronizing the Synergis™ unit with its Access Manager

Some settings on the Synergis™ unit are not automatically synchronized with the Access Manager. If you change any settings on the Synergis™ unit through the Synergis™ Appliance Portal, such as its logon password, its IP address, or the way it responds to connection requests, then you must also change the same settings on the Access Manager in Config Tool.

To synchronize the Access Manager with a Synergis™ unit:

1　Connect to Security Center with Config Tool.

2　Open the *Access control* task, and click the **Roles and units** view.

3　Select the Synergis™ unit you modified.

4　Click the **Properties** tab to update the necessary properties.
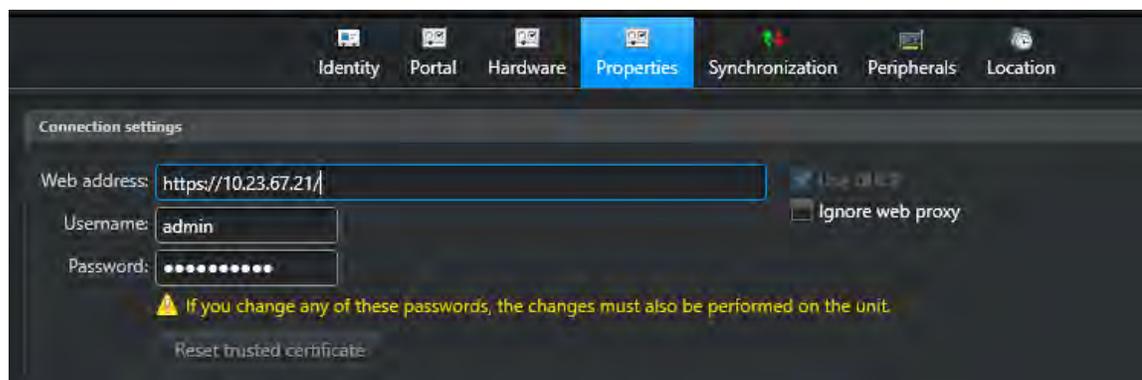
5   Under **Connection settings**, enter the parameters used to connect to this Synergis™ unit.

IMPORTANT: The following settings are all correctly initialized at the time the Synergis™ unit is enrolled in your system. Do not change these settings unless you changed the unit's settings with Synergis™ Appliance Portal after the unit has been enrolled, or one of our representatives instructs you to do so.

• **Web address:** Web address for contacting Synergis™ Appliance Portal.

• **Username and Password:** Logon username and password.

• **Use DHCP:** Do not change this parameter unless asked by a Genetec™ Technical Assistance representative. This parameter is reset every time the Access Manager reconnects to the Synergis™ unit.

• **Ignore web proxy:** Select this option to instruct the Access Manager to ignore the Proxy Server settings on the server currently hosting the role. Clear this option to instruct the Access Manager to follow the Proxy Server settings (default=cleared).

• **Reset trusted certificate:** (Only enabled when the unit is offline) Click this button to make the Access Manager forget the trusted certificate for this unit so that the new one can be accepted. Use this feature when you changed the digital certificate of the unit after it has been enrolled.

6   Click **Apply**.

Deactivating peer-to-peer and anti-passback for the Access Manager role (Basic, Advanced)

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

To deactivate peer-to-peer and global anti-passback:

1 From the Config Tool home page, open the *Access Control* task and click the Roles and units view.

2 In the *Synergis™ units only* section of the *Properties* page, clear **Activate peer to peer** and **Activate global antipassback**.
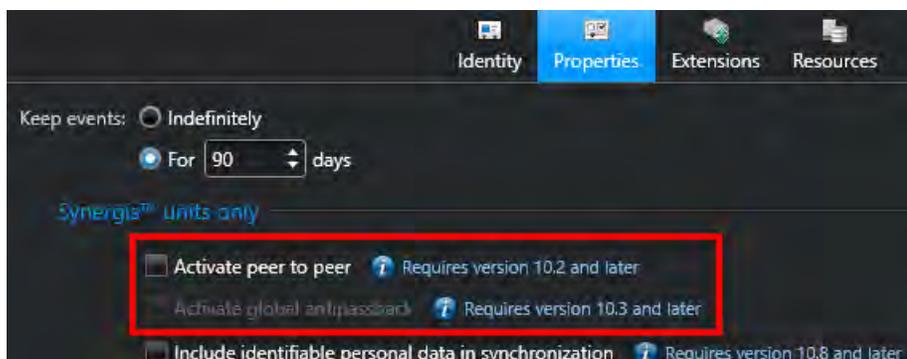
3 Click **Apply**.

Whitelisting your IP address (Basic, Advanced)

Using IP whitelisting, you can create lists of trusted IP addresses or IP ranges from which your users can access your domains.

To whitelist your IP address:

1   Log on to the Synergis™ Appliance Portal.

2   Click **Configuration** > **Network**.

3 In the *Access Manager settings*, verify that the IP address listed under **Accepted Access Manager connections** is the IP address of your Synergis™ unit.
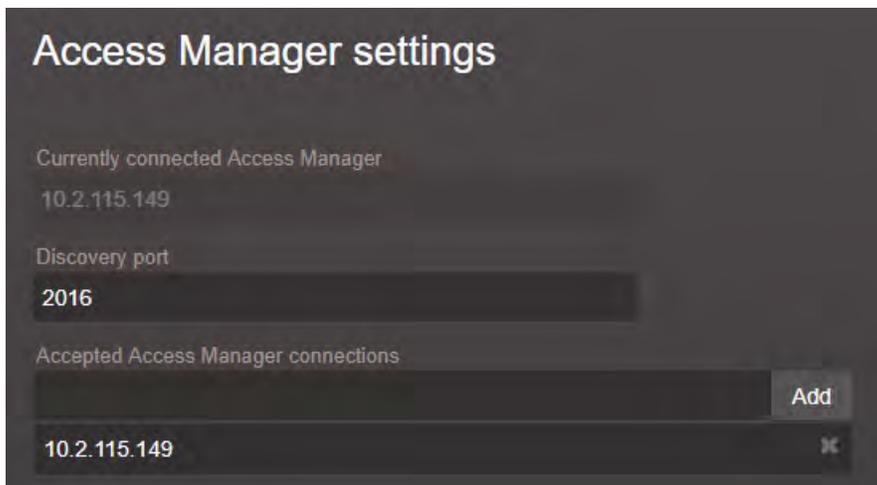
NOTE: This information can also be viewed on the *System Status* page in the Synergis™ Appliance Portal.
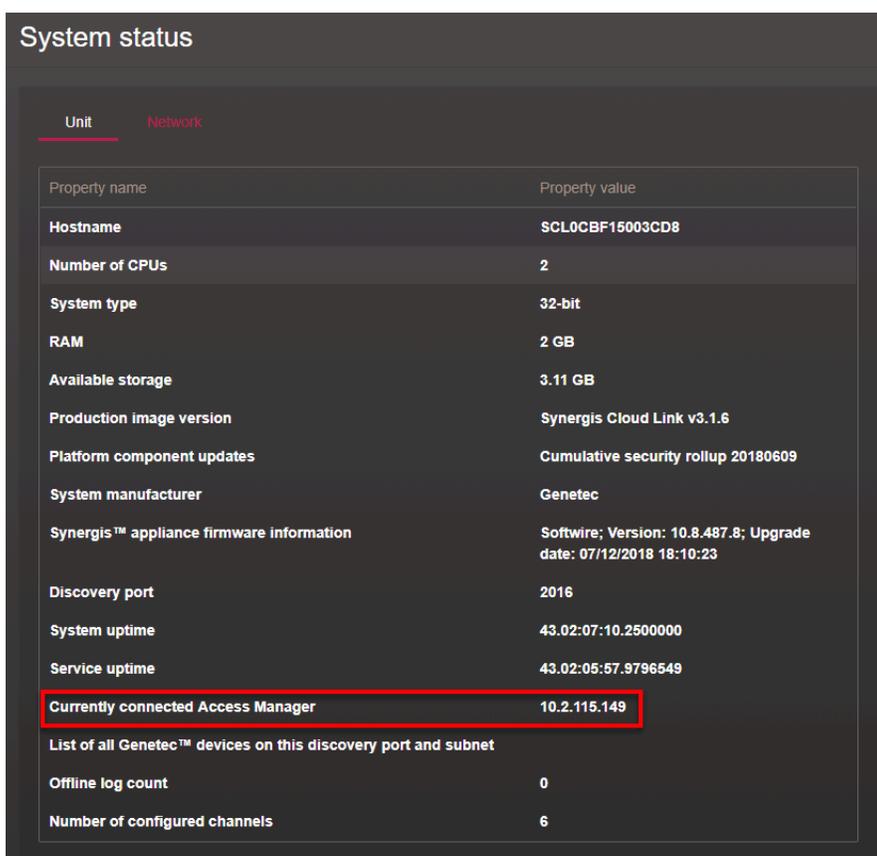
Using trusted certificates on Synergis™ appliances (Advanced)

By default, Synergis™ appliances come with a self-signed certificate. This means that the authenticity of the certificate will not be enforced as usual with the Public Key Infrastructure.

What you should know

It is possible to use a fully trusted certificate signed by a Certificate Authority on the Synergis™ Appliance.

To use trusted certificates on Synergis™ Appliances:

1   Log on to the Synergis™ unit.

2   On the *Configuration* page, click **Create certificate signing request**.

A *.req* file is generated, containing the public portion of the certificate and does not contain the private key. Therefore, it is not confidential.
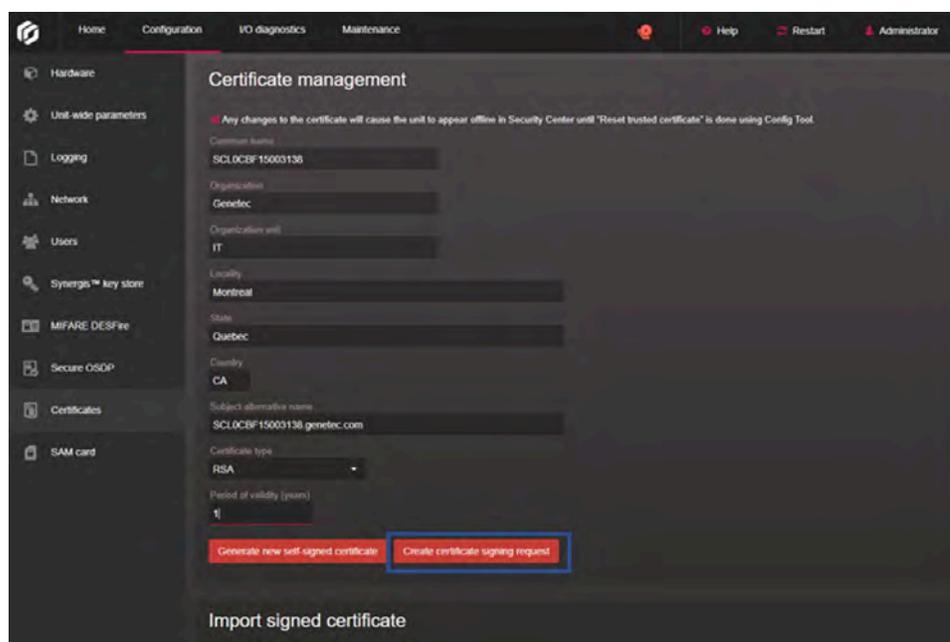
3   Send this *.req* file to a Certificate Authority to be signed.

After verification, the Certificate Authority will sign the public portion of the certificate with its own private key.

4 Install the signed certificate on the Synergis™ Appliance.
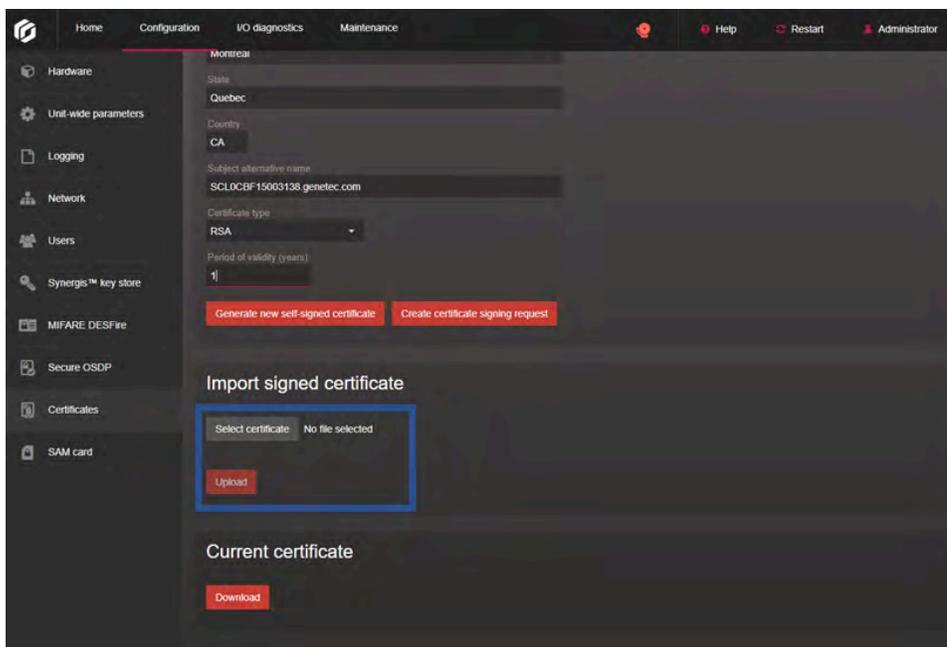
a) In the *Import signed certificate* section of the Synergis™ Synergis™ Appliance Portal**Select certificate**.
b) Select the *.req* file.
c) Click **Upload**.

NOTE: If the Synergis™ appliance was added into Security Center before the steps above were made, the Access Manager will not trust the new certificate or connect to the appliance. To bring the appliance back online, open Config Tool and click **Reset trusted certificate** in the *Properties* tab of the appliance while it is offline.
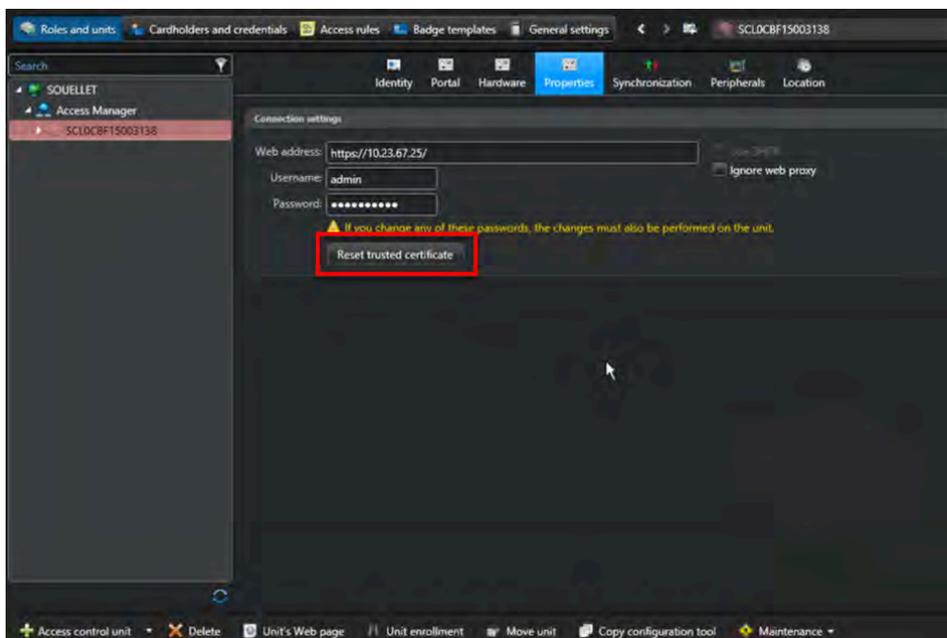
Logging

This section includes the following topics:

-

Logging Activity trails for security-related events (Basic, Advanced)

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, Advanced)" on page 69
- "Disabling unlimited session time in Security Center Web Server (Basic, Advanced)" on page 70
- "Installing a valid certificate on the Security Center Web Server (Advanced)" on page 71

Changing default Web Server ports (Basic, Advanced)

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**.
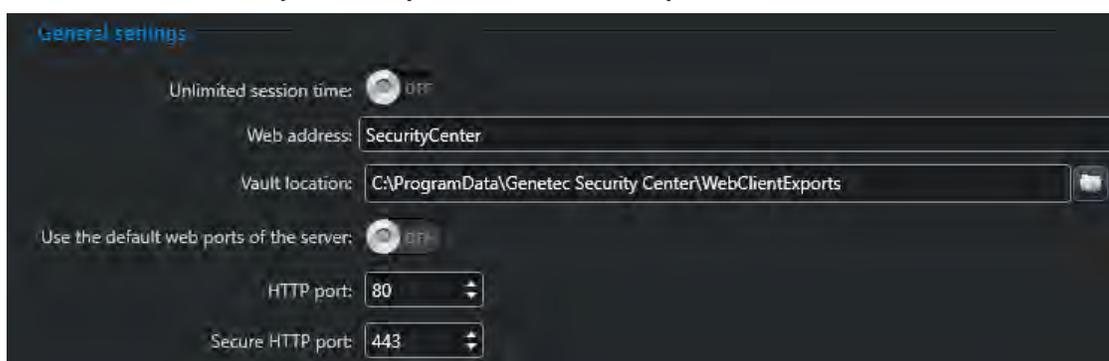
5 Click **Apply**.

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

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**.
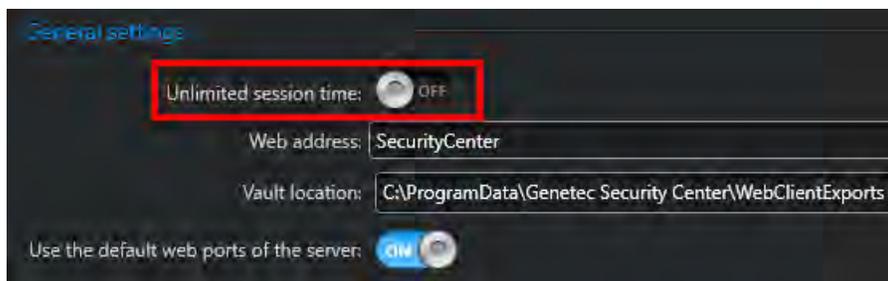
4   Click **Apply**.

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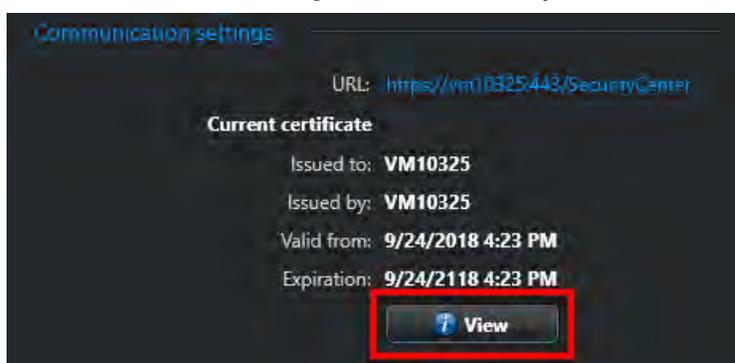
4   In the **General** tab of the *Certificate* window, click **Install Certificate** and follow the *Certificate Import Wizard*.

9

Genetec™ Mobile

This section includes the following topics:

- "Changing the default Mobile Server port (Basic, Advanced)" on page 73
- "Always use trusted connections by enforcing certificate validity (Advanced)" on page 74
- "Verifying the list of mobile devices connected to Security Center (Advanced)" on page 75

Changing the default Mobile Server port (Basic, Advanced)

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.
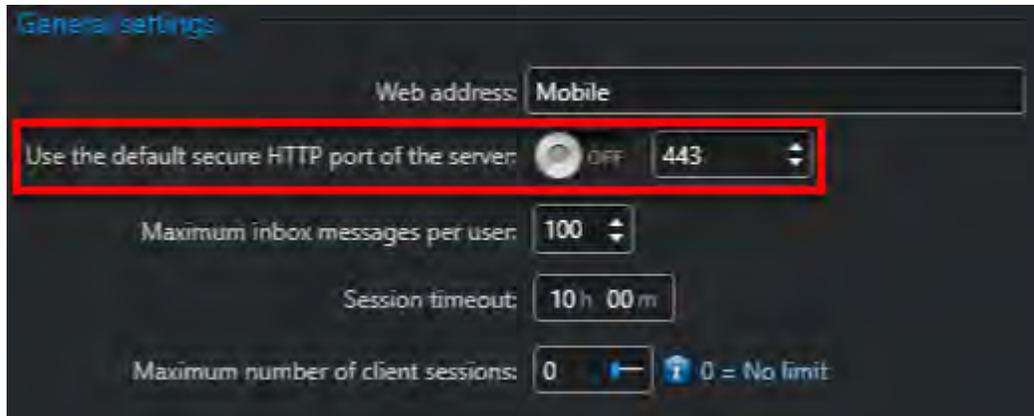
4 Click **Apply**.

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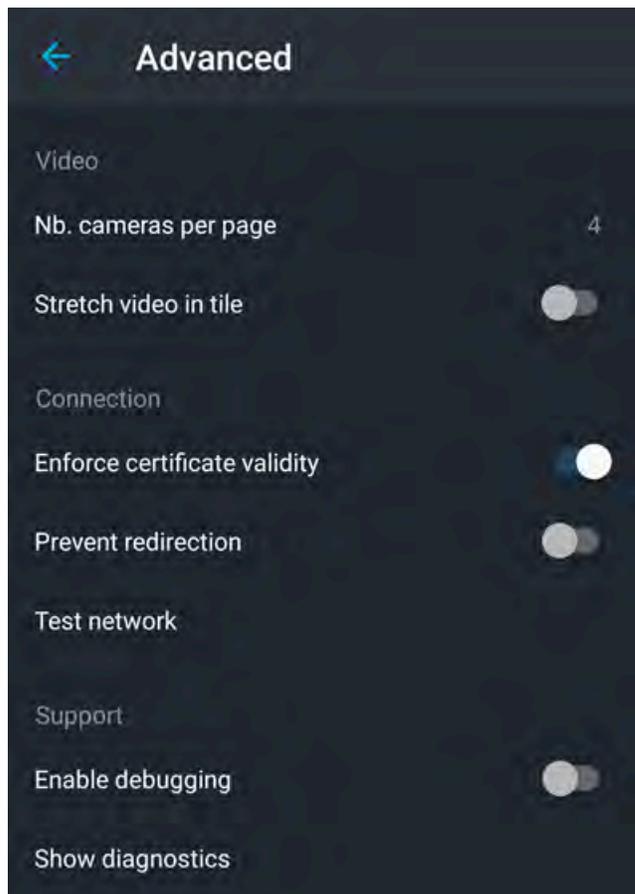
Verifying the list of mobile devices connected to Security Center (Advanced)

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**.

10
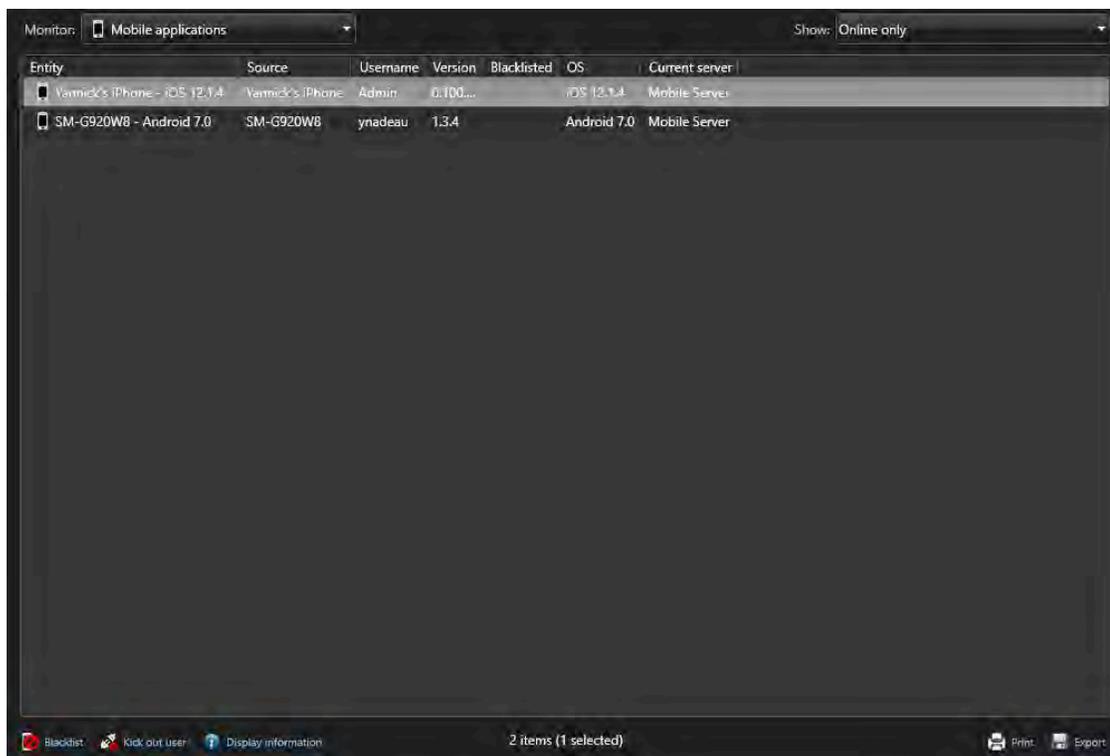
License Plate Recognition

This section includes the following topics:

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

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 had one.

• In the *Sharp Administrator 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 the Knowledge Base article KBA01405.

• 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 LPR 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 SharpV Portal using a self-signed certificate:

1 Log on to the SharpV Portal.
2 From the **Configuration** menu, select the **Security** page.
3 From the **Certificate** section, select **+ Self-signed**.
4 Enter the required information for the certificate and click **OK**.

  At a minimum, you must enter a two-letter **Country** code and you must define the **Validity (in years)**. The other fields are optional.

  NOTE: 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 SharpV IP address, not the SharpV name.

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

5 Select the **Active** check box for the certificate.

6   Click **Save and reboot** and click **OK** to confirm the reboot.

When you log in to the SharpV, the *HTTPS connection policy* on the *Security* page displays *Active*. A lock icon (🔒) in the browser's address bar indicates that you are now logged on to the SharpV with a secure connection.

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*.
2   Click **Download certificate** and save the certificate file as prompted by your browser.
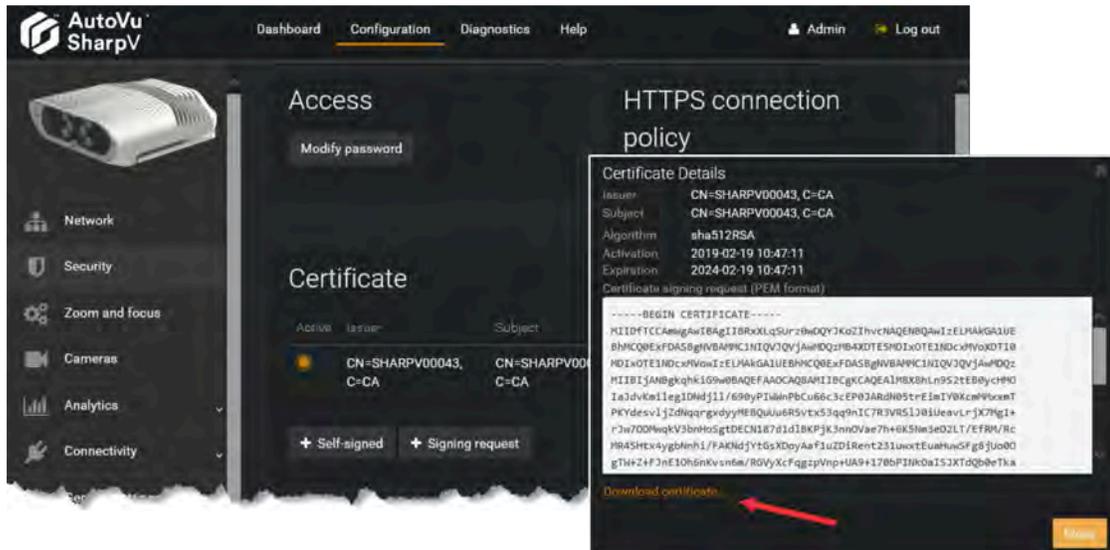
3   Double-click the *certificate.cer* file and click **Install Certificate**.
4   The *Certificate Import Wizard* prompts you to select a store location. Select **Local Machine** and click **Next**.
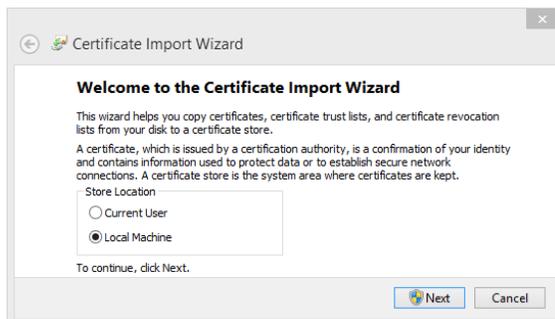
5   The wizard prompts you to select the certificate store you want to use. Select **Place all certificates in the following store** and click **Browse**.
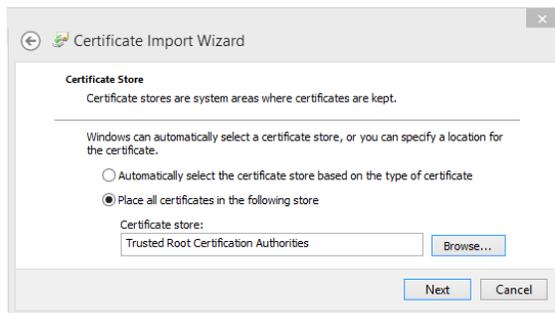
6   From the **Select Certificate Store** window, select **Trusted root certification Authorities** and click **OK**.
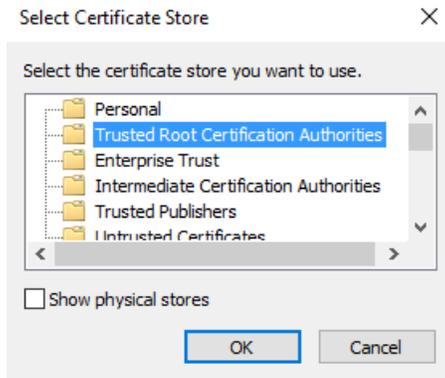
7   Click **Next** to continue, and click **Finish** to close the *Certificate Import Wizard*.

The system displays the message "The import was successful."

If you see a warning indicating that there is a problem with the website's security certificate, note that for the certificate to be properly registered, you must be logged on as an Administrator on the machine where you want to register the certificate.

8   Close all web browsers and open the Windows Task Manager to ensure that no browser processes are running in the background.

9   Log on to the SharpV 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 SharpV with a secure connection.

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

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 had one.

To encrypt the connection to the SharpV web portal using a signed certificate:

1   Log on to the SharpV Portal.
2   From the **Configuration** menu, select the **Security** page.
3   Click **+ Signing request**.
4   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 SharpV IP address, not the SharpV name.

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

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

6 Click **Copy to clipboard**.
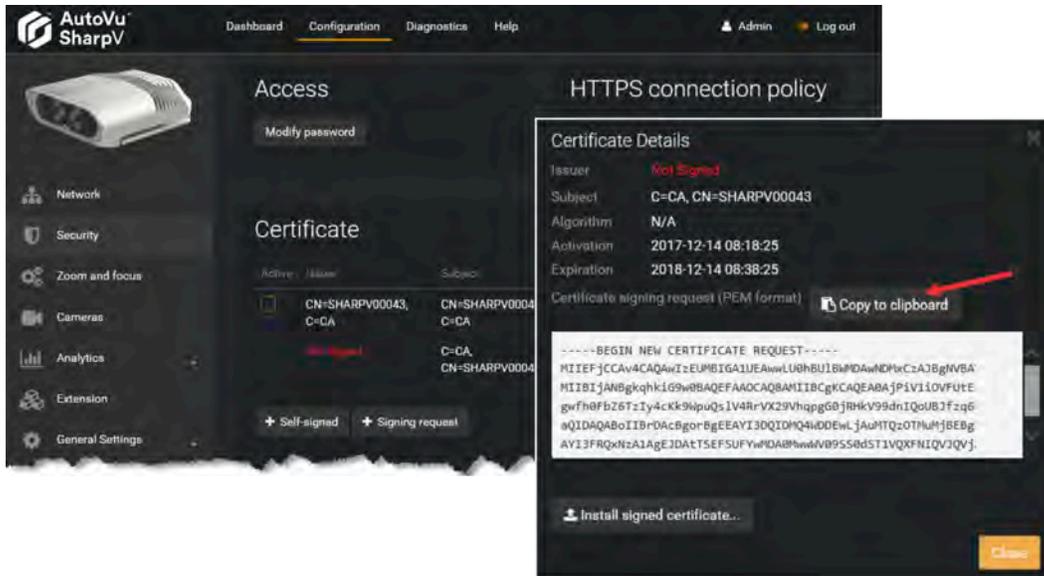
7 Send the certificate signing request to a certificate authority.

 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.

8 In the *Certificate Details* window, click **Install signed certificate** then browse to the certificate location and click **Open**.

9 Click **Save**.

 The system displays the message "Installed signed certificate... successful".

10 Refresh the browser (F5).

 The certificate is displayed in the *Certificate* list.

11 Select the Active check box for the certificate and click **Save and Reboot**.

12

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 SharpV with a secure connection.

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

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 LPR 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 LPR 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 > Extension* will be **Security Center (LMP 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 *LPR* task and select **Roles and units**.

2 Select the **LPR Manager** role from the drop-down list.

3 Expand the list of cameras under the LPR 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.
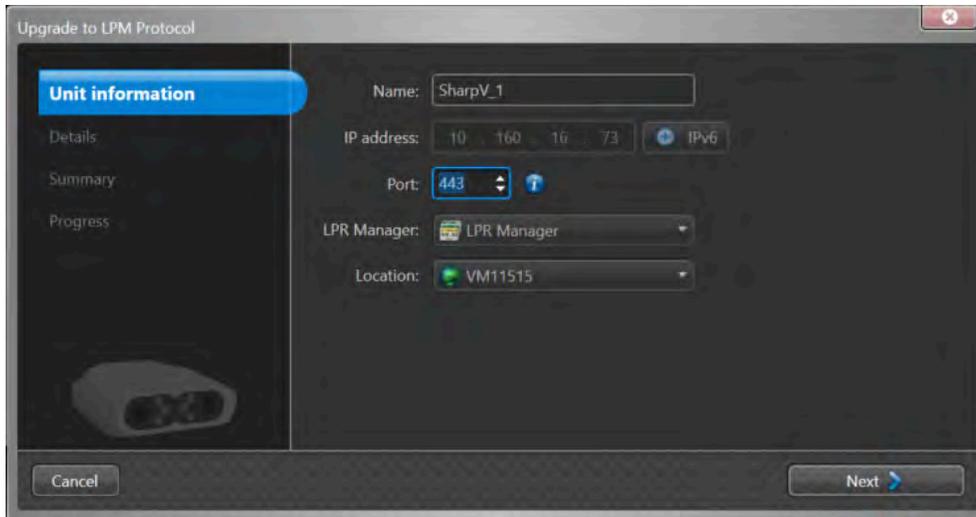
9　Click **Next**.

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 LPR Manager.
- The Sharp Portal shows that the camera is connected to Security Center.
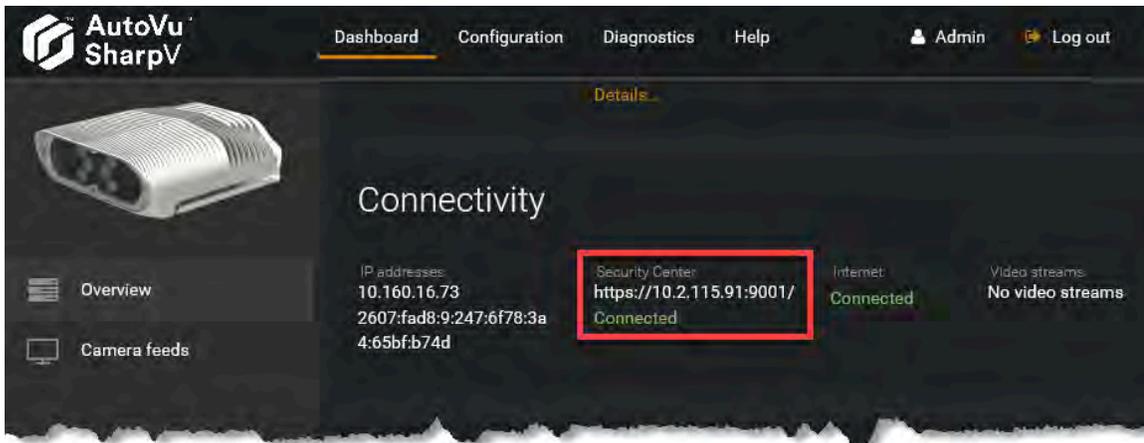
Changing the default password of a SharpX unit (Basic, Advanced)

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**.

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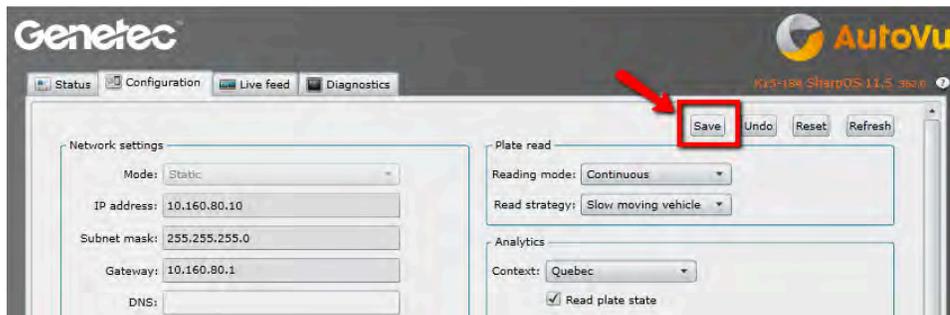
Encrypting the connection to the SharpX portal using a certificate from a certificate authority (Basic, Advanced)

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, Advanced)

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 level)

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 *LPR* task, and click **Roles and units**.

2   Select the LPR 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, Advanced)

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 *LPR* task and select **Roles and units**.

2   In the Channel security section of the *Properties* page, select **Encrypt communication channel** and click **Apply**.
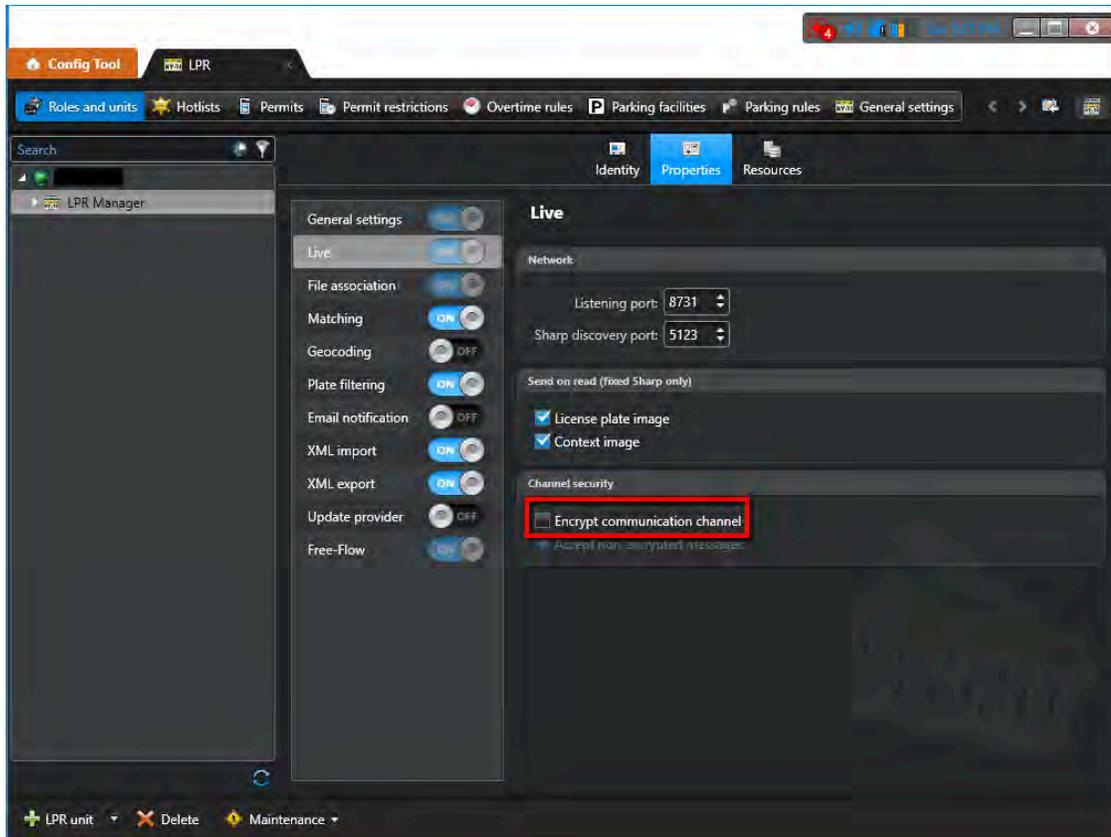
3   From the Genetec Patroller™ Config Tool home page, open the *Security Center* page.

4 Turn on **Encrypt communication channel** and click **Apply**.
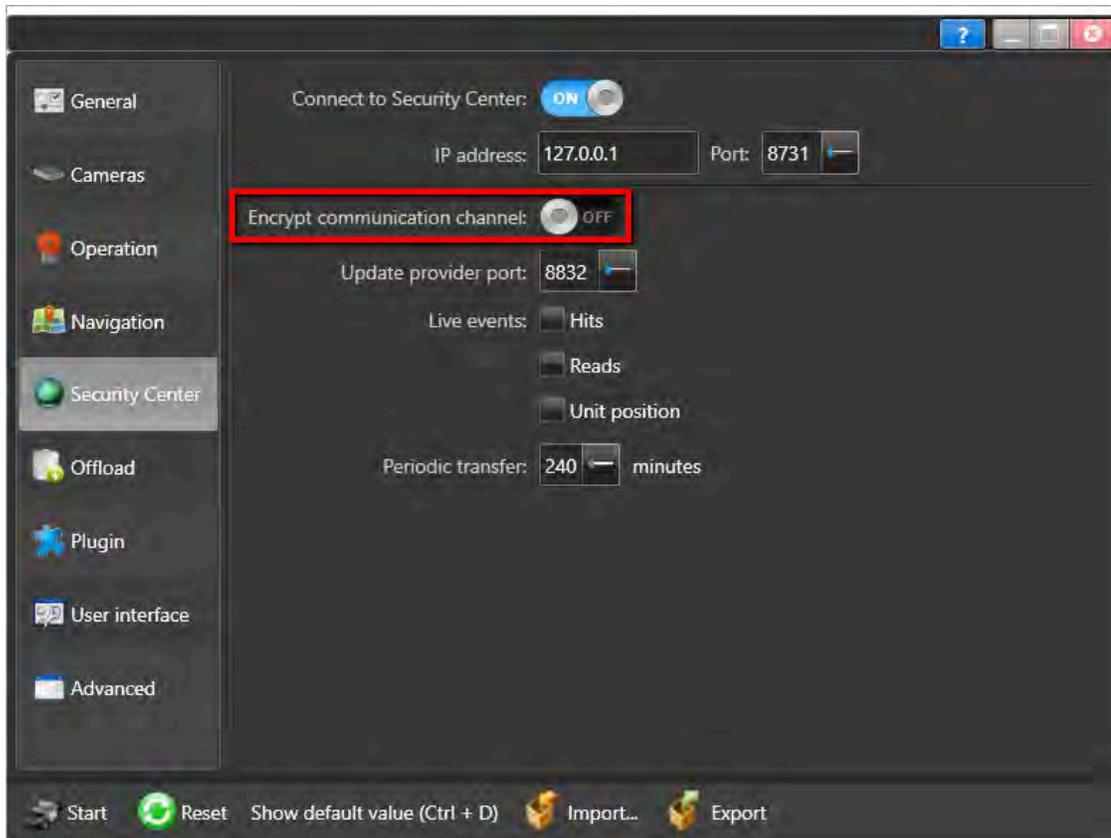
Encrypting the Genetec Patroller™ database (Advanced level)

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, Advanced)

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, Advanced)

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**.
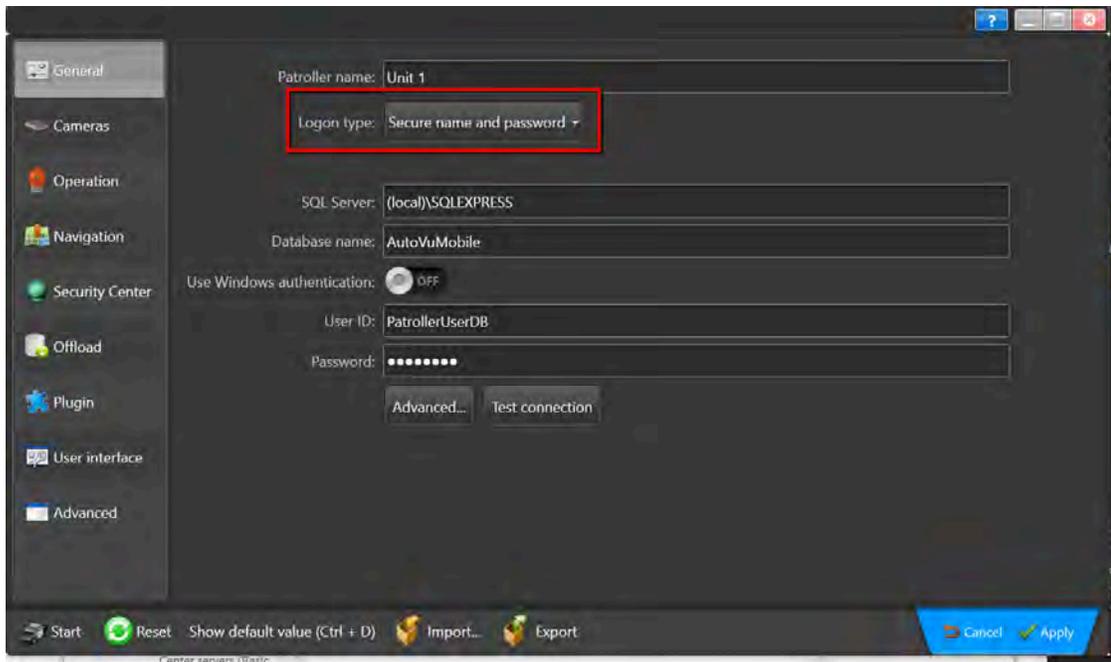
3 Click **Apply**.

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

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**.

11

Database

This section includes the following topics:

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

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. Therefore, it is possible to restrict the permission set before and after the first execution. 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	Process admin
Access 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
LPR Manager	X	X[1]	X
Media Router	X	X[1]	X
Zone Manager	X	X[1]	X
Intrusion Manager	X	X[1]	X
Plugin: KiwiVision Manager	X	X[1]	X
Mobile Server	X	X[1]	X

[1] dbCreator is only necessary for the first Security Center execution; it should be removed after.

[2] dbCreator is necessary when using Directory database failover through backup and restore. If failover through backup and restore is not used, dbCreator is only necessary for the first Security Center execution and should be removed after.

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
Archiver	X	X	X	X	
Auxiliary Archiver	X	X	X	X	
Directory	X	X	X	X	X
Health Monitor	X	X	X	X	X
LPR Manager	X	X	X	X	X
Media Router	X	X	X	X	
Zone Manager	X	X	X	X	X
Intrusion Manager	X	X	X	X	
Plugin: KiwiVision Manager	X	X	X	X	X
Mobile server	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, Advanced)

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.
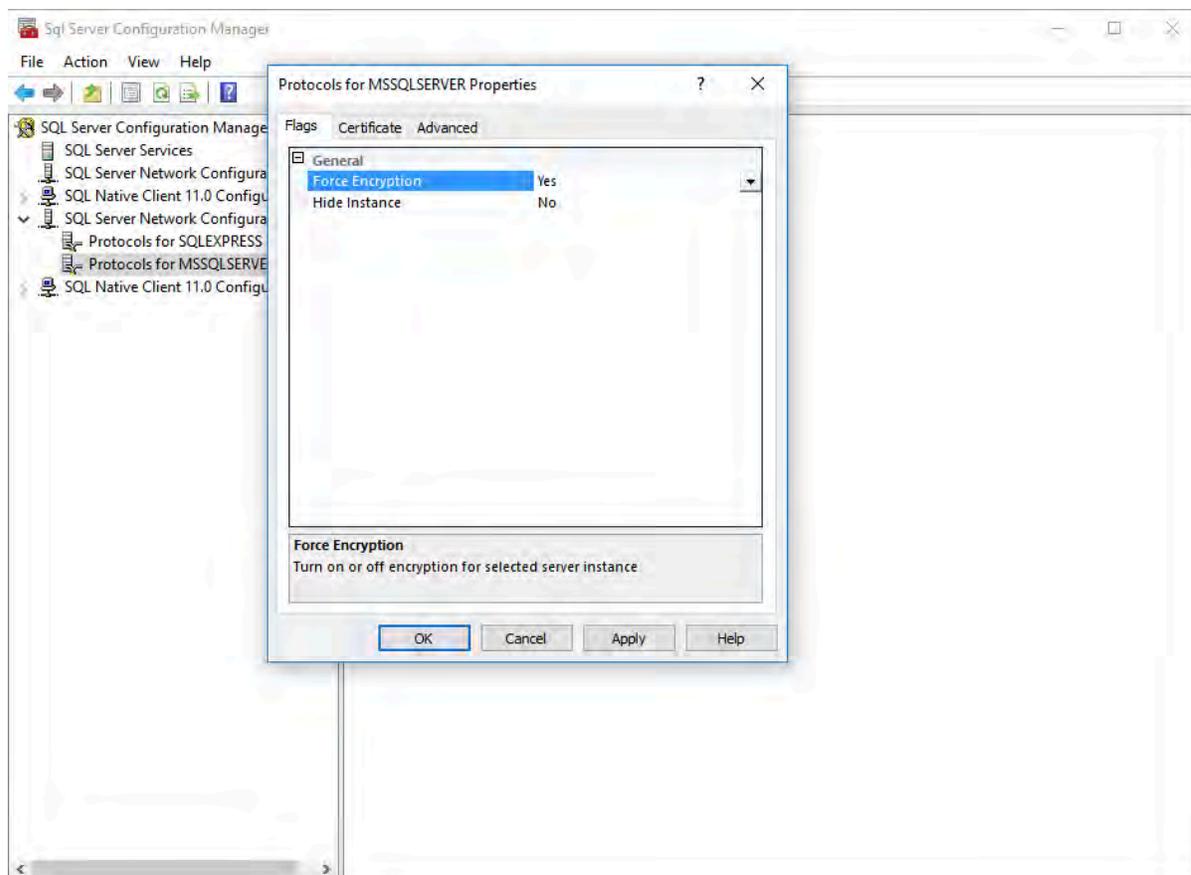
About the encryption of database files (Advanced)

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**.
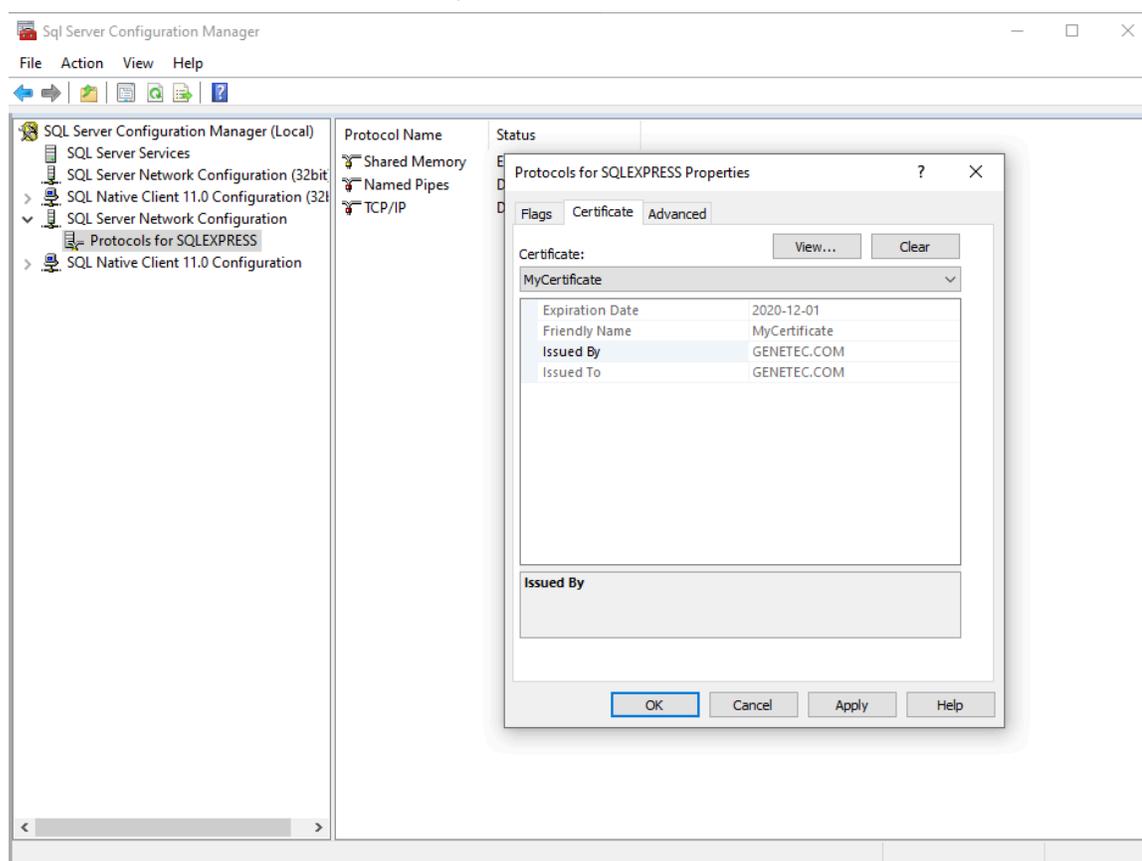
3   Under **Protocols for <SQL_instance>**, right-click **TCP/IP**, and select **Properties**.

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>*
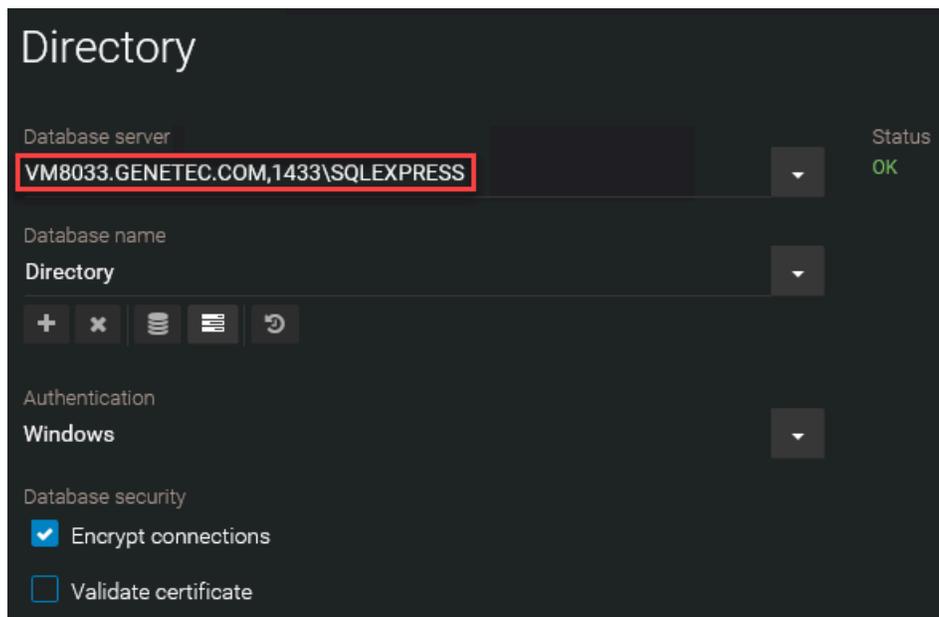
   c) Select **Validate certificate**.

   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>*
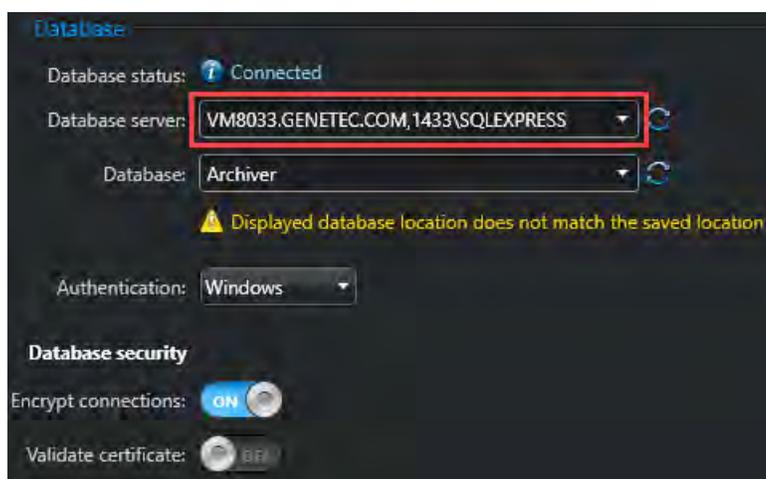
   c) Set **Validate certificate** to **ON**.

   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 level)

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]
```

12

Windows

This section includes the following topics:

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 enforces 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, Advanced)

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 configuring Windows securely (Basic, Advanced)

Microsoft provides ready-to-deploy security policies tailored to each of their operating system versions through the Security Compliance Manager (SCM).

More information about SCM can be found on the following page:

- Security Compliance Manager (SCM)

Microsoft also provides recommendations through their security baseline. For more information, refer to the Microsoft documentation and recommendations:

- Windows Server 2012 R2 Security Baseline
- Windows 8.1 Security Baseline
- Windows 10 Security Baseline
- SQL Server 2012 Security Baseline

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

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   Activity trails is a type of 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.

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 *broadcasts* 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.

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.

digital certificate   A digital certificate, also known as an *identity certificate* or *encryption certificate*, is an electronic "passport" that allows a person, computer, or organization to exchange information securely over the Internet using the public key infrastructure (PKI).

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, LPR 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 *digital certificate* or *public key certificate*, is an electronic document that contains a public and private key pair used in Security Center for *fusion stream encryption*. Information encrypted with the *public key* can only be decrypted with the matching *private key*.
Federation™	The Federation™ feature joins multiple, independent Genetec™ IP security systems into a single virtual system. With this feature, Security Center users can view and control entities that belong to remote systems, directly from their local Security Center system.
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).
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 LPR Manager role.
license plate recognition	License plate recognition (LPR) is an image processing technology used to read license plate numbers. LPR converts license plate numbers cropped from camera images into a database searchable format.
load balancing	Load balancing is the distribution of workload across multiple computers.

macro	A macro is a type of 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 to all client applications that require maps.
Media Router	The Media Router is the central role that handles all stream requests (audio and video) in Security Center. It establishes streaming sessions between the stream source (camera or 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.
Mobile Server	The Mobile Server role provides Security Center access on mobile devices.
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 LPR camera (1024 x 946 @ 30 fps), and a color context camera (640 x 480 @ 30 fps). The LPR data captured by the SharpX camera unit is processed by a separate hardware component called the AutoVu™ LPR 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. Supporting an ever-growing portfolio of third-party door control hardware and electronic locks, it allows you to 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).

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 explain 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://gtap.genetec.com.
- 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://gtap.genetec.com to address any issue regarding Genetec™ appliances or any hardware purchased through Genetec Inc.