Unified Security Platform

Security Center 5.6
Hardening Guide
Version: 1.2

Innovative **Solutions**

Genetec

Document Title: Hardening Guide
Date: April 13, 2017

Table of Contents

1 New in the Security Center 5.6 Hardening Guide

- New chapter on the completely redesigned Web Client
- New information on the Mobile Server.
- New chapter on Access Control.
- New chapter on Windows, introducing the Microsoft Security Compliance Manager.
- New information on using Directory authentication.
- New information on creating passwords.
- Updated screenshots.

2 Abstract

This document contains information to help harden your Genetec™ Security Center system. It addresses the general configuration of the system as well as the configuration related to video units. Most of the actions suggested here are already covered by the *Security Center Administrator Guide*. Consult the guide for more details.

3 Hardening Level

We define two levels of security in this guide: Basic level and Advanced level.

3.1 Basic level

This level provides the user with basic security measures for all systems that require only minimal security.

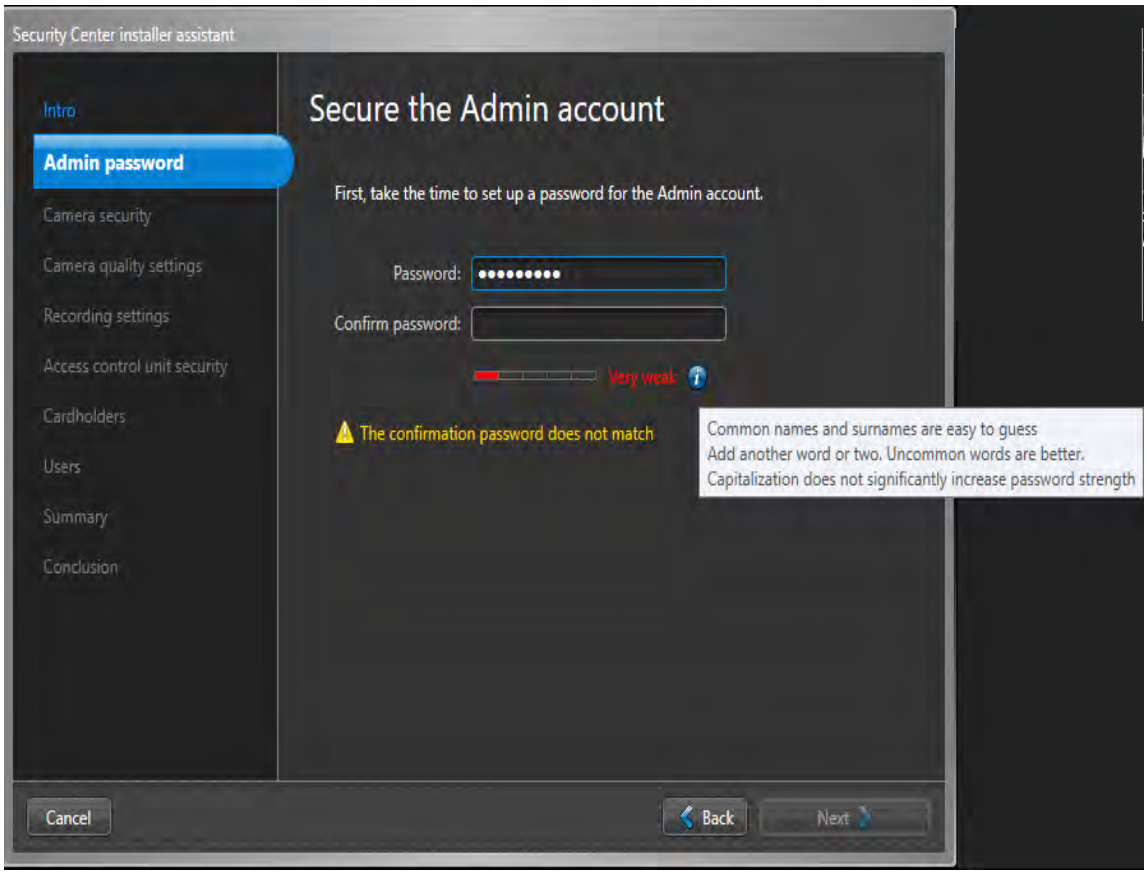
3.2 Advanced level

This level provides the user with higher security than the basic level, but requires a greater effort from the user to be put in place. Organizations with strict security policies should adhere to this level.

4 User Management

4.1 Change the default Admin password (Basic level, Advanced level)

It is strongly recommended to change the default Admin password to a long, unique, random string. Starting in Security Center 5.6, an advanced password strength meter with contextual help has been added to help you choose a strong password. This password strength meter recognizes weak passwords and gives contextual advice on how to improve your password. Examples of weak passwords include common names, dates, common passwords, repeat sequences, and keyboard patterns. We recommend that you only use passwords that are considered **Very strong** by the password strength meter.



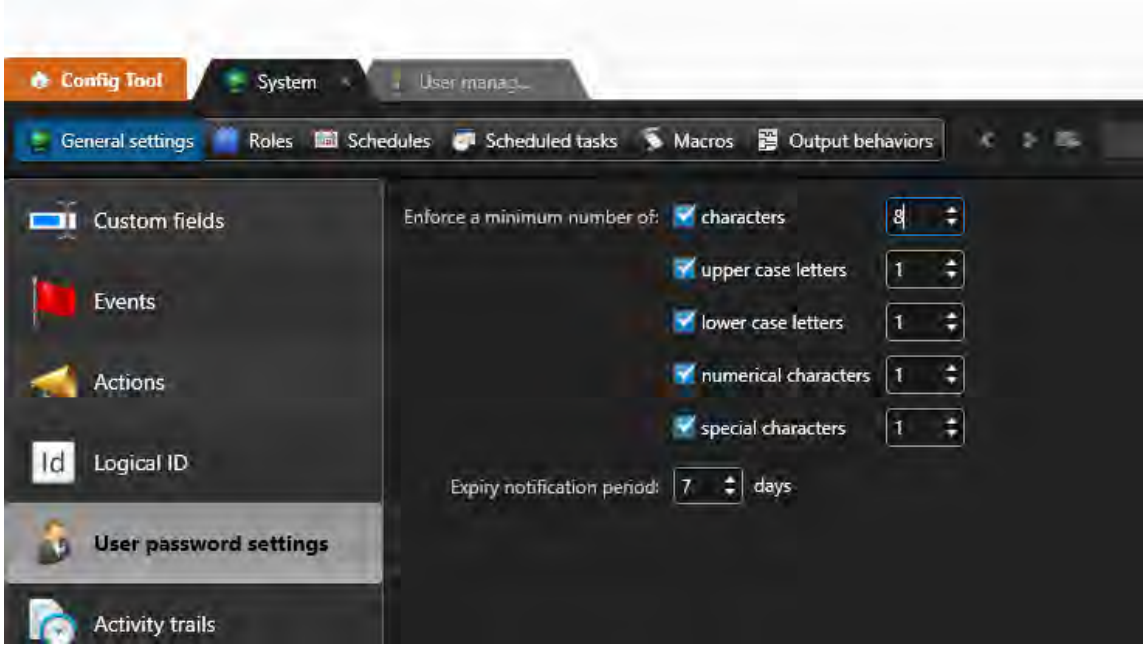
Admin account password configuration with password “Adam1234” in the Installer Assistant

4.2 Enforce a strong user password policy (Basic level, Advanced level)

Enforce a strong user password policy for every user account created in Security Center. A strong password policy should require a minimum length, complexity, and expiration period for each password.

To edit your password settings:

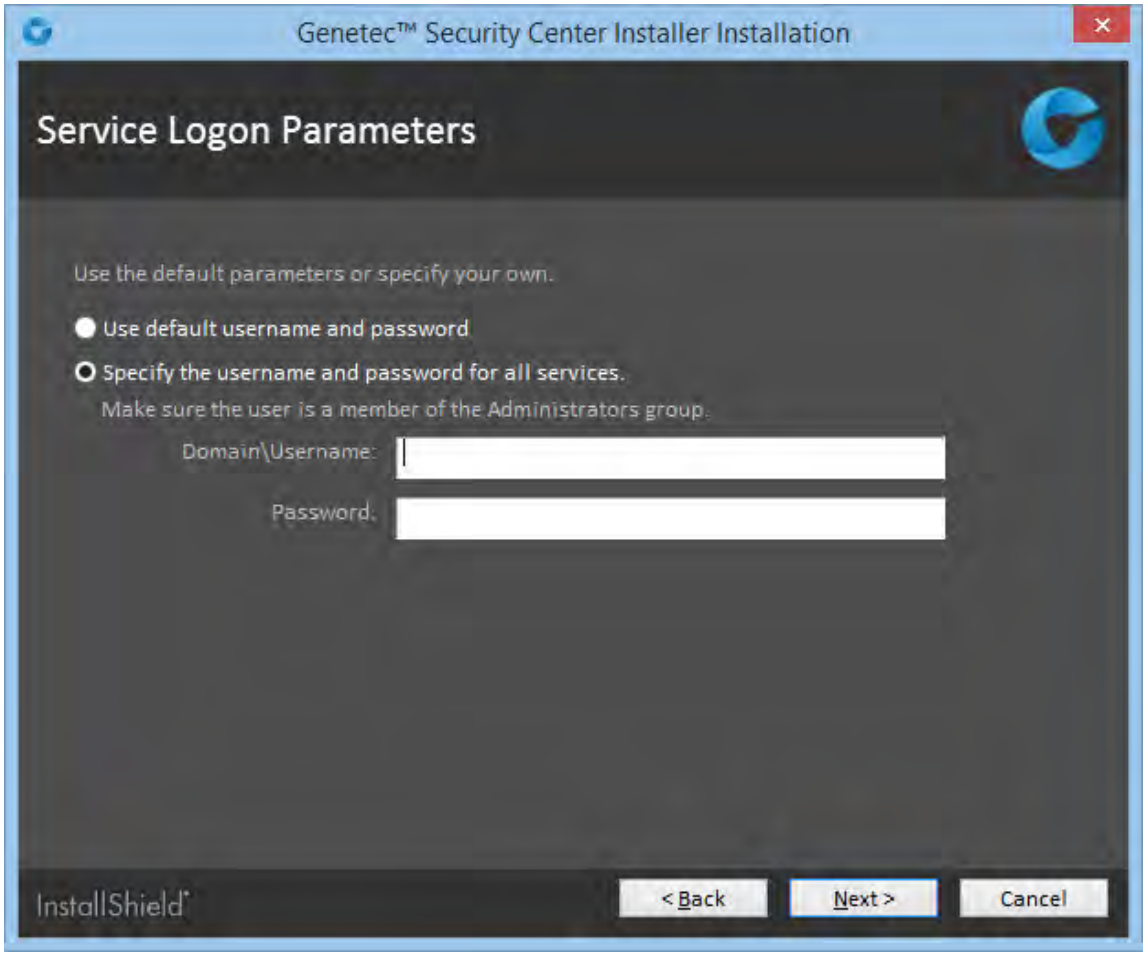
1. In Config Tool, open the *System* task.
2. Click the **General settings** view.
3. Select the *User password settings* page, and create your password policy.



Password policy configurations in the *System* task in Config Tool

4.3 Use a strong password for the Genetec™ Server Windows service account (Basic level, Advanced level)

If the option **Use default username and password** is selected, Security Center uses the predefined LocalSystem account. If you want to use a different user account, make sure to use a strong password. This account is used to run the Genetec™ Server service, and administrator privileges are required. However, only local privileges on the machines are needed and not domain privileges. The use of a domain admin is not recommended.

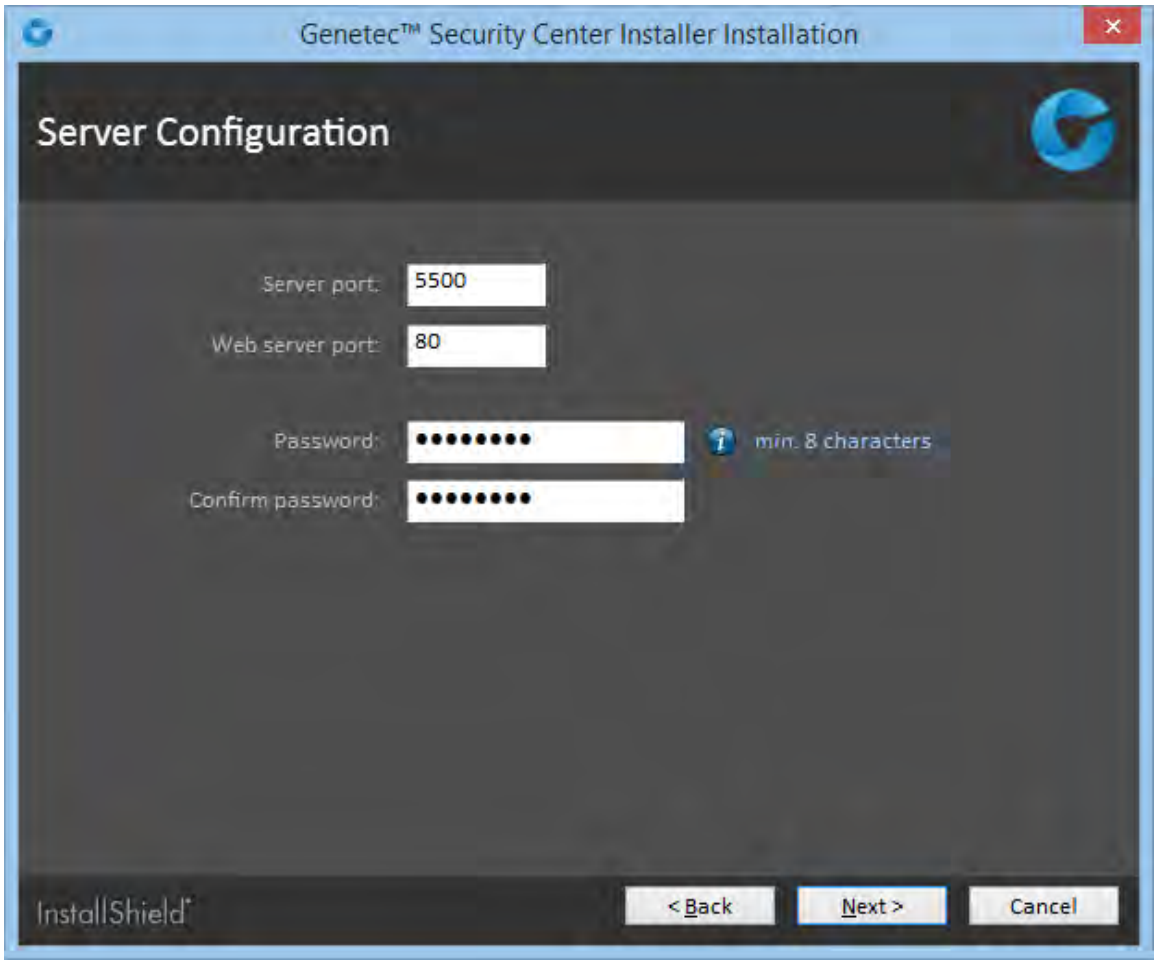


Service Logon Parameters in the Install Shield

4.4 Change the default logon password for Security Center servers (Basic level, Advanced level)

4.4.1 Installing a main server

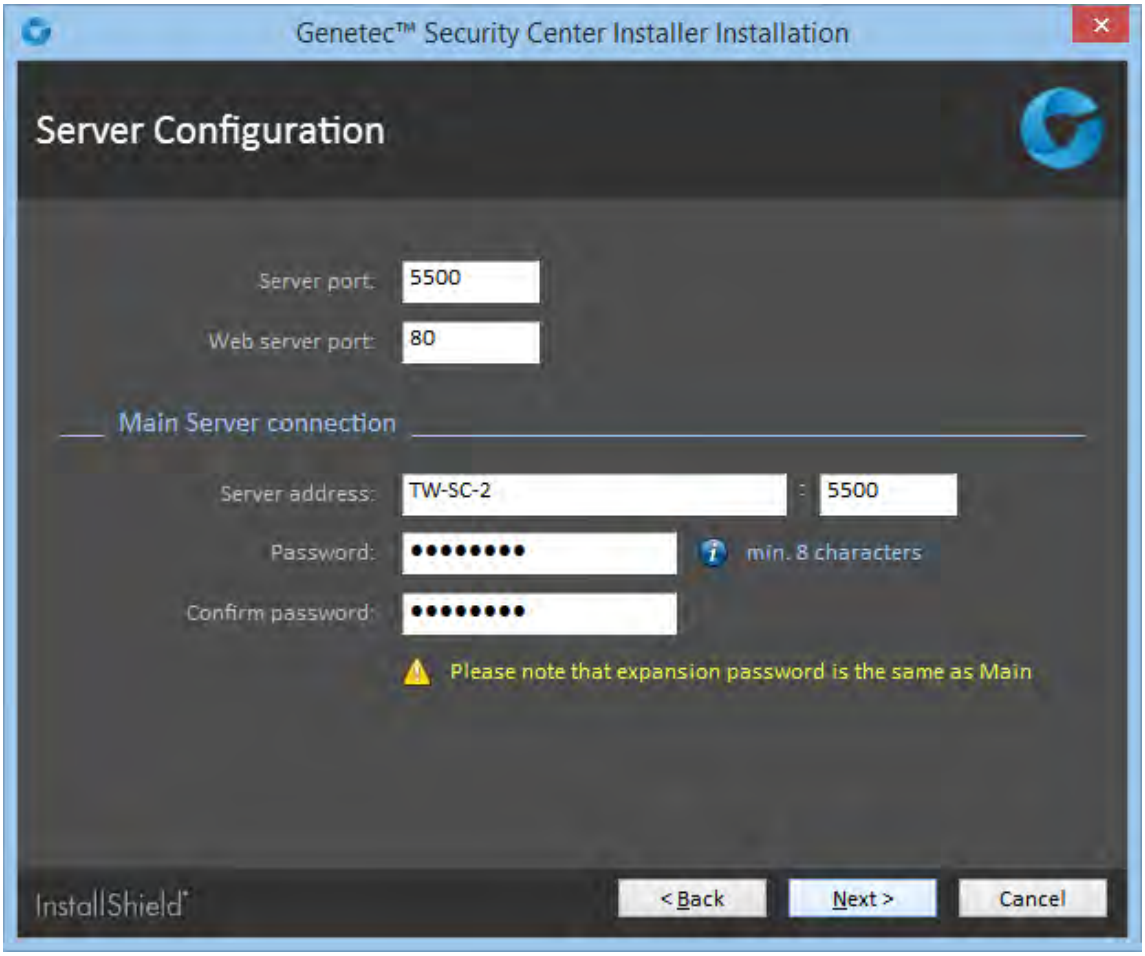
Use a long, unique, random password for your main server. This is the password you must enter in Server Admin to access the configuration settings of your main server. The installation wizard requires you to enter a password with a minimum length of 8 characters.



Server Configuration for a main server in the Install Shield

4.4.2 Installing an expansion server

Use the same password that you created for your main server.



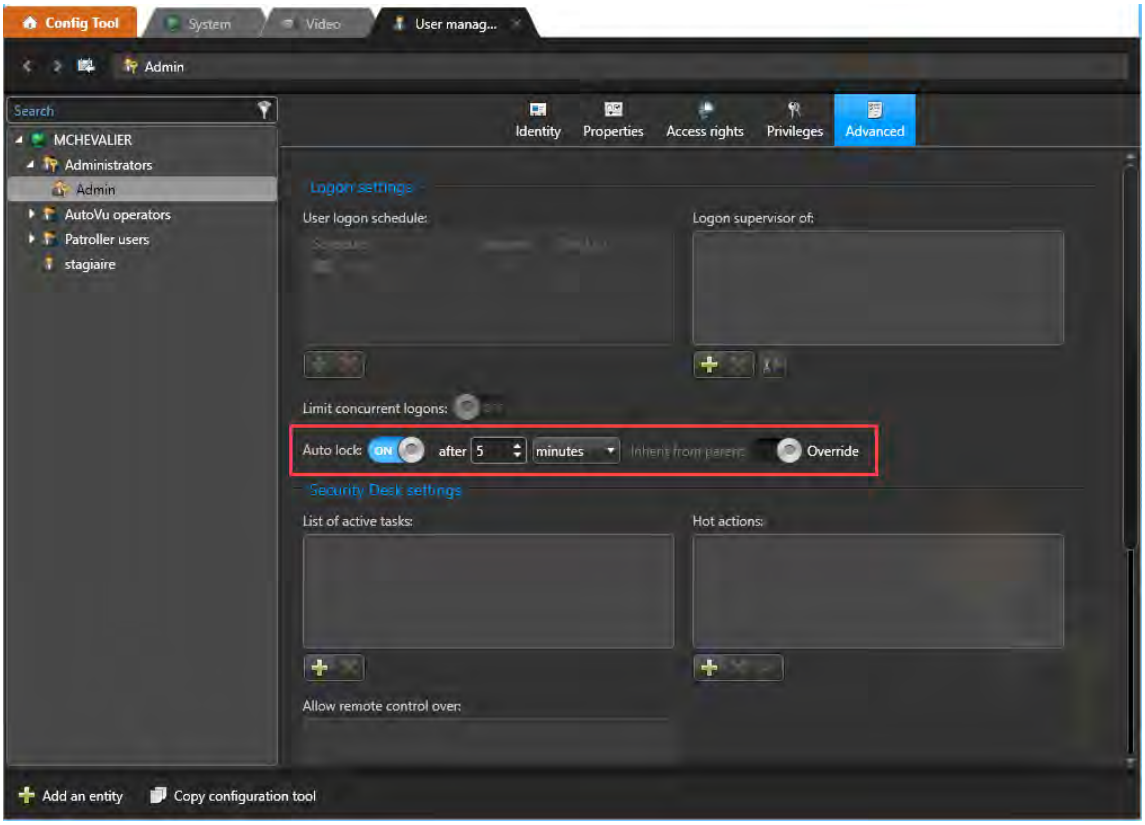
Server Configuration for an expansion server in the Install Shield

4.5 Activate auto locking for Security Desk after a period of inactivity (Basic level, Advanced level)

A Security Desk system that is left unattended can be used by an intruder to access the system. Activate the auto lock feature to automatically log off a user from the system when no action is detected from the user's workstation.

To activate auto lock:

1. In Config Tool, open the *User Management* task.
2. Click the **Advanced** tab.
3. Set **Auto lock** to **ON** and configure the rest of the settings.



Auto lock configurations in the *User management* task in Config Tool

Automatic session logout in Security Desk

4.6 Configure the Federation™ user (Advanced level)

The Federation™ role uses a remote user account to connect to a remote Security Center system. You should configure a dedicated user account on the remote system specifically for this purpose. Do not use a user account with administrative privileges for the Federation™ feature. You should assign this user only the minimum set of privileges required.

4.7 Use Windows Active Directory Integration (Advanced level)

It is possible to log into Security Center using Windows credentials. You can do this by synchronizing the Windows Active Directory with the Security Center Active Directory role. Using this feature allows you to manage all user accounts from a single location in your organization, thereby reducing errors and facilitating user account management. A strong password policy including a minimum password length, complexity, and expiration period should be enforced for Active Directory user accounts.

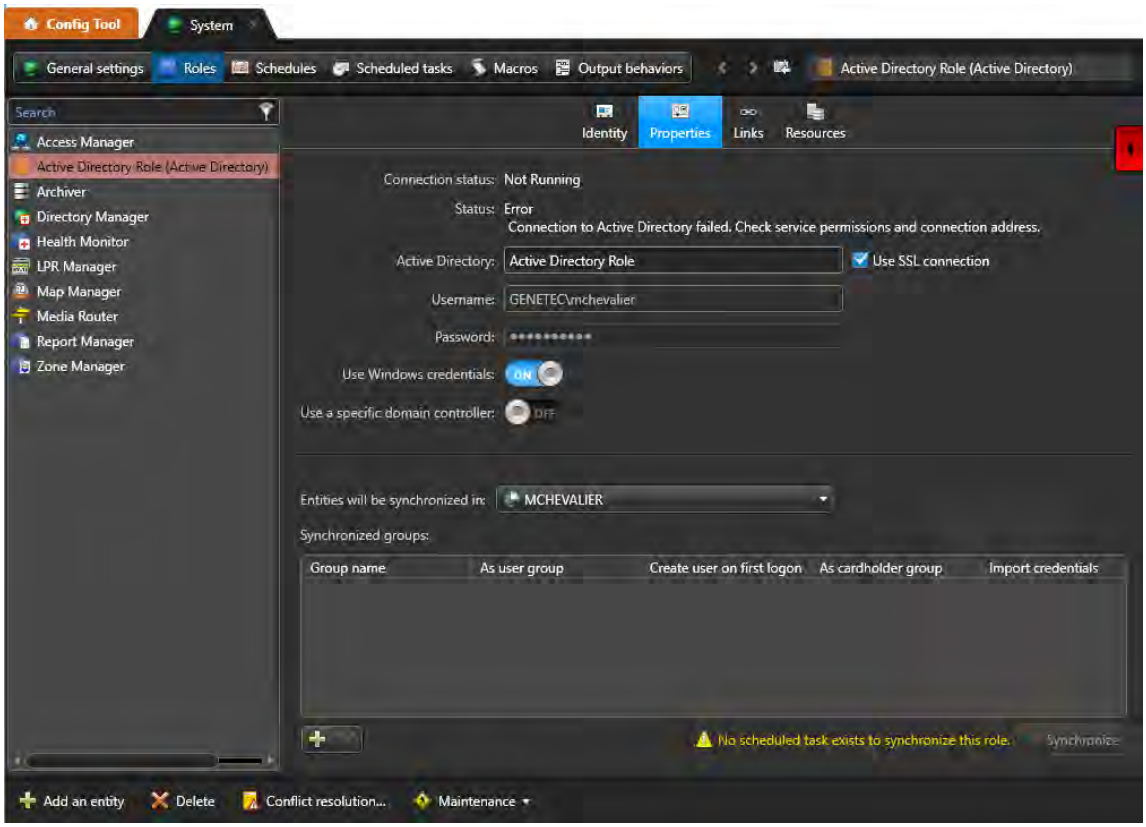
Use a unique Active Directory account for the Active Directory role that has the capability to read all Active Directory forest entities (but do not use a domain administrator). This approach allows you to monitor access attempts to the Active Directory role, and reduces the risk of causing unintended modifications to your domain content due to a compromised system.

It is also important that you activate the SSL connection option in the configuration of the Active Directory role.

To configure your Active Directory role:

1. In Config Tool, open the *System* task.
2. Click the **Roles** view, and select the *Active Directory Role (Active Directory)* page.
3. Click the **Properties** tab, and make your modifications.

Refer to the chapter on Active Directory integration in the *Security Center Administrator Guide* for more details.



Active Directory role configuration in the *System* task in Config Tool

4.8 Use claims-based authentication to authenticate a user for Security Center (Advanced level)

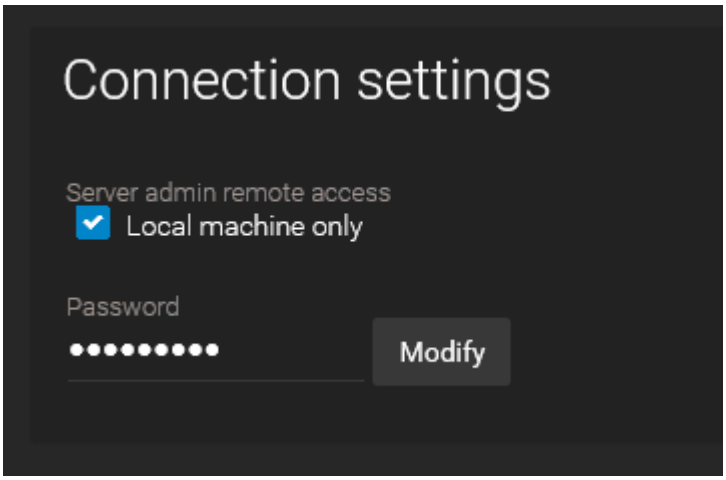
Claims-based authentication is a way for external users to log on to Security Center if your company's IT service does not have the ability to verify their identity. One way to do this is to use an Active Directory Federation Service (ADFS). Refer to the chapter on claims-based authentication in the *Security Center Administrator Guide* for more details.

4.9 Restrict Server Admin access to local connection only (Advanced Level)

You can configure Server Admin so that only local users of the Security Center server (the machine where Genetec™ Server is installed) can access it.

To restrict Server Admin access:

1. Open Server Admin.
2. Click the *Overview* page.
3. Under *Connection settings*, select **Local machine only.** Enabling this removes the multi-server capability of Server Admin.



Connection settings in Server Admin

4.10 Restrict user privileges (Advanced level)

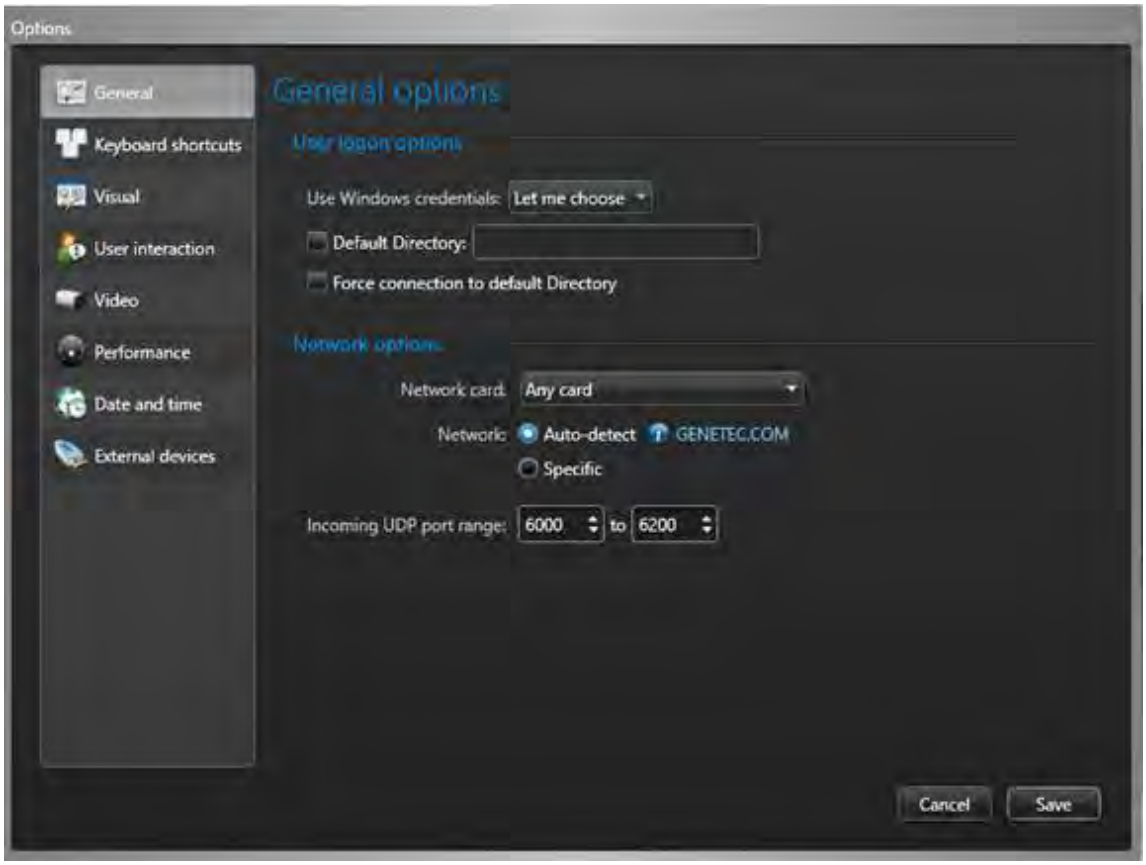
In Security Center, you can configure what each user can do, such as arming zones, blocking cameras, and unlocking doors. These settings are called *Privileges* in Security Center. We recommend that you assign each user only the privileges that they require to perform their job, and no more. Multiple templates already exist in Security Center with a predefined set of

privileges (Operator, Investigator, Supervisor, and so on). Refer to the chapter on Users and User groups in the *Security Center Administrative Guide* for more information.

Users should also be limited by partitions that provide access to only the entities related to their work. For more information, see Control access to your resources (Advanced level).

4.11 Restrict connection of client applications to a specific Directory (Advanced level)

Apart from user access management, it is also possible to restrict Config Tool and Security Desk to connect to a specific Directory. This can be configured under **Options > General** in the client applications.



Default Directory configuration in Config Tool

5 System

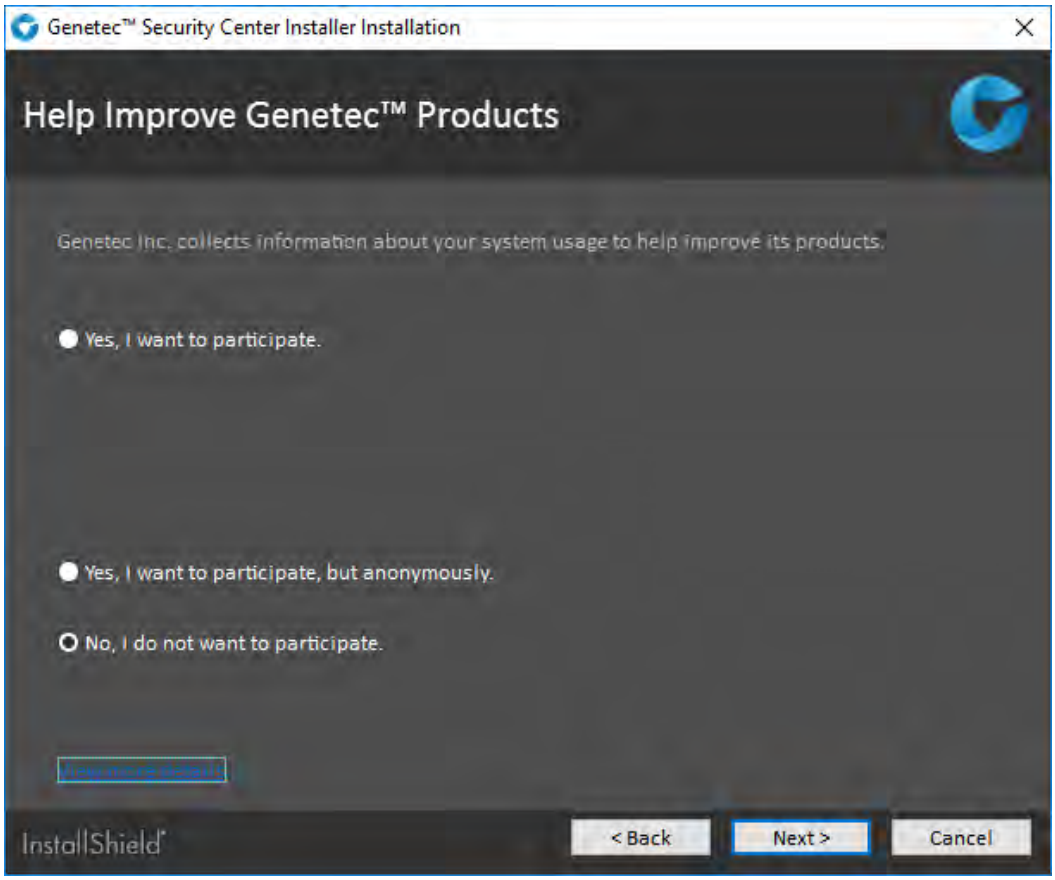
5.1 Use the recommended security settings from the Install Shield (Basic level)

Beginning in Security Center 5.6, the Install Shield offers new default security settings. Client applications will now trust the server certificates upon first connection, and will warn the user if certificates change in subsequent connections. This represents the best balance in terms of security and convenience for users who do not want to manage the server certificate themselves. These certificates will be used to establish TLS connection between the Directory and clients (Security Desk, Config Tool), and also between the Genetec™ servers. For more information, refer to the chapter on TLS and Directory authentication in the *Security Center Administrator Guide*.

Security Settings page in the Install Shield

5.2 Review the Product Improvement Program (Basic level, Advanced level)

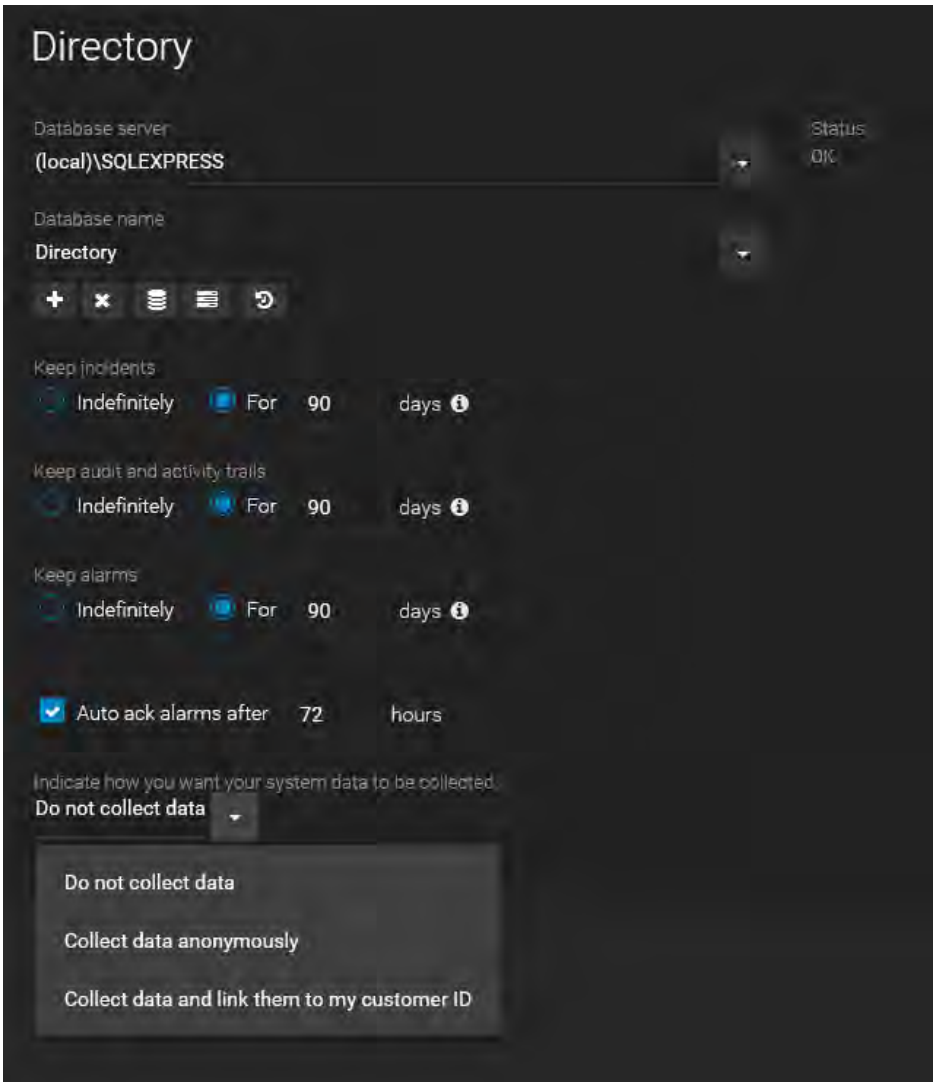
The goal of the Product Improvement Program is to collect data on the usage and the availability of our products. This helps us to collect feedback on how our products are used and where to focus our efforts. However, sharing system data might pose privacy concerns for some customers. Make sure to choose the right option according to your privacy policy. This option is chosen during installation and can be modified in Server Admin.



Help Improve Genetec™ Products page in the Install Shield

To modify your data collection settings:

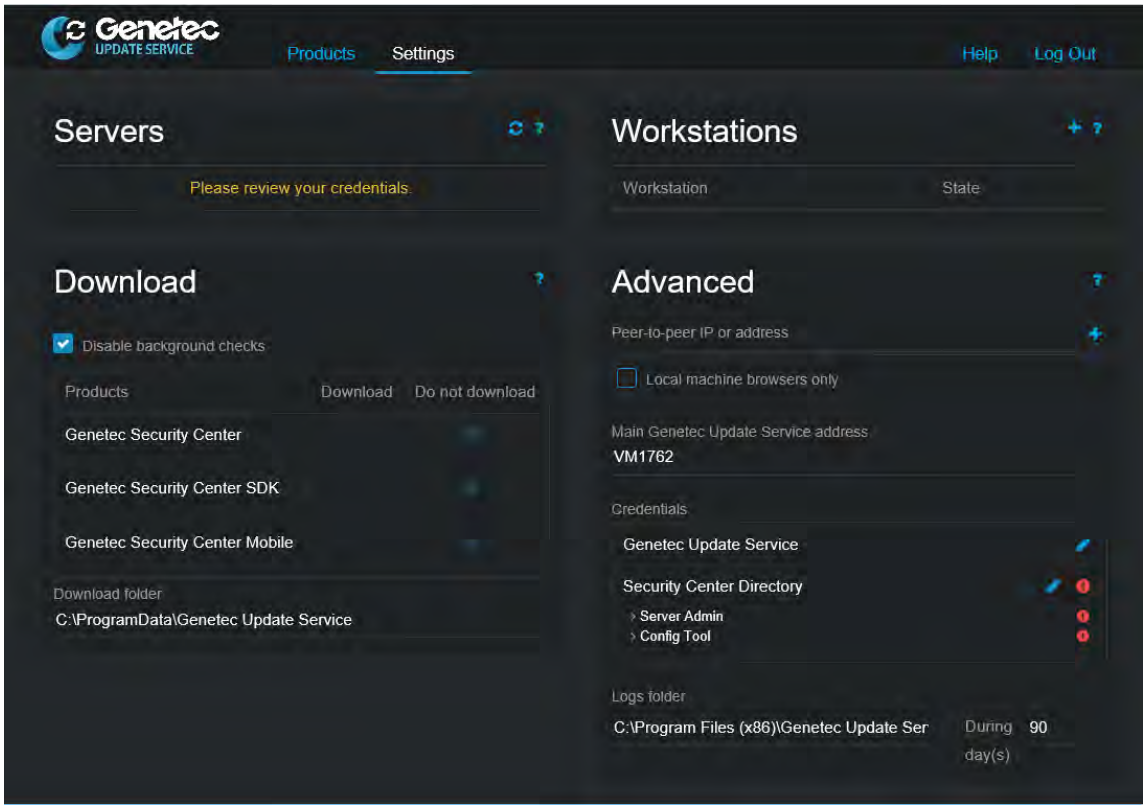
1. Open Server Admin.
2. Select your server from the **Servers** list.
3. Under **Indicate how you want your system data to be collected,** select your method of data collection from the drop-down list.



Data collection options in Server Admin

5.3 Keep Security Center updated with the Genetec™ Update Service (Basic level, Advanced level)

Keep your version of Security Center up-to-date to ensure that you have the latest security fixes and improvements. The Genetec™ Update Service (GUS) is installed with Security Center and automatically keeps your system up-to-date if you have Internet access. You can also install your updates manually. Go to https://gtap.genetec.com to get the latest Security Center version.



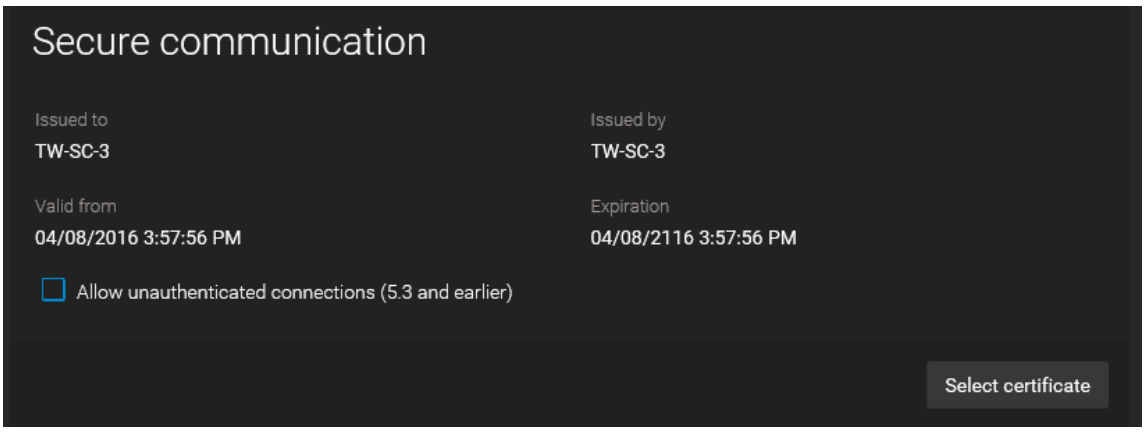
Settings page in Genetec™ Update Server

5.4 Use trusted certificates on Security Center servers (Advanced level)

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. Make sure to check the option **Always validate the Directory certificate** in the advanced *Security Settings* page of the Install Shield:

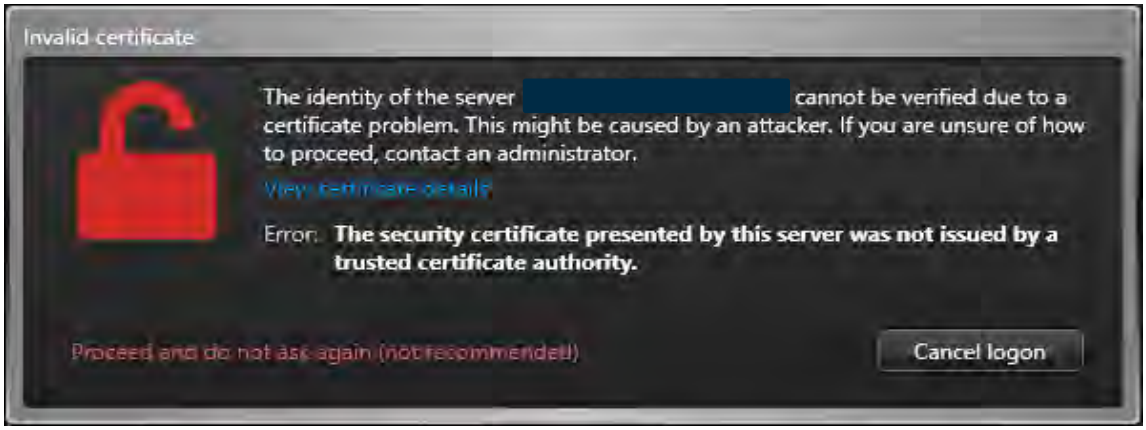
Custom (advanced) *Security Settings* page of the Install Shield

The certificate used by the Genetec™ Server service can be configured in Server Admin on each server:



Certificate information in Server Admin

If users do not use a trusted certificate, the following dialog box appears which forces the user to make a security decision that they might not be qualified to make.



Identity warning pop-up

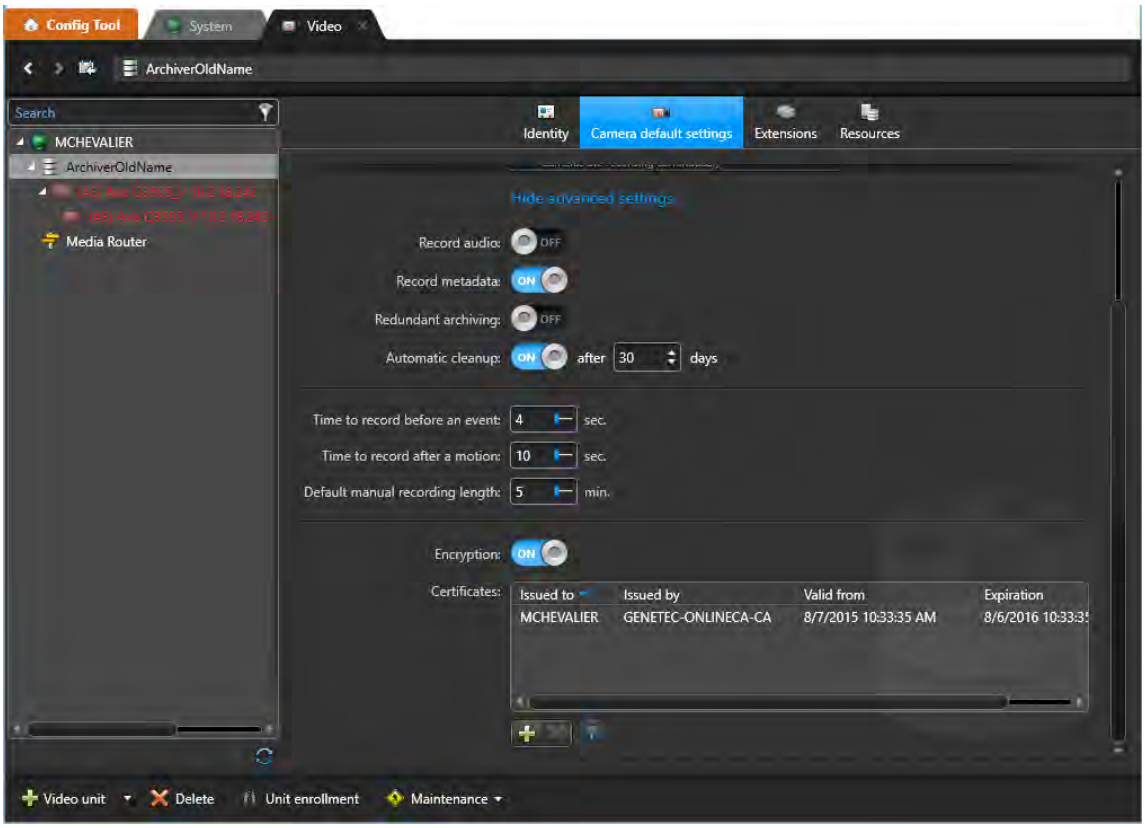
For more information, refer to the chapter on replacing default certificates in the *Security Center Administrator Guide*.

5.5 Control access to your resources (Advanced level)

Security Center provides a convenient way to manage access to the system resources. You can group related assets (buildings, equipment, cameras, important data collected in the fields, etc.) in a container called a partition. You can then control which users or user groups can access each partition. For more information, read the chapter on partitions in the *Security Center Administrator Guide*.

5.6 Use fusion stream encryption to protect your data (Advanced level)

Consider enabling fusion stream encryption to protect your multimedia stream (video, audio, etc.) both at rest and in transit. For a video stream, the Archiver 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. For more information, refer to the chapter on fusion stream encryption in the *Security Center Administrator Guide*.



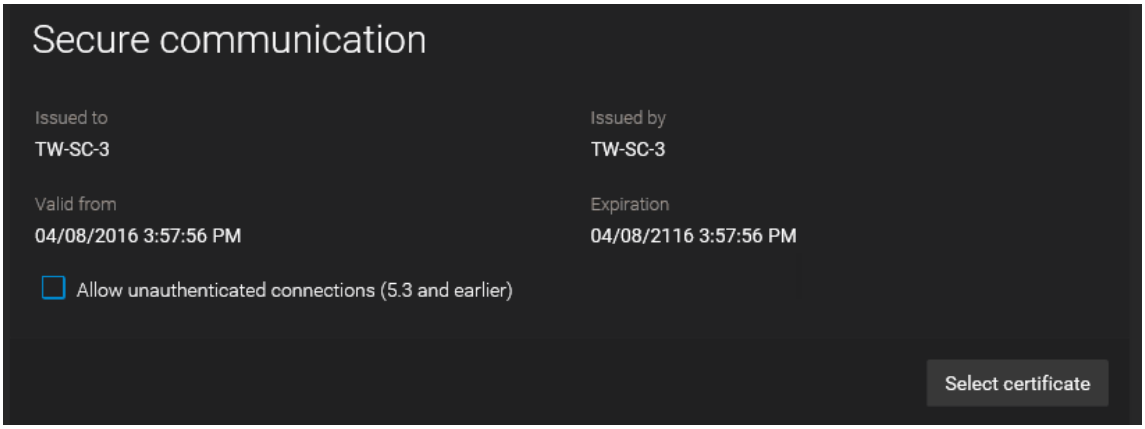
Fusion stream configuration in Config Tool

5.7 Do not use Security Center in backward compatibility mode (Advanced level)

Security fixes and improvements are constantly added into Security Center. Sometimes architectural changes are needed and it is not always possible to port them into an older version of the product. Consequently, using Security Center in backward compatibility mode might pose a security risk. We recommend that you only use backward compatibility mode when you are in the process of upgrading your system.

To disable backward compatibility:

1. Open Server Admin.
2. Select your main server from the **Server** list.
3. Under *Secure communication*, clear the **Allow unauthenticated connections (5.3 and earlier)** option.



Secure communication section in Server Admin

5.8 Use a Directory gateway when outsiders need access to a Security Center system that resides on a secure network (Basic level, Advanced level)

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 Directory server must connect to the Directory database, and the Directory gateway must not for security reasons. For more information, refer to the chapter on system security in the *Security Center Administrator Guide*.

6 Video

6.1 Turn off basic authentication (Basic level, Advanced level)

Basic authentication means that camera passwords are sent in clear text over the network. Therefore, an attacker only has to passively listen to capture the passwords. Because of this, you should turn off basic authentication when interacting with cameras during installation. Be aware that some camera manufacturers only support basic authentication, so disabling this authentication might cause some cameras to be unable to connect to Security Center. Basic authentication is disabled by default when the **Recommended** security setting is selected. If you do want to enable basic authentication, select **Custom (Advanced)** and click **Next** to adjust your settings on the advanced *Security Settings* page of the Install Shield.

Security Settings page in the Install Shield

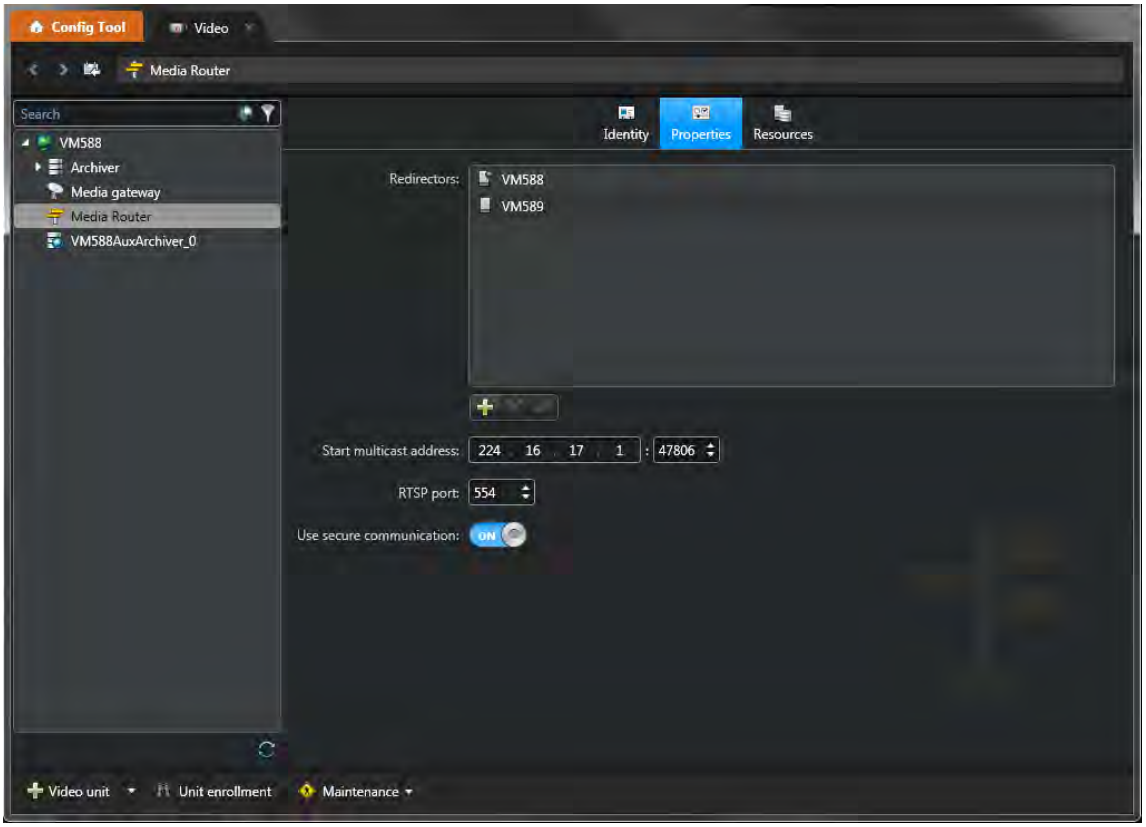
Advanced *Security Settings* page of the Install Shield

6.2 Turn on secure communication in the Media Router (Basic level, Advanced level)

Beginning in Security Center 5.5, the connection made by Security Desk when requesting a video sequence is authenticated and encrypted using the TLS protocol. This feature is set to **ON** by default.

To activate or deactivate secure communication:

1. In Config Tool, open the *Video* task.
2. Select the *Media Router* page.
3. Click **Properties**.
4. Set **Use secure communication** to the desired setting.



Using secure communication in the Media Router

6.3 Update camera firmware (Basic level, Advanced level)

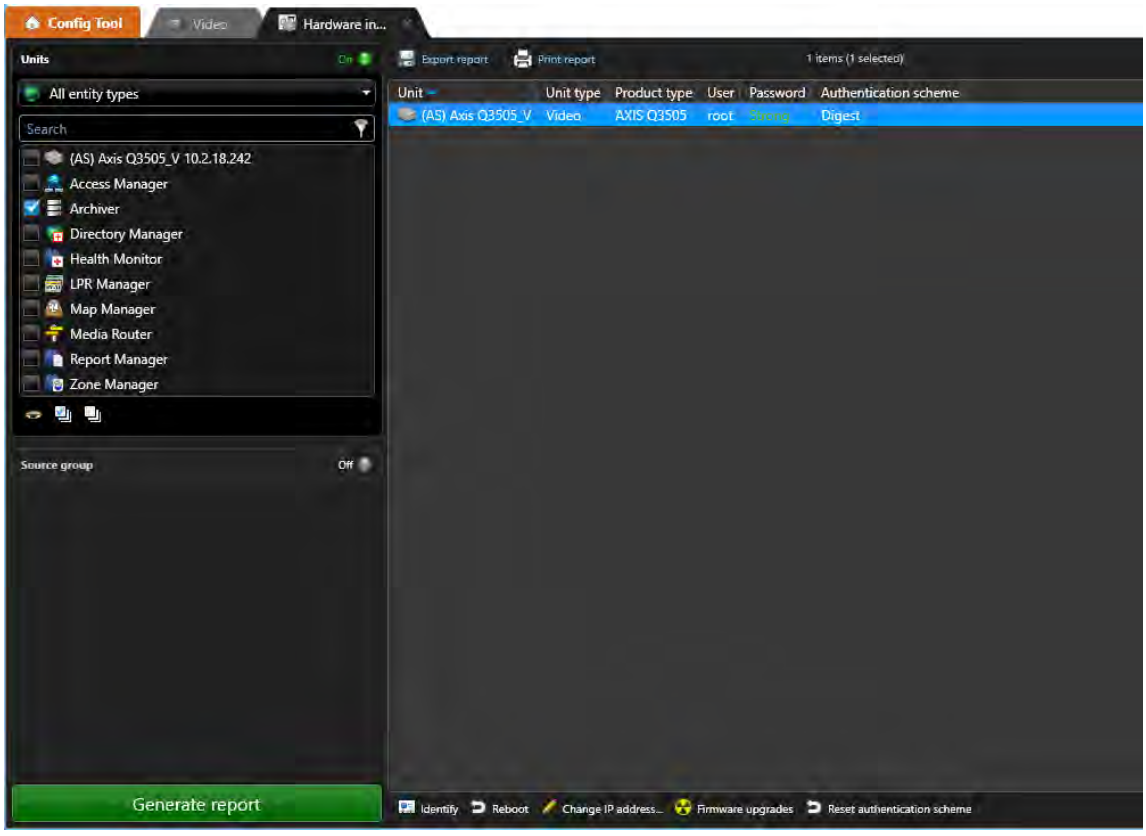
Camera manufacturers frequently update their products and fix security vulnerabilities within new firmware. Therefore, it is best practice to update cameras with the latest firmware certified by Genetec Inc.

6.4 Change default admin passwords for cameras (Basic level, Advanced level)

Some cameras ship with default administrative passwords. **Do not use default passwords when connecting to cameras**, since these passwords might be known. Change the passwords on the camera's webpage prior to adding the cameras in Security Center.

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

You can review the strength of your camera's password and its authentication scheme in the *Hardware inventory* task in Config Tool:



Viewing password strength in the *Hardware inventory* task in Config Tool

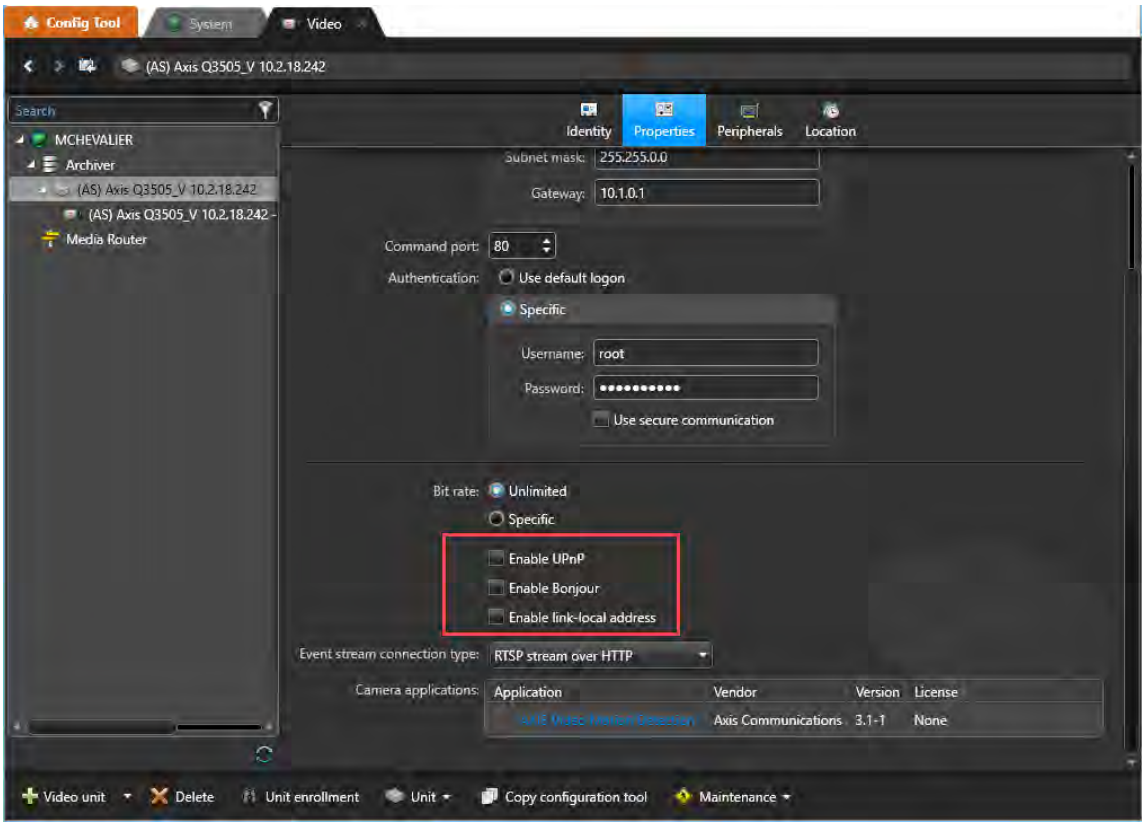
6.5 Connect to cameras through HTTPS (Advanced level)

Activate https connections between the Archiver and compatible cameras, which include Axis, Bosch, Euklis, Extreme CCTV, Genetec™ Protocol, Intelbras, IONODES, ISD, March Networks, OTN Systems, SightLogix, Sony, and Verint. Note that a certificate must be installed on the cameras and that the certificate must be trusted by the Archiver.

Manual add pop-up window for adding a camera with HTTPS activated

6.6 Deactivate unused services and roles (Advanced level)

All active services and roles increase the attack surface. It is possible that an attacker finds an exploitable vulnerability in any of these software components. As a defense in depth strategy, it is recommended to deactivate any unused services and roles to reduce this risk. Some of the services that can be disabled inside Security Center for most users are UPnP, Bonjour, and Local-link Address.

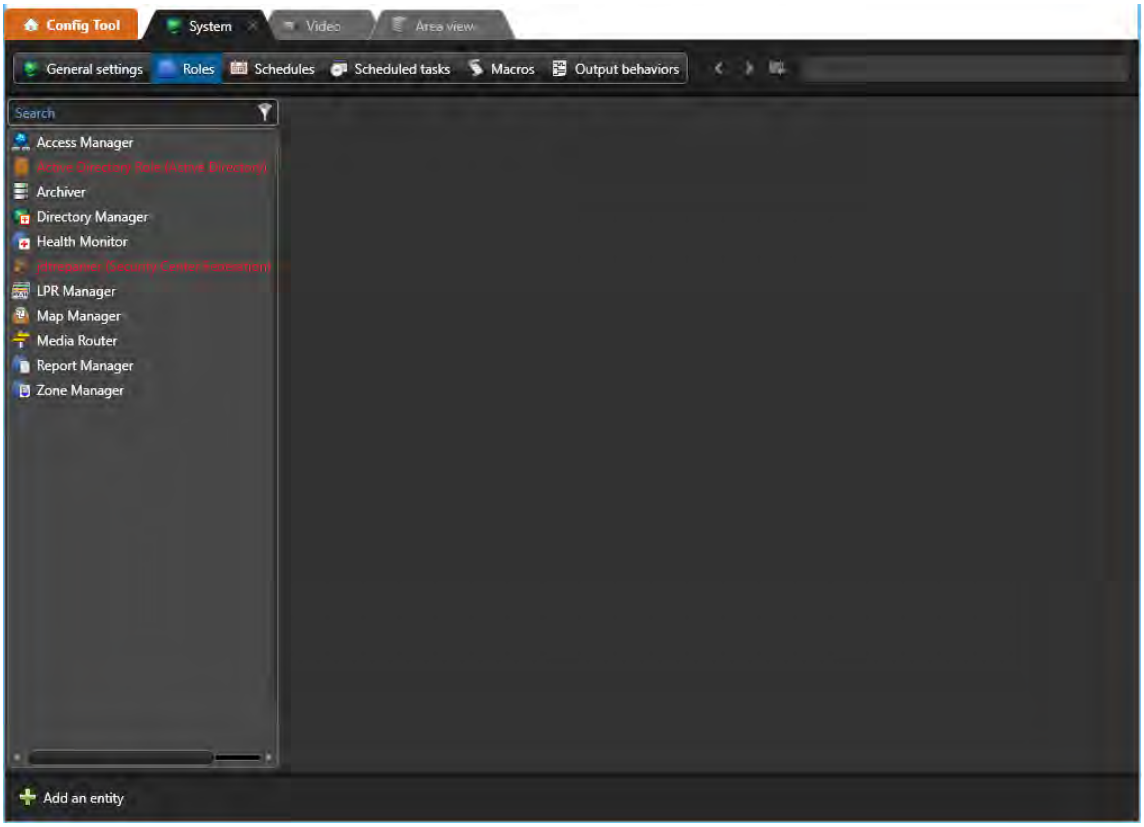


Disabling unused services on the *Properties* page of a camera

Multiple roles are activated by default and might not be needed by all users.

To review your activated roles:

1. In Config Tool, open the *System* task.
2. Click the **Roles** view.
3. Deactivate all roles that are not in use.

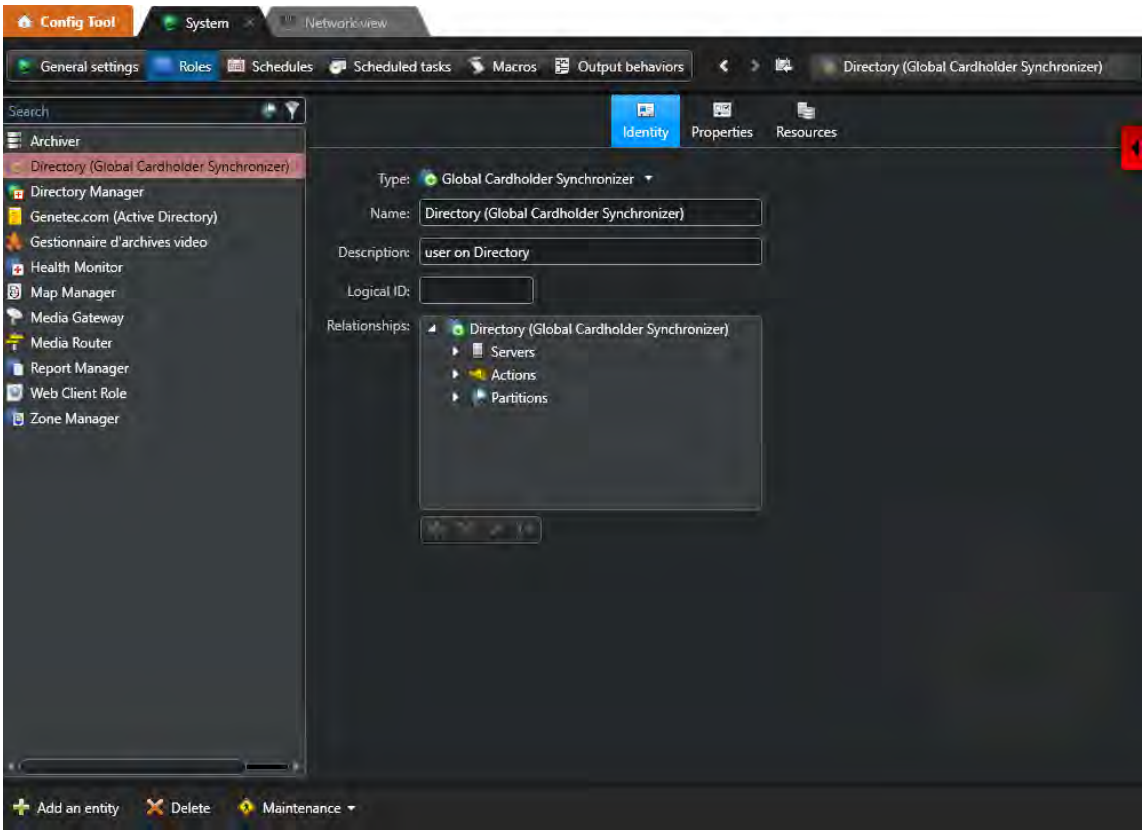


Role configuration in the *System* task

7 Access Control

7.1 Global Cardholder Synchronizer (Basic level, Advanced level)

The 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 GSC role on a sharing guest system requires a dedicated user on the sharing host system in order to connect to the latter. The dedicated user should not be an administrator of the entire system. Grant just enough privileges and access rights to the dedicated user for the sharing guest to perform what they need. 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.



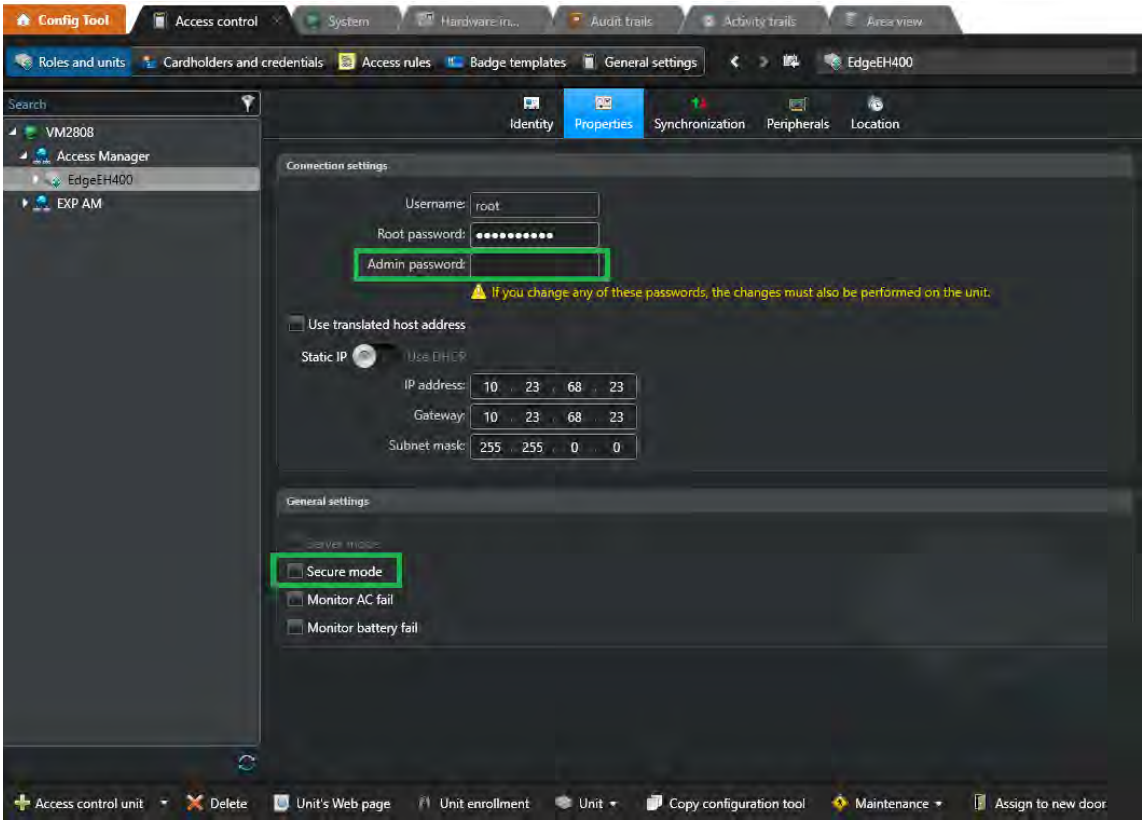
Global Cardholder Synchronizer Role in Config Tool

7.2 HID Extension

7.2.1 Enable Secure mode on HID units (Basic level, Advanced level)

A **Secure mode** option has been added for HID units that support it. When **Secure mode** is enabled, Telnet, FTP, and SSH protocols are disabled, and communication between the HID access control unit and the Access Manager is encrypted. Communication between the access control unit and the Access Manager is protected from packet sniffing, replay attacks, and injection attacks. See the *Security Center Release Notes* for supported firmware versions.

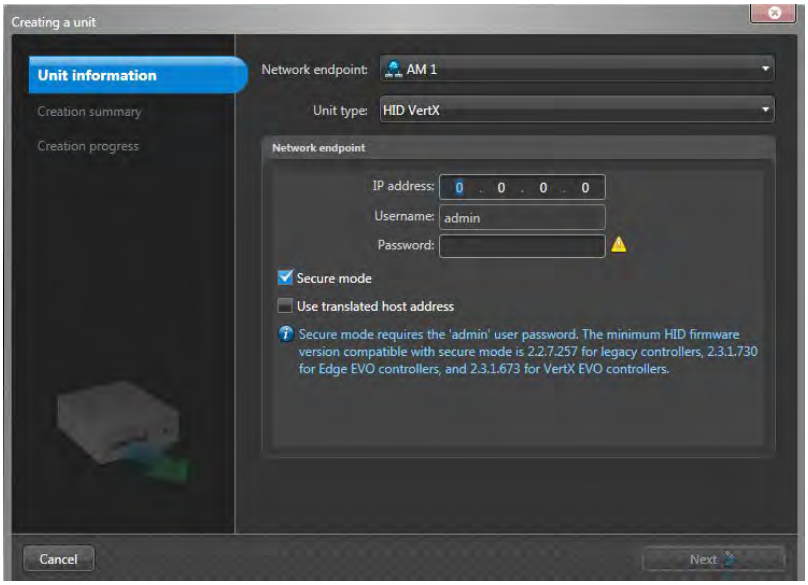
We recommend enabling **Secure mode** on HID access control units. The HID **Admin password** is required to enable **Secure mode**.



Role configuration in Config Tool

7.2.2 Enroll HID access control units with Secure mode enabled (Basic level, Advanced level)

We recommend adding HID access control units to the Access Manager with **Secure mode** enabled.

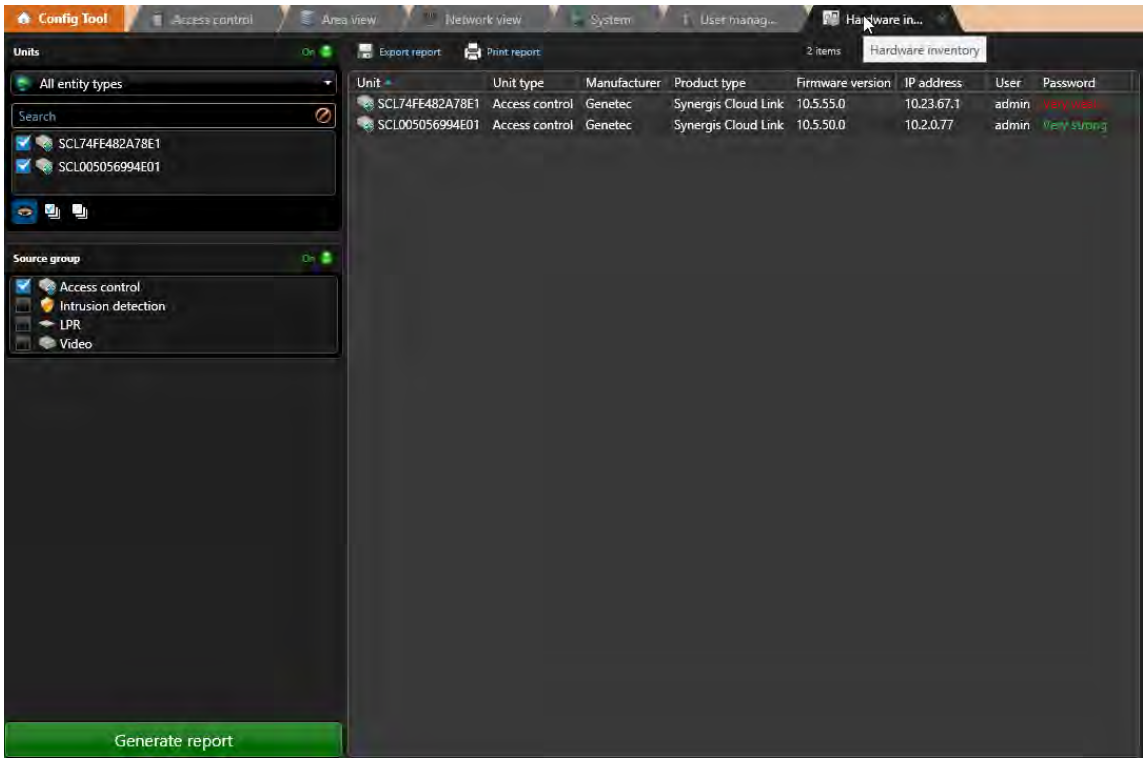


Creating a unit with **Secure mode** enabled

7.2.3 Change the default Admin password for HID controller (Basic level, Advanced level)

We recommend that you use a strong HID admin password. A valid admin password is between 6 and 10 characters in length, and can include all printable ASCII characters from 32 to 126 (decimal). See http://www.asciitable.com for more guidelines.

You can review the strength of your HID admin password in the *Hardware inventory* task in Config Tool.



Hardware inventory task in Config Tool

7.2.4 Update HID access control units with the latest firmware (Basic level, Advanced level)

To ensure you have the latest security fixes and improvements, keep the firmware for your HID access control unit up-to-date. For more information, see KBA01134.

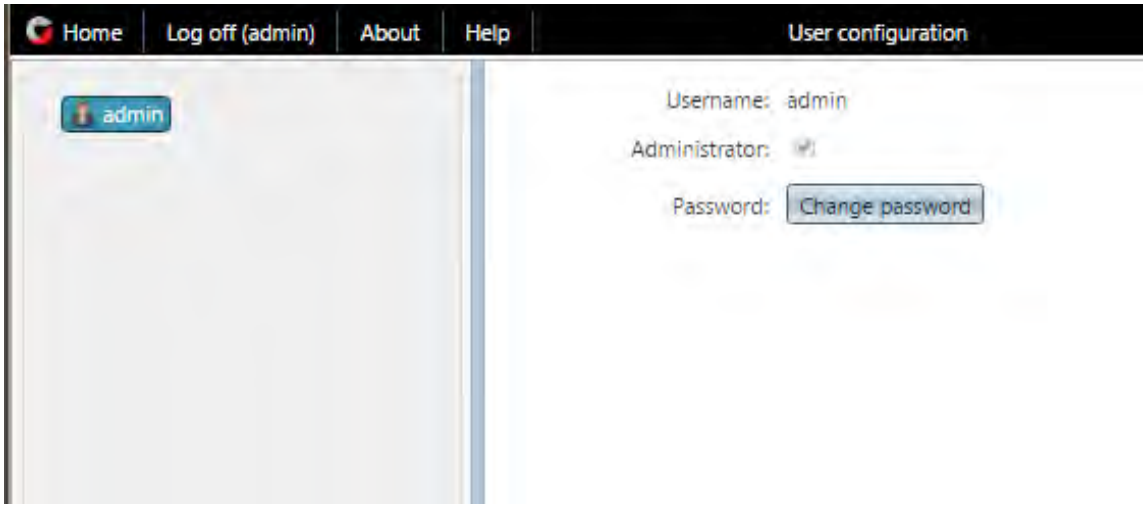
7.3 Genetec Synergis™ Extension

7.3.1 Synergis™ appliance firmware (Basic level, Advanced level)

To ensure that you have the latest security fixes and improvements, keep your Synergis™ appliance up-to-date with the latest Synergis™ Softwire firmware. Visit our Product download page for the latest Synergis™ Softwire firmware version.

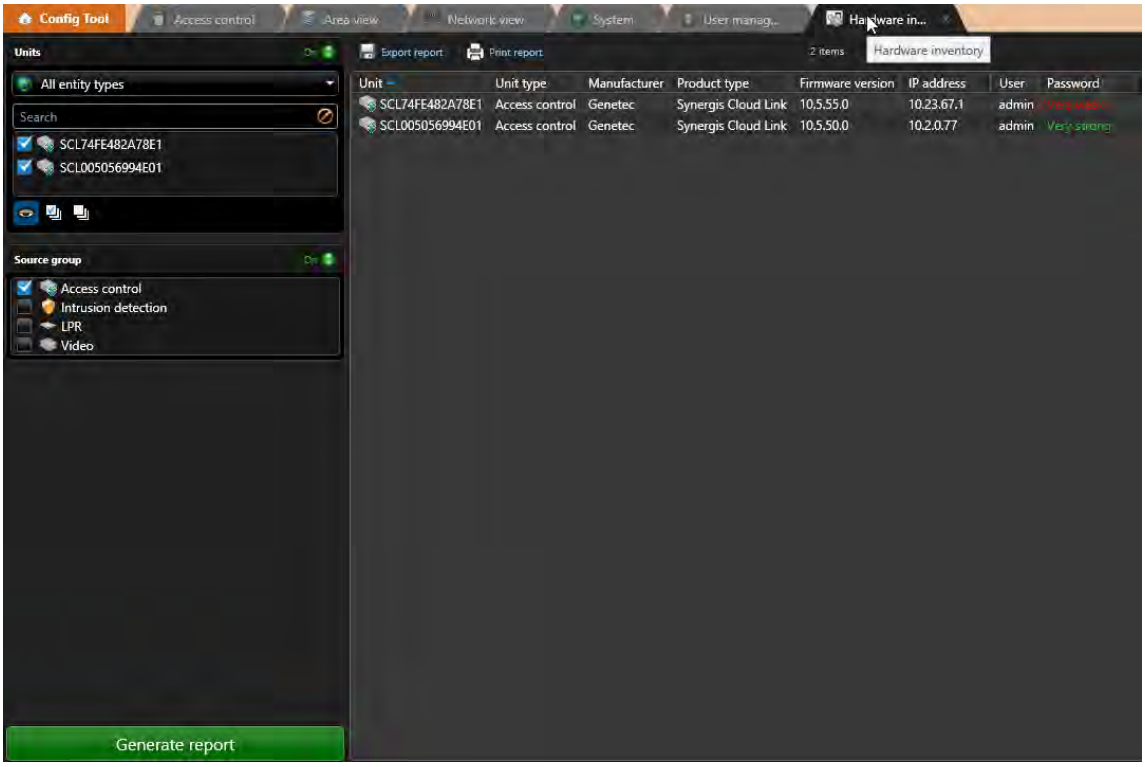
7.3.2 Change the default Admin password for your Synergis™ appliance (Basic level, Advanced level)

Synergis™ appliances are shipped with a default administrative password. **Do not use the default admin password** when adding your Synergis™ appliance to Security Center, since these passwords might be known to others. Change the default admin password using the Synergis™ Appliance Portal.



User configuration page in the Synergis™ Appliance Portal

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

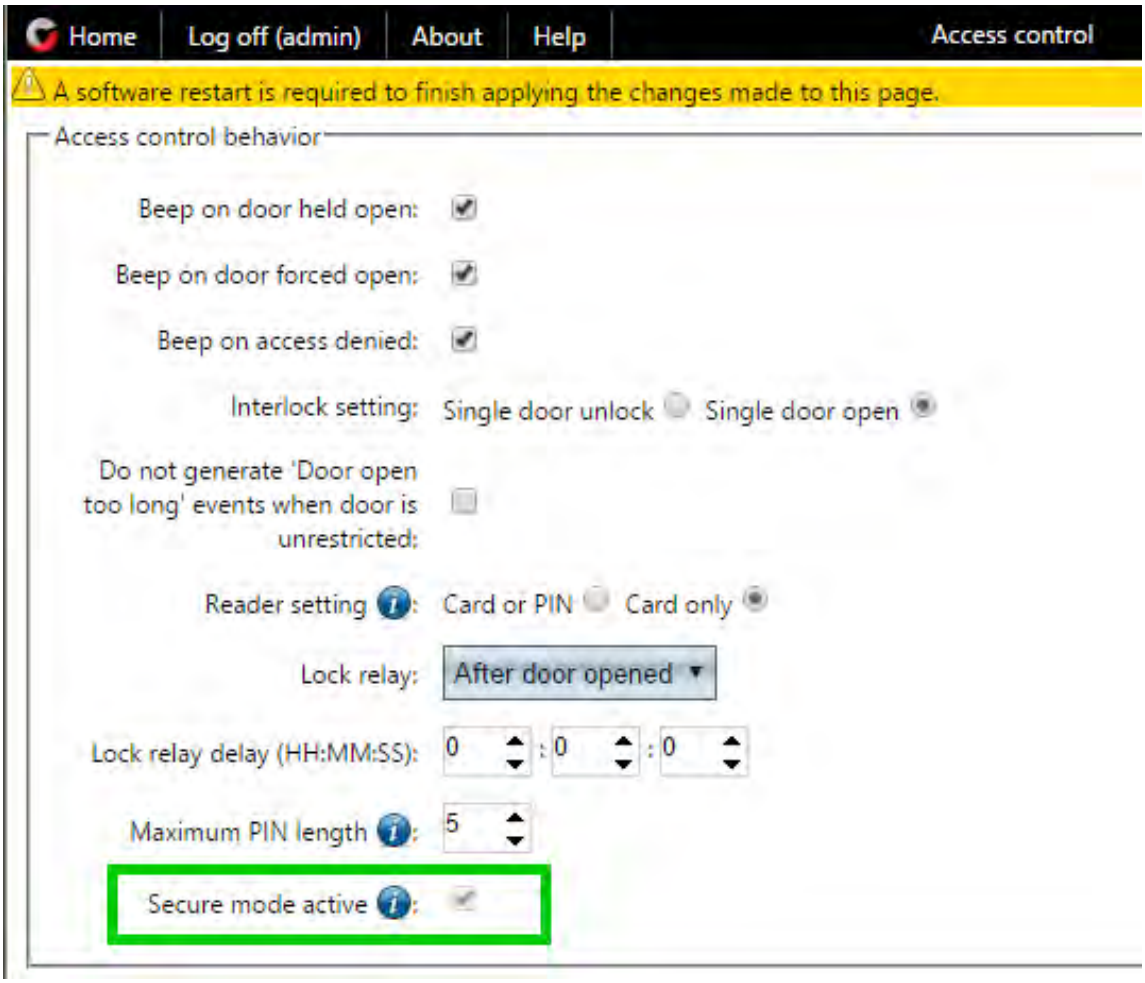


Hardware inventory task in Config Tool

7.3.3 Enable Secure mode on your Synergis™ appliance as soon as possible (Basic level, Advanced level)

Enabling **Secure mode** blocks all firmware upgrades that are not signed by Genetec Inc.

Important: Once enabled, **Secure mode** cannot be disabled using the Synergis™ Appliance Portal. It can only be disabled using a dual in-line package (DIP) switch command, which requires physical access to the unit.



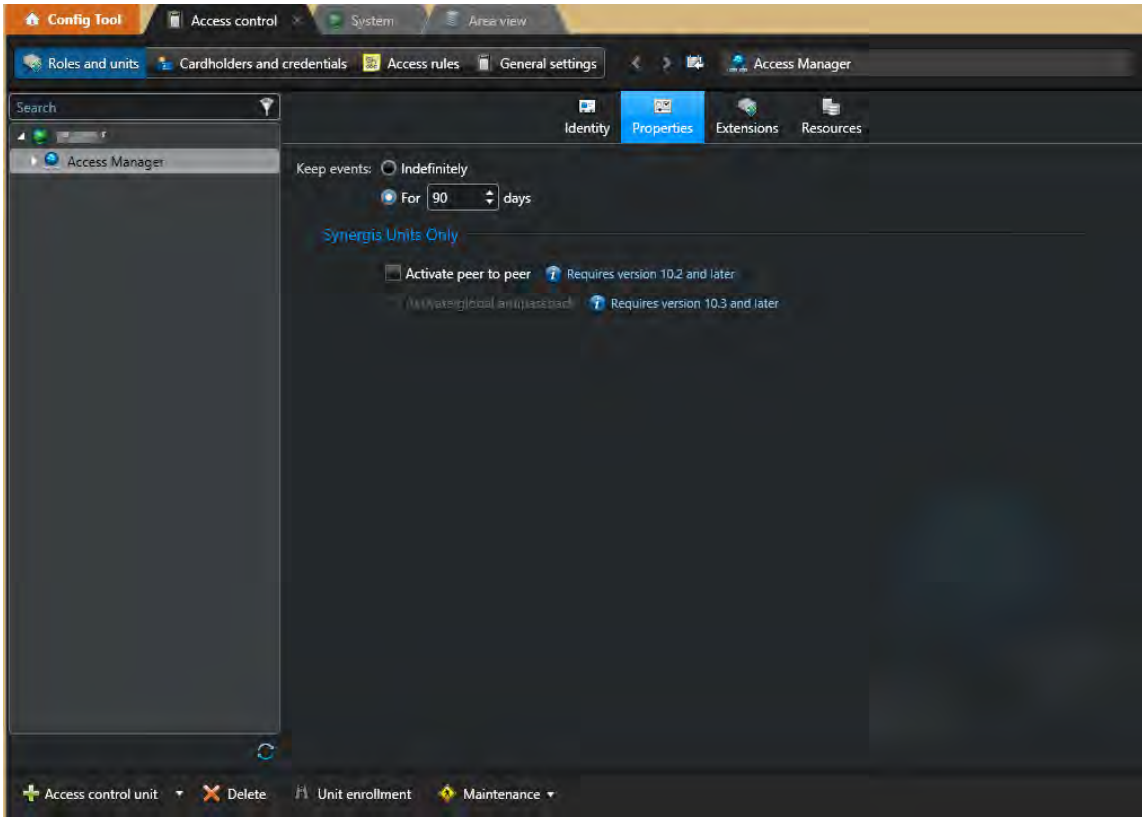
Secure mode settings on the *Access control* page in the Synergis™ Appliance Portal

7.3.4 Do not activate peer-to-peer and global antipassback for the Access Manager (Basic level, Advanced level)

If Global Antipassback or I/O zones are not used, do not activate these options.

To verify if these options are activated:

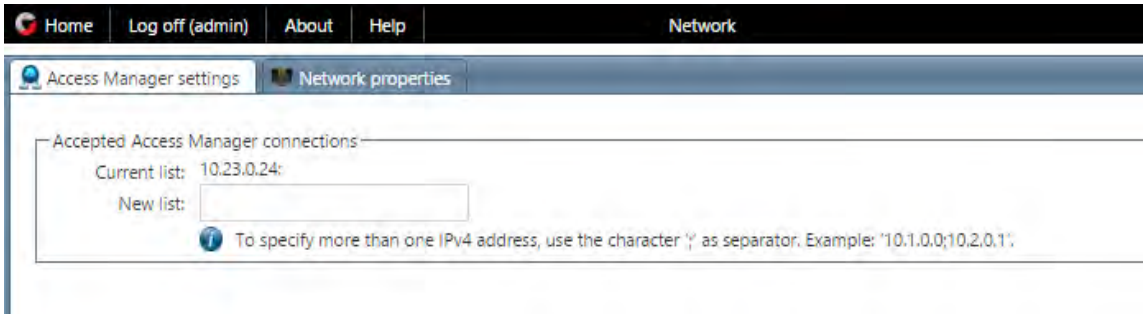
1. In Config Tool, open the *Access control* task.
2. Click **Roles and units**.
3. Open the *Access Manager* page and click the **Properties** tab. Make sure that the options for **Activate peer to peer** and **Activate global antipassback** have not been selected.



Properties page of the Access Manager in Config Tool

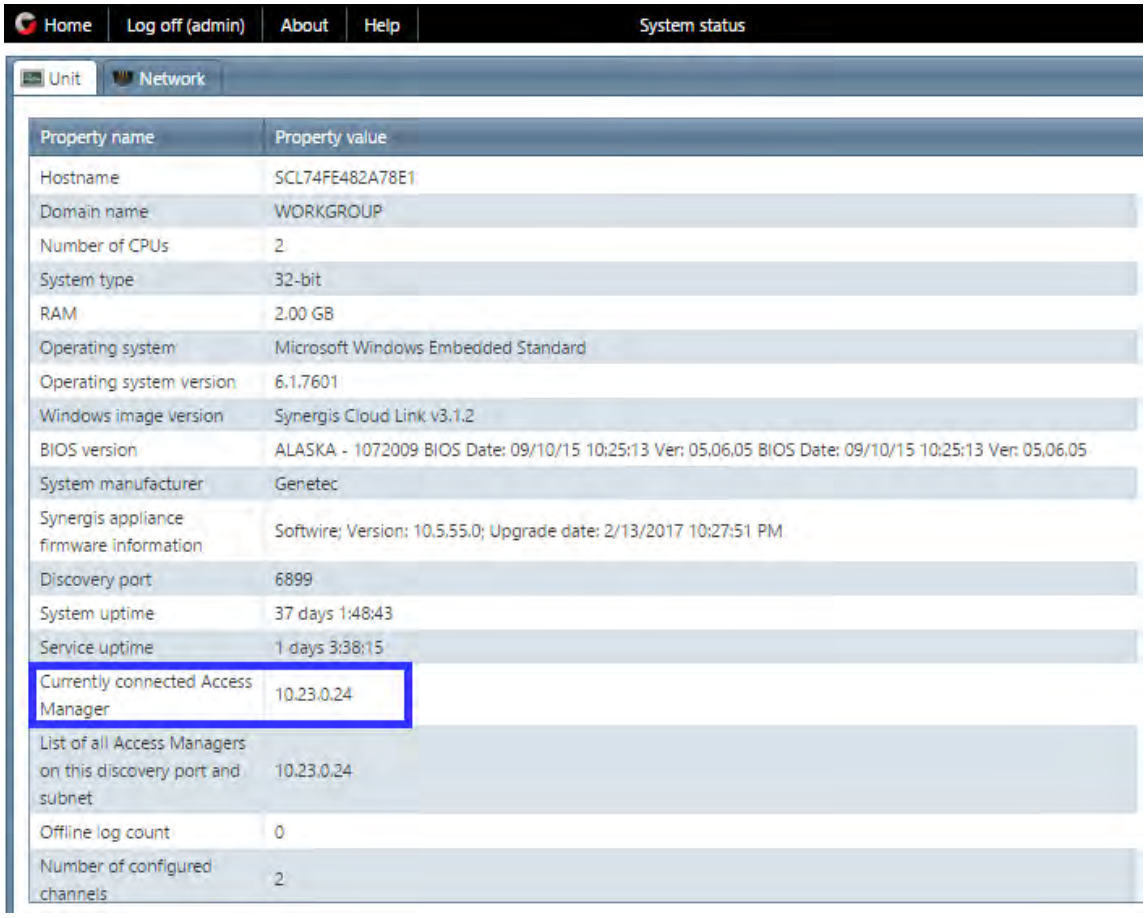
7.3.5 Whitelist your IP address (Advanced level)

Make sure the only IP address listed in **Accepted Access Manager connections** is the IP address of the Access Manager associated with the Synergis™ appliance you are connected to.



Access Manager settings in the Synergis™ Appliance Portal

This information can also be viewed on the *System Status* page of the Synergis™ Appliance Portal.



Property name	Property value
Hostname	SCL74FE482A78E1
Domain name	WORKGROUP
Number of CPUs	2
System type	32-bit
RAM	2.00 GB
Operating system	Microsoft Windows Embedded Standard
Operating system version	6.1.7601
Windows image version	Synergis Cloud Link v3.1.2
BIOS version	ALASKA - 1072009 BIOS Date: 09/10/15 10:25:13 Ver: 05.06.05 BIOS Date: 09/10/15 10:25:13 Ver: 05.06.05
System manufacturer	Genetec
Synergis appliance firmware information	Softwire; Version: 10.5.55.0; Upgrade date: 2/13/2017 10:27:51 PM
Discovery port	6899
System uptime	37 days 1:48:43
Service uptime	1 days 3:38:15
Currently connected Access Manager	10.23.0.24
List of all Access Managers on this discovery port and subnet	10.23.0.24
Offline log count	0
Number of configured channels	2

System status page in the Synergis™ Appliance Portal

8 Logging

8.1 Activate logging in the Activity trails for every event related to security (Basic level, Advanced level)

This includes but is not limited to: connected to remote Security Desk, disconnected from remote Security Desk, user logged off, user logged on, user logon failed, camera blocked, and video file deleted.

9 Web Client

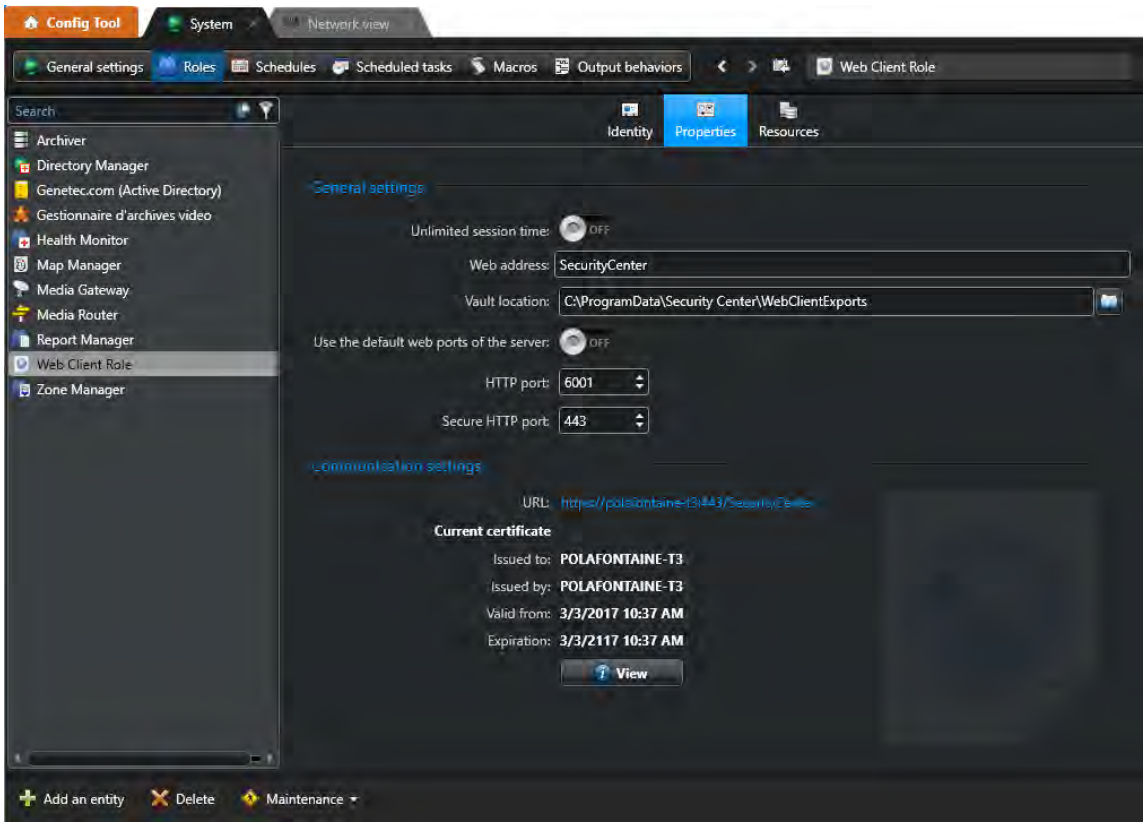
Beginning in Security Center 5.6, a completely redesigned Web Client has been introduced. This new Web Client is no longer dependent on the Mobile Server, and is now configured as a role directly in Security Center.

9.1 Turn off the Unlimited session time option (Basic level, Advanced user)

You can disable **Unlimited session time** to automatically log off users after 12 hours of inactivity.

To turn off Unlimited session time:

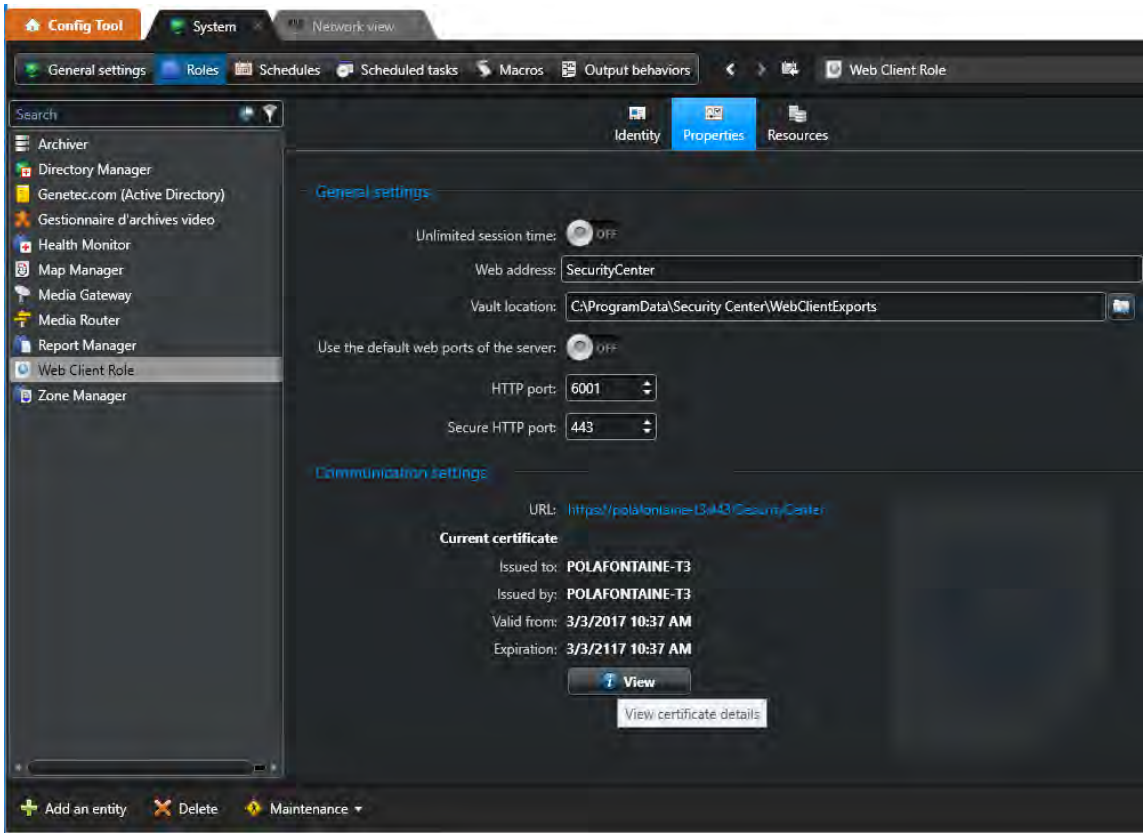
1. In Config Tool, open the *System* task.
2. Click the **Roles** view.
3. Select the *Web Client Role* page, and then click **Properties**.
4. In the *General settings* section, set **Unlimited session time** to **OFF**



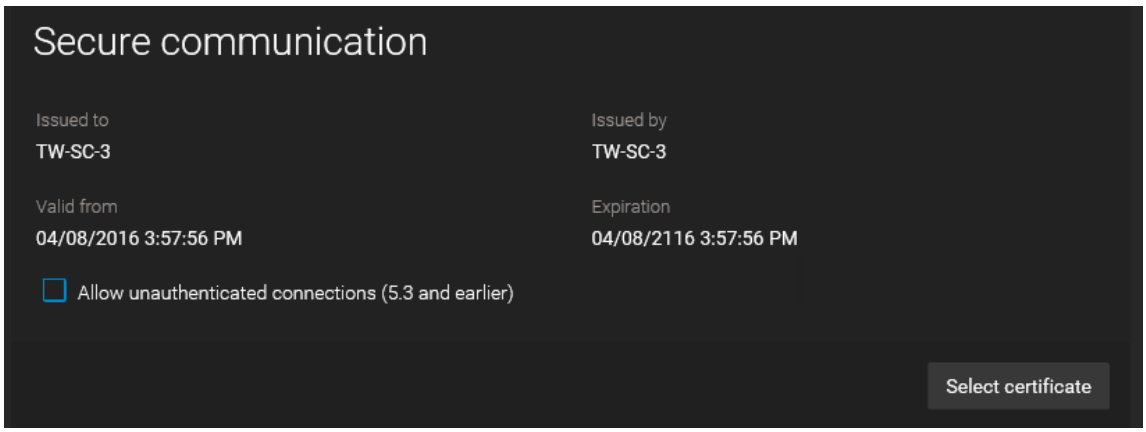
Web Client Role page in Config Tool

9.2 Install a valid certificate on the Mobile Server (Advanced user)

The Web Client 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 for a certificate signed by a trusted certificate authority. You can view the details of the Web Client role's certificate in Config Tool. To change the certificate, you must access Server Admin.



Certificate details on the *Web Client Role* page in Config Tool

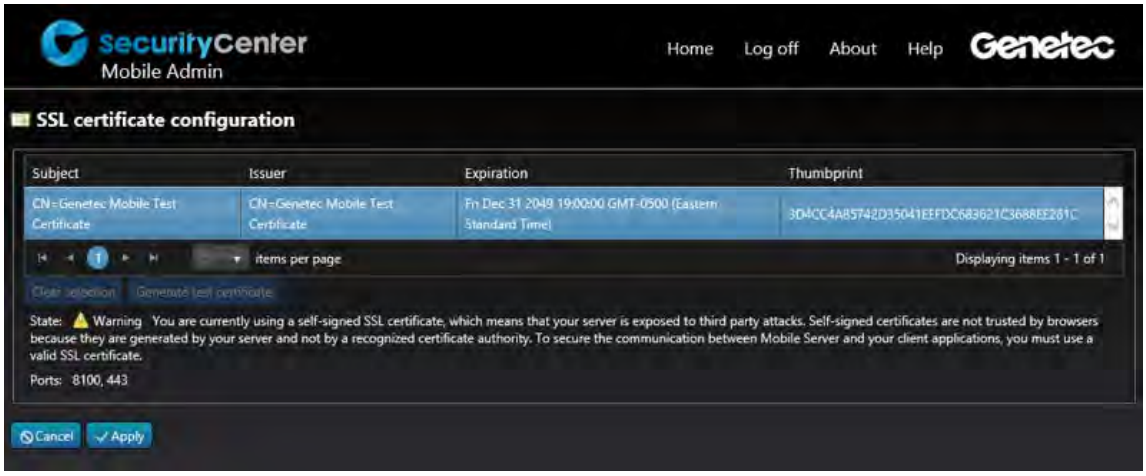


Certificate information in Server Admin

10 Security Center Mobile

10.1 Install a valid certificate on the Mobile Server (Advanced level)

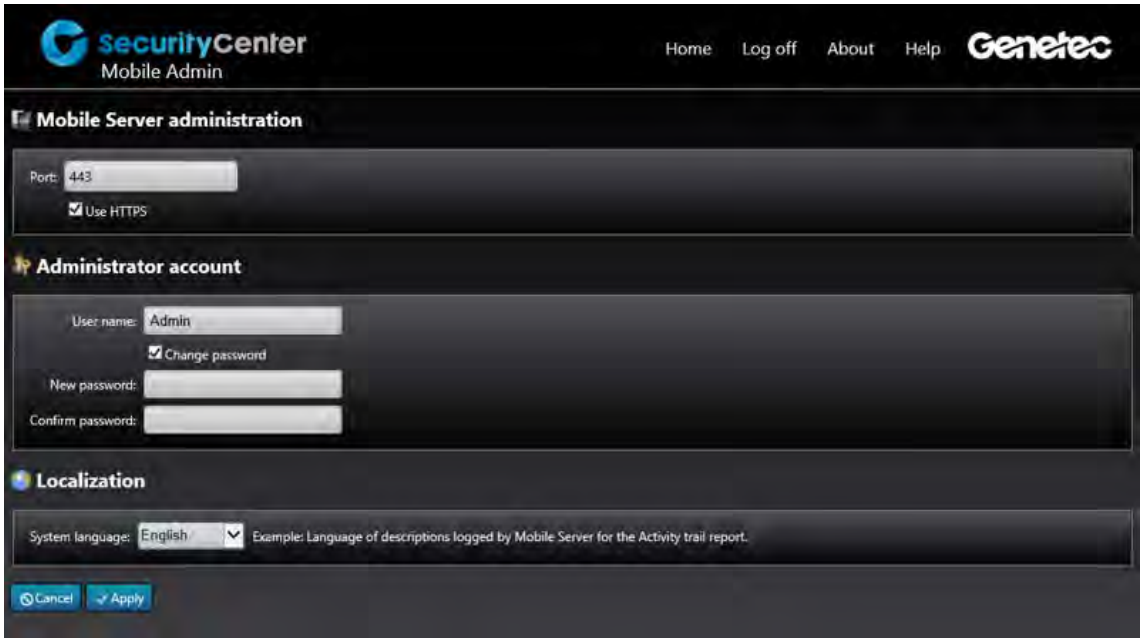
The Security Center Mobile Server generates and installs a self-signed certificate by default during installation. However, you should replace the self-signed certificate with a valid certificate. If you do not change the certificate, a message is displayed in Mobile Admin prompting you to act. For more information, refer to the chapter on encrypting communication between Mobile components in the *Security Center Mobile Installation and Administration Guide*.



SSL certificate configuration section in Mobile Admin

10.2 Make sure that HTTPS is used for communication between the Mobile Admin and Server (Basic level, Advanced level)

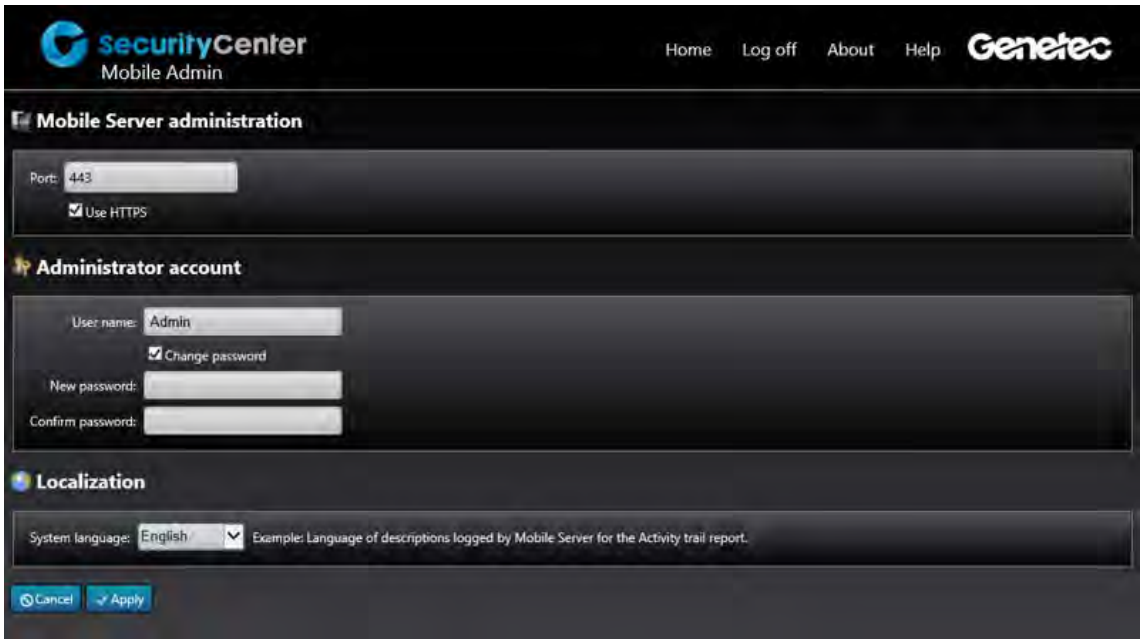
In Mobile Admin in the *Mobile Server administration* section, make sure that the **Use HTTPS** checkbox is selected (this is the default setting).



Mobile Server administrator panel in Mobile Admin

10.3 Select a long, unique, random password for the Mobile Admin user (Basic level, Advanced level)

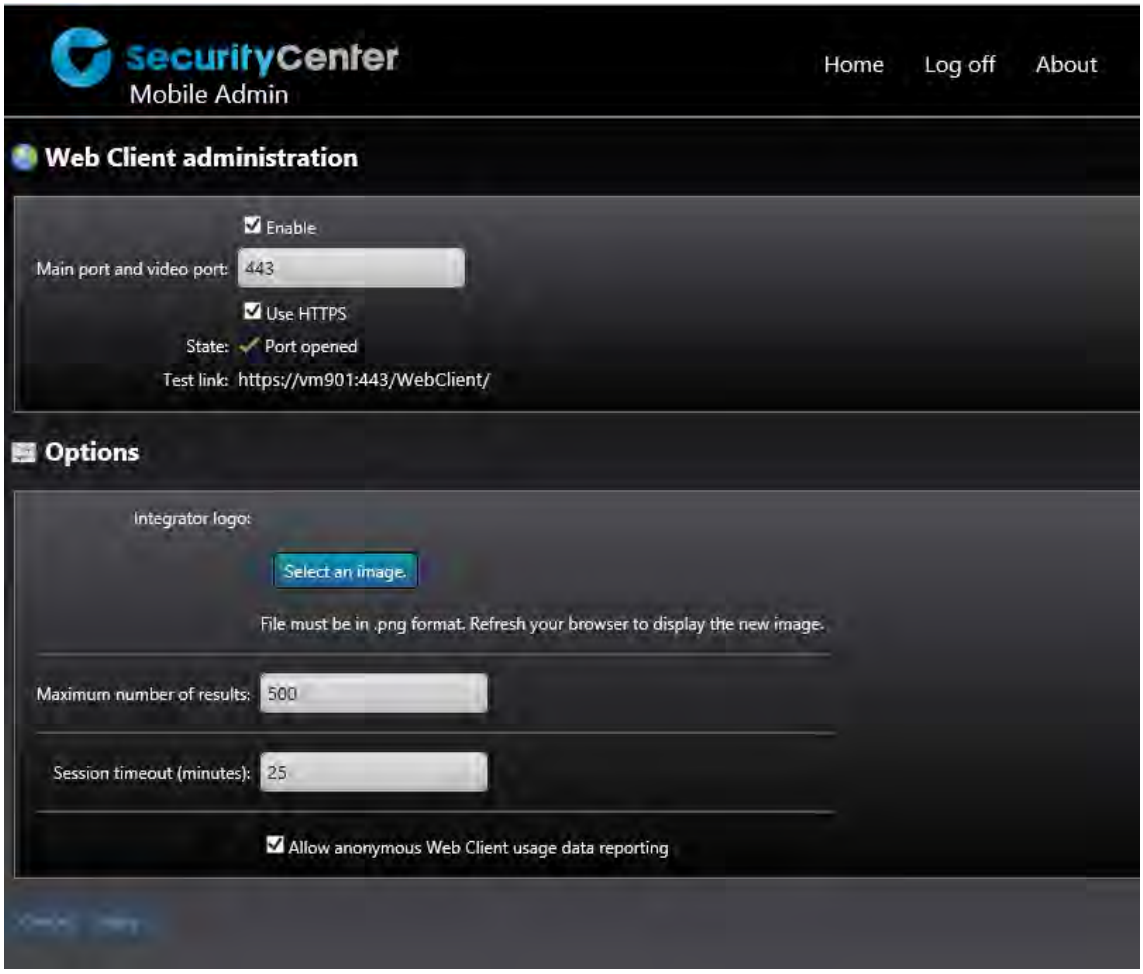
Choose a long, unique, random password for the Mobile Admin user account. See the OWASP Password length & complexity for best practices. The user account password can be configured in Mobile Admin in the *Administrator account* section.



Mobile Server administrator section in Mobile Admin

10.4 Make sure that HTTPS is used to communicate between the Mobile Server and Web Clients (Basic level, Advanced level)

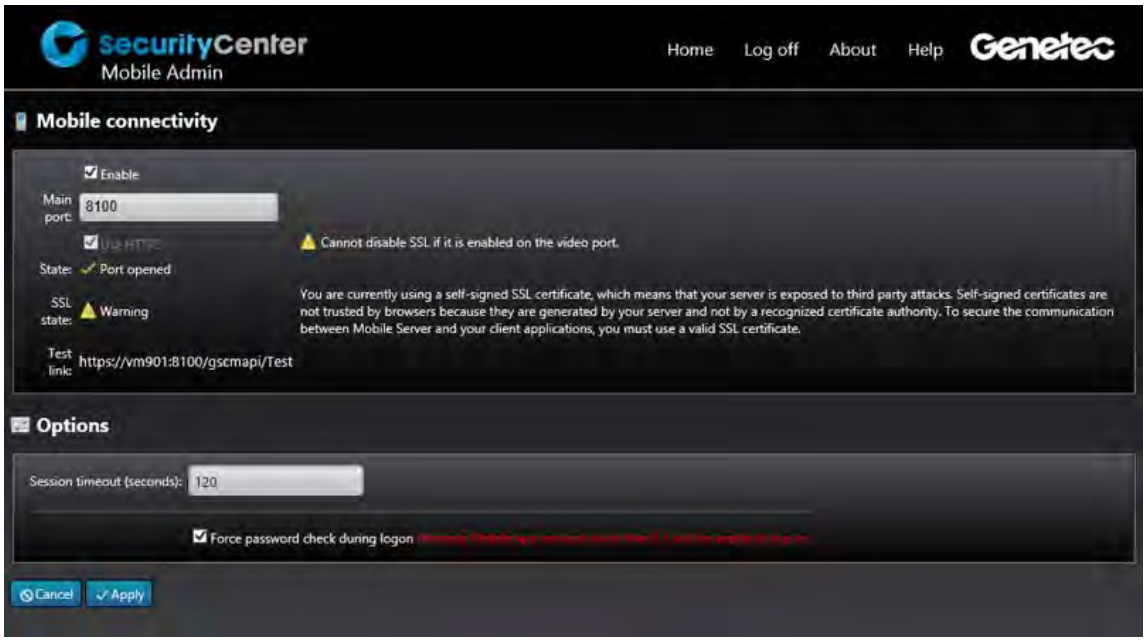
In Mobile Admin in the *Web Client administration* section, ensure that the **Use HTTPS** checkbox is selected (this is the default setting).



Web Client administration section of the Mobile Server

10.5 Make sure that HTTPS is used to communicate between the Mobile Server and the Mobile Apps (Basic level, Advanced level)

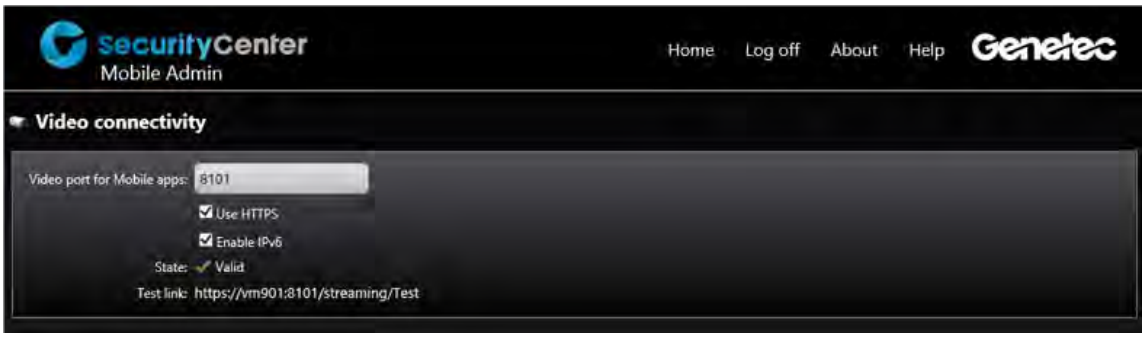
In Mobile Admin in the *Mobile connectivity* section, ensure that the **Use HTTPS** checkbox is selected (this is the default setting). This setting should also be activated on each Mobile App. For more information, refer to the *Security Center Mobile Installation and Administration Guide* for your device version.



Mobile connectivity section of the Mobile Server

10.6 Encrypt video streams from Mobile Server to Mobile Apps and Web Clients

You can encrypt video streams by HTTPS when going from the Mobile Server to the Mobile Apps and Web Client. To do this, navigate to the *Video connectivity* section in Mobile Admin, and select the **Use HTTPS** checkbox.



Video connectivity section of the Mobile Server

11 Database

11.1 Do not connect to the SQL Server with an account that has administrative privileges (Basic level, Advanced level)

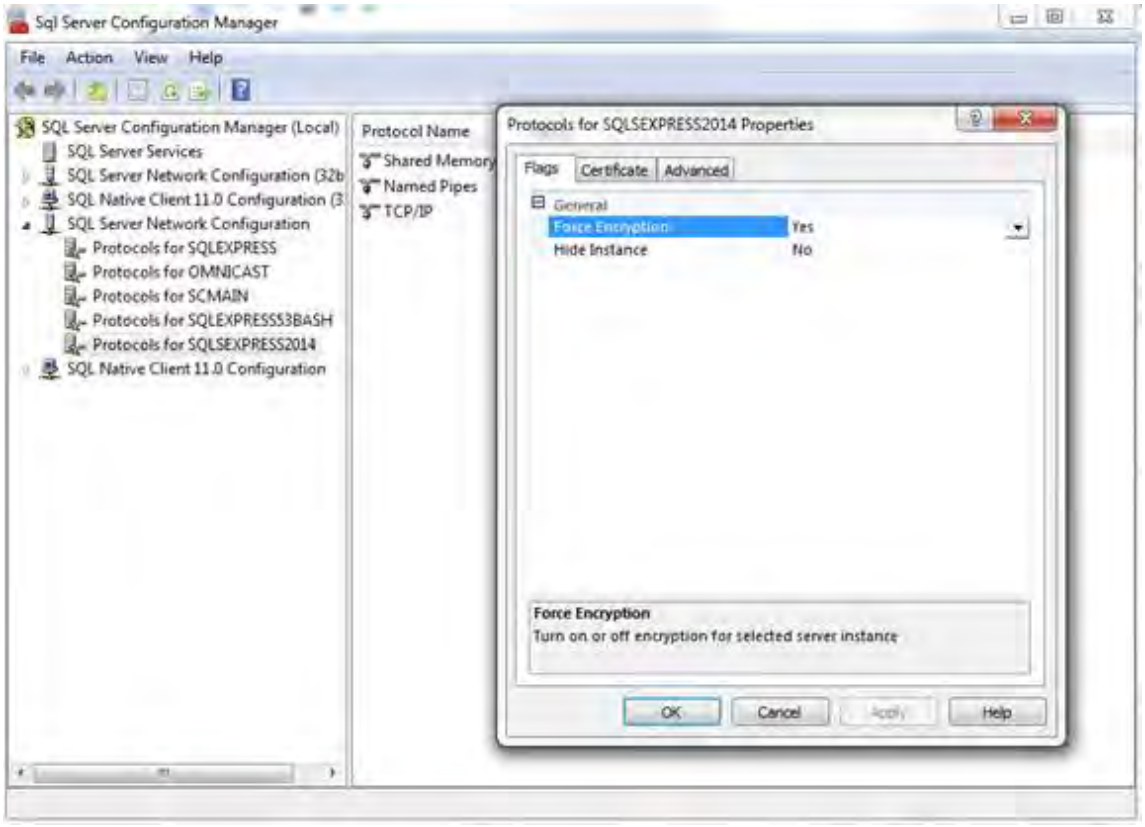
Security Center **does not** require the *sysadmin* server role on the database server. The specific permissions needed depend on the role. Refer to the table below for more information. Also, a Security Center Directory requires the *View Server State* permissions in order to work properly. This is mandatory when Directory failover is configured. We recommend that this permission be enabled at all times.

	Server Permissions		Database Permissions		
Database	`public`	`dbCreator`	`db_datareader`	`db_datawriter`	`db_owner`
Directory	X	X[1]			X[2]
Health Monitoring	X				X[3]
Media Router	X		X	X	
Archiver	X		X	X	
Auxiliary Archiver	X		X	X	
Access Manager	X				X[3]
LPR Manager	X				X[3]
Zone Manager	X				X[3]

[1] When using Directory failover with database backup & restore
[2] Because of dynamic creation of tables and columns
[3] Because of dynamic creation of tables

11.2 Use encrypted communication between the Databases and Genetec™ services (Basic level, Advanced level)

You can configure the SQL service to force the use of encryption for communication between the databases and Genetec™ services. This protects data while in transit. Note that this might impact performance.



Forcing encryption usage when communicating with SQL Server in the SQL Server Configuration Manager

11.3 Encrypting the database file (Advanced level)

The SQL server offers the option to use Transparent Data Encryption (TDE) to encrypt database data files. This protects data while at rest. Note that this might impact performance.

12 Windows

12.1 Run client applications without administrative privileges (Basic level, Advanced level)

You can run client applications (Security Desk and Config Tool) under a non-administrative account. This helps to reduce the damage caused by a compromised application.

12.2 Configure Windows securely (Basic level, Advanced level)

Microsoft provides ready-to-deploy security policies tailored to each of their operating system versions through the Security Compliance Manager (SCM). For more information on the SCM, visit the following page:

- Security Compliance Manager (SCM)

Microsoft also provides recommendations through their security baseline. For more information, see 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

12.3 Use Microsoft EMET (Advanced level)

You can apply the defense in depth strategy of making it more difficult for an attacker to exploit a vulnerability, by using the Microsoft Enhanced Mitigation Experience Toolkit (EMET) on machines that are running Security Center. EMET anticipates the most common techniques used by attackers to exploit vulnerabilities in computer systems, and helps protect by diverting, terminating, blocking, and invalidating these actions and techniques. Note that this can cause compatibility issues with your system. For more information, refer to the Microsoft documentation: https://technet.microsoft.com/en-us/security/jj653751

12.4 Keep system time up-to-date (Advanced level)

Keep system time up-to-date with NTP time synchronization. This is considered best practice and helps correlate attacker actions when reviewing logs. This should be done on all machines running Genetec™ software.

You can also force the usage of Active Directory on all client machines and servers running Security Center. This enforces strict time synchronization between all members.