Streamvault™ Appliance User Guide

Click here for the most recent version of this document.

Document last updated: April 15, 2025

Legal notices

Document information

Document title: Streamvault™ Appliance User Guide

Original document number: EN.803.003

Document number: EN.803.003

Document update date: April 15, 2025

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

About this guide

This guide explains how to set up and configure your Streamvault appliance to work with Security Center access control and video surveillance using the current SV Control Panel version. This guide supplements the Security Center Administrator Guide and the Synergis™ Appliance Configuration Guide.

This guide is written for the integrator who performs the initial setup of the SV appliance. It is assumed that you are familiar with the terminology and concepts used in Security Center.

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

1

Introduction to your Streamvault appliance

This section includes the following topics:

Getting started with your Streamvault appliance

You can deploy your Streamvault™ appliance with Security Center by following a sequence of steps.

Deployment overview

Step	Task	Where to find more information
Understand prerequisites and key issues before deploying		
1	Open the required network ports to connect the core systems in Security Center and modules of Streamvault. Connect the peripherals, such as monitor, keyboard, analog encoder card, and devices to inputs and outputs. Connect the appliance to your network.	• Default ports used by Streamvault on page 4. • Connecting Streamvault appliance components on page 8. • Genetec analog encoder cards on page 8. • Disabling camera inputs on encoder cards on a Streamvault appliance on page 9. • Alarm inputs and outputs of a Streamvault appliance on page 10.
2	Before deploying your appliance, learn about the contents of your image version.	• Contents of each Streamvault image release.
3	Log on to Windows as Admin using the password that is printed on your appliance, then change the password.	• Logging on to a Streamvault appliance on page 14.
Complete the setup wizards		
4	Complete the *Streamvault Control Panel setup* wizard. **NOTE:** Remote desktop is disabled by default. To enable remote desktop, turn on the **Remote Desktop service** setting on the *Security* page of the SV Control Panel.	• Setting up your appliance in the SV Control Panel on page 19. • Allowing Remote Desktop connections to a Streamvault appliance on page 76.
5	Activate your Security Center license. • If the appliance is connected to the internet, activate your license using the *Streamvault Control Panel activation* wizard. • If the appliance isn't connected to the internet, activate your license manually from Server Admin.	• Activating your Security Center license on an appliance on page 22. • Activating a license manually from Server Admin on page 24.
6	Activate the System Availability Monitor.	• Activating System Availability Monitor on page 26.
7	Configure the Genetec™ Update Service so that you can get the latest version of Security Center and the SV Control Panel. If there are updates, install them.	• Configuring Genetec Update Service.
8	If the SV Control Panel indicates that there are more updates available, install them now.	• About updating SV software in the SV Control Panel on page 7.

Step	Task	Where to find more information
9	For an Archiver appliance, create the number of Archiver roles that you need to support the number of cameras and the total network bandwidth planned for your deployment.	• For SV-1000E, SV-2000E, SV-4000E series: Adding Archiver roles in the SV Control Panel on page 39. • For SV-7000EX and for All-in-one: Adding partitions and Archiver roles manually on page 40.
10	Log on to Config Tool and configure your Security Center video and access control features.	• Enabling Security Center video and access control features on page 27. • Configuring unit enrollment settings on page 29.
11	Back up the Security Center configuration.	• Backing up your Directory database on page 36.

Default ports used by Streamvault

The required network ports must be opened to allow the following Streamvault™ components to work correctly.

Streamvault Maintenance plugin required ports

The following port must be opened on an external firewall for inbound traffic so that the Streamvault™ Maintenance plugin can communicate with the Streamvault hardware. This requirement applies only if the following three conditions are met:

- The internal OS to iDRAC Pass-through connection is disabled
- The iDRAC is using a dedicated LAN port
- There's a firewall between the iDRAC network and the host network

In every other situation, this requirement can be ignored.

Module	Inbound port	Port usage
Streamvault hardware monitor	65116	Used for HTTPS communication between Security Center and the Streamvault hardware's iDRAC baseboard management controller through the network.

SV Control Panel required ports

The outbound traffic ports listed below must be opened to allow the Streamvault Control Panel components to connect to the Genetec™ cloud services.

Outbound port	Port usage	Destination URL
TCP 443	HTTPS communication with Genetec backup services	svbackupservices.genetec.com genetecbackupservice.blob.core.windows.net

CylancePROTECT required ports

The outbound traffic ports listed below must be opened to allow the CylancePROTECT desktop agent to communicate with the Genetec management console and receive agent updates.

Outbound port	Port usage	Destination URL
TCP 443	HTTPS communication in North America	cement.cylance.com data.cylance.com protect.cylance.com update.cylance.com api.cylance.com download.cylance.com venueapi.cylance.com

Outbound port	Port usage	Destination URL
TCP 443	HTTPS communication in Asia-Pacific Northeast	cement-apne1.cylance.com data-apne1.cylance.com protect-apne1.cylance.com update-apne1.cylance.com api.cylance.com download.cylance.com venueapi-apne1.cylance.com
TCP 443	HTTPS communication in Asia-Pacific Southeast	cement-au.cylance.com cement-apse2.cylance.com data-au.cylance.com protect-au.cylance.com update-au.cylance.com api.cylance.com download.cylance.com venueapi-au.cylance.com
TCP 443	HTTPS communication in Central Europe	cement-euc1.cylance.com data-euc1.cylance.com protect-euc1.cylance.com update-euc1.cylance.com api.cylance.com download.cylance.com venueapi-euc1.cylance.com
TCP 443	HTTPS communication in South America	cement-sae1.cylance.com data-sae1.cylance.com protect-sae1.cylance.com update-sae1.cylance.com api.cylance.com download.cylance.com venueapi-sae1.cylance.com

Outbound port	Port usage	Destination URL
TCP 443	HTTPS communication in GovCloud	cement.us.cylance.com data.us.cylance.com protect.us.cylance.com update.us.cylance.com api.us.cylance.com download.cylance.com download.us.cylance.com venueapi.us.cylance.com
TCP 443	HTTPS communication to activate Cylance after reinstallation	svservices.genetec.com

NOTE: If you don't want to open the above outbound connections, CylancePROTECT can be switched to disconnected mode. In disconnected mode, CylancePROTECT receives agent updates from the Genetec™ Update Service (GUS).

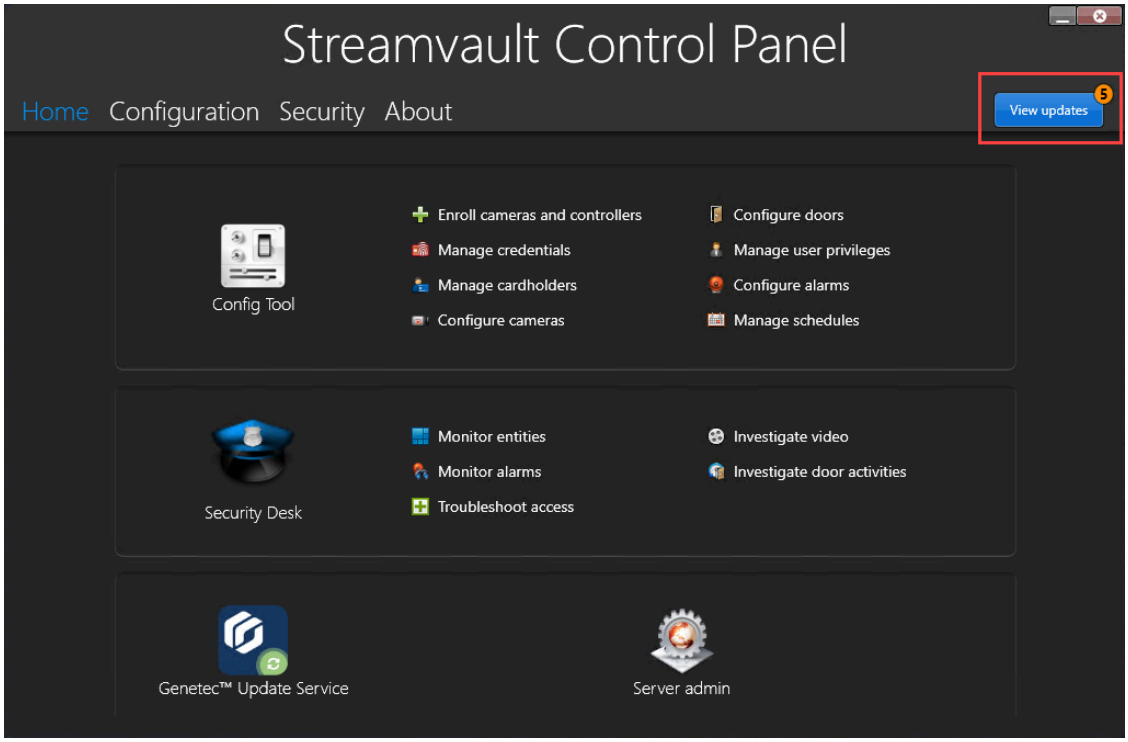
For more information about the modes in which the Streamvault appliance communicates with Genetec management services, see Security page of the SV Control Panel on page 66.

About updating SV software in the SV Control Panel

The Genetec™ Update Service (GUS) is integrated into the SV Control Panel to help ensure that the software components on your appliance are up to date.

When updates are available, the **View updates** button is displayed with a badge indicating how many updates are available. Clicking on the **View updates** button launches GUS in a browser.

NOTE: The color of the badge varies depending on the importance of the updates. An orange badge indicates recommended updates, and a red badge indicates critical updates.



The main features of GUS are as follows:

- Update your Genetec™ products when a new release becomes available.
- Check for updates at regular intervals.
- Configure updates to be downloaded in the background, but you still need to manually install.
- View when the last check for updates occurred.
- Automatically refreshes the license in the background to ensure it's valid and the expiry date is updated.
- Enable various features such as the Genetec Improvement Program.
- Reviews your firmware and recommends upgrades or notifies you of vulnerabilities.

For more information about how to use GUS, refer to the Genetec™ Update Service User Guide on the TechDoc Hub.

Connecting Streamvault appliance components

To prepare your Streamvault™ appliance for use, you must connect the required peripherals (monitor, keyboard, and mouse), the optional peripherals, the network, and a power source.

Before you begin

Clear space around the power button. To prevent accidentally turning off the appliance, ensure that nothing touches or is too close to the power button.

Procedure

1 Connect the display monitor cable to a supported video input: VGA, HDMI, or DisplayPort connector.

At least one monitor must be connected to the appliance. You can connect up to three monitors to the same appliance.

2 Plug the monitor into an AC outlet and power on the monitor.

3 Connect the keyboard and mouse to an available USB port.

4 (Optional) Connect the optional peripherals:

- Speakers
- Analog cameras
- Alarm inputs and outputs

5 Connect an Ethernet cable to the Ethernet port on the appliance. Connect the other end of the cable to the IP network RJ-45 jack.

6 For Streamvault™ SV-100E appliances, insert the DC plug into the appliance's 19.5V input jack and the other end into the power supply brick. Plug the cord from the brick to an electrical outlet.

7 To power on the Streamvault appliance, press the power button.

After you finish

Log on to your Streamvault appliance.

Genetec analog encoder cards

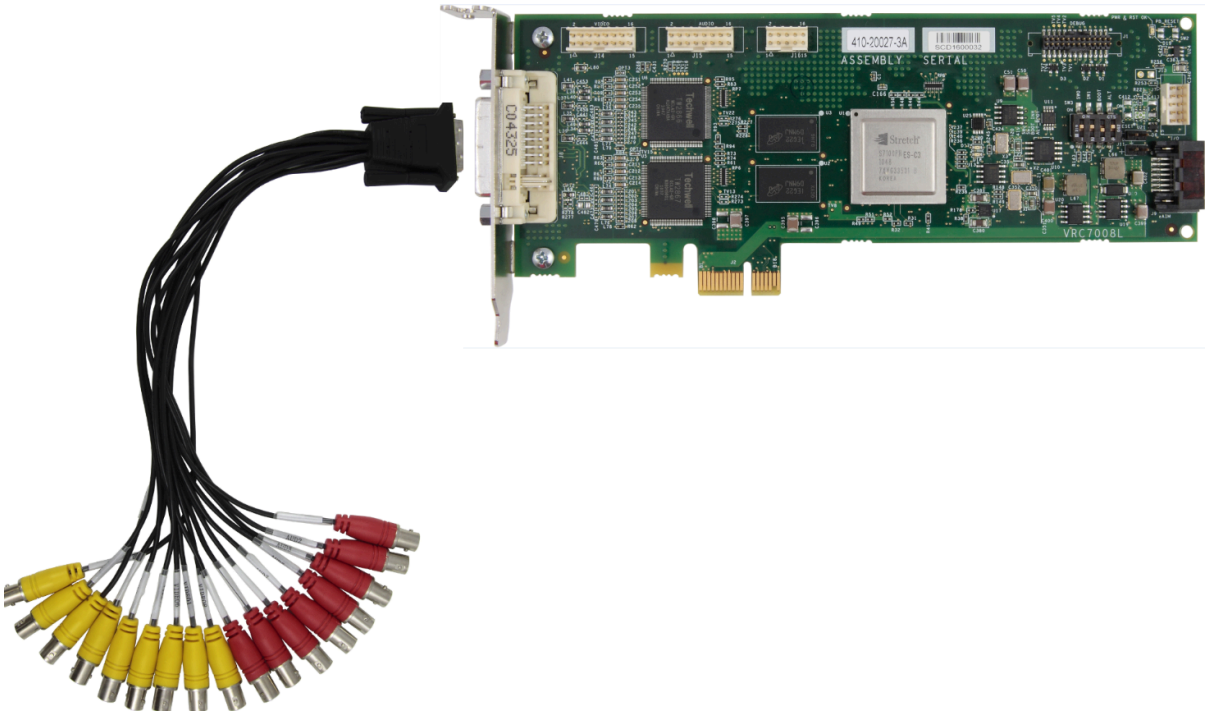
If you're using a Streamvault appliance to implement a video management system with analog cameras, you must connect the cameras to the Genetec™ analog encoder card on the appliance.

Analog encoder card specifications

The following specifications apply to Streamvault appliances that include the analog video card:

- 8 or 16 analog video inputs, depending on which card is installed
- 4CIF max video resolution
- Maximum frame rate: 30 FPS
- Supports H.264 compression format

Limitation: For the analog encoder card to be able to record, your Streamvault appliance must have a network connection. If a network connection is unavailable, you must configure a loopback interface so that the encoder card can function properly.



About connecting analog cameras

If your Streamvault appliance includes the Genetec analog encoder card, it's shipped with a breakout cable with BNC connectors. The BNC connectors are used to connect the analog cameras directly to the built-in encoder card.

About adding analog cameras in Security Center

To add analog cameras in Security Center, you must use the Unit enrollment tool. For more information, see About the Unit enrollment tool.

Consider the following when adding analog cameras:

- You can't add analog cameras in Security Center using the *Manual add* method. Use the Unit enrollment tool.
- To discover new units and use the Unit enrollment tool, you must connect to Config Tool locally.
- When selecting the camera's manufacturer in the Unit enrollment tool, you can find all the analog cameras listed under the *Genetec encoder card* manufacturer.

Disabling camera inputs on encoder cards on a Streamvault appliance

To upgrade a camera connection license from analog to IP, you must disable the camera inputs on the encoder card.

Procedure

1 From the Config Tool homepage, click the *About* tab.

2 Click the **Omnicast**™ tab and verify the number of cameras listed next to *Number of cameras and analog monitors*.

For example: 16 / 16.

3 Open the *Video* task.

4 From the entity tree, click the video unit that corresponds to the encoder card.

5 Click the **Peripherals** tab and select the cameras you need to disable.
You can select multiple cameras by pressing Ctrl and clicking the cameras.

6 At the bottom of the *Peripherals* page, click the red circle ( ) to disable the cameras, and then click **Apply**.
The disabled cameras are grayed-out and a red dot is shown to the left of each disabled camera in the list.

7 On the *About* page, verify that the number of cameras is accurate.
You might need to restart Config Tool to refresh the number of cameras.
NOTE: If a camera that you disabled recorded video, the camera is shown in the entity tree in the Security Desk *Monitoring* task. You can view playback from that camera.

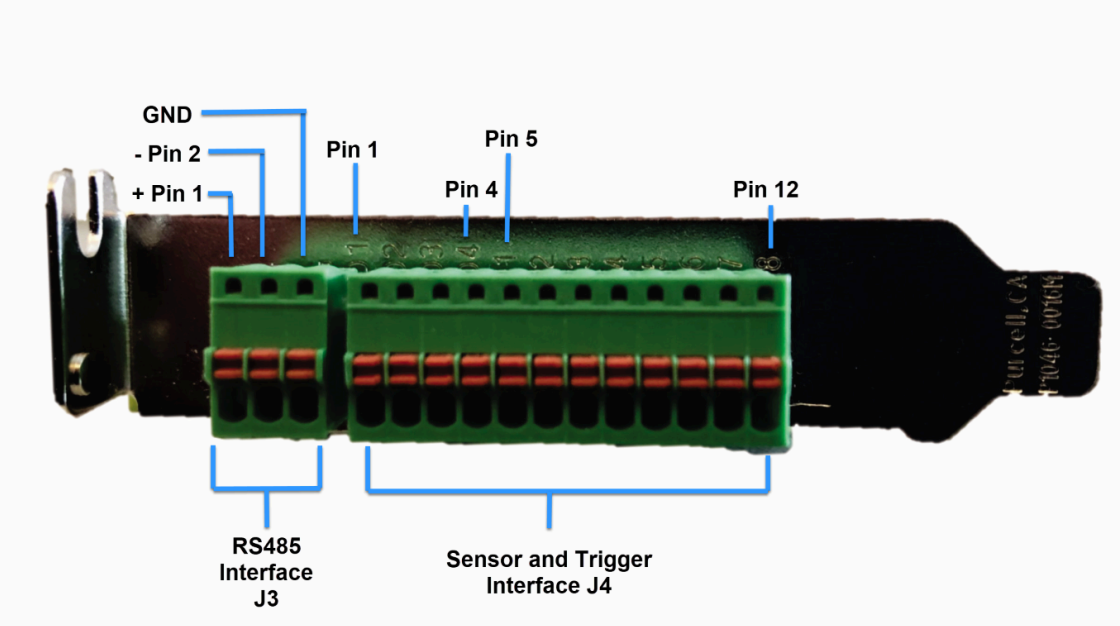
Alarm inputs and outputs of a Streamvault appliance

If you're using a Streamvault appliance to implement an access control system, you can use the I/O card to connect hardware alarm inputs directly to the appliance, and then control its outputs using event-to-actions in Security Center.

I/O card specifications

The following specifications apply to Streamvault models that include the I/O card:

- 4 trigger outputs
- 8 alarm inputs
- RS-485 communications port



About connecting I/O inputs

You can connect the input and output wires from hardware devices directly to the I/O card on the back of the Streamvault appliance. The wires should be inserted using a small flat-head screwdriver to push in the tension clamps on the connector.

About creating event-to-actions

For information on how to create event-to-actions for Streamvault, see Creating event-to-actions on the TechDoc Hub.

About Streamvault user accounts

There are two types of Streamvault™ user accounts: local administrator and local non-administrator. Depending on which type of user account you log on to the SV Control Panel with, you see only those features that are relevant to you.

Local administrator

The local administrator (Admin) user account is created by default. A person logged on as Admin has full administrative rights to the SV Control Panel. The Admin can configure all system- and security-related settings in the SV Control Panel, and can create non-administrator user accounts.

Local non-administrator

The default non-administrator local user account for All-in-one appliances and workstations is the Operator account. A person logged on as Operator has restricted access to SV Control Panel features. The Operator can launch Config Tool and Security Desk, view system and licensing information, and access product documentation.

A person logged on as Admin can create other non-administrator accounts, which also have limited access to the SV Control Panel.

NOTE: It's possible to remove the default access restrictions placed on all non-administrator user accounts. For information on how to do so, see Removing restrictions from non-administrator user accounts on page 99.

Related Topics

Login information for default user accounts on a Streamvault appliance on page 12

Login information for default user accounts on a Streamvault appliance

The first time your Streamvault appliance starts, the Windows Admin and Operator user accounts are created. These accounts have different access rights, and default passwords. Server Admin also has a default password.

The following default passwords are for initial login. During setup, you create your own password for Config Tool and Security Desk.

Username	Default password	Access granted to	Access denied for
Admin	admin	Full system access: • Windows: all system and administrative features • Security Center • SV Control Panel	Not applicable

Username	Default password	Access granted to	Access denied for
Operator	operator	• Recycle Bin • Libraries • My Computer • C: drive • SV Control Panel homepage, Configuration page Regional settings only, About page • Server Admin: requires Admin password for full rights	• Windows: shut down and restart • System settings • Video partition
Not applicable	genetecfactory	Server Admin	**NOTE:** This option is unavailable for Workstation appliances.

To change your Windows user account, client application, or Server Admin password, log on to the SV Control Panel using your Windows Admin user account. On the *Security* page, in the *Credentials* section, you can manage all your passwords.

NOTE: The Operator account isn't created with a template. If you create a new user account, they won't have the same restrictions by default.

Security Center Server Admin

- Only Admin users can log on to Server Admin.
- To log on from your local machine, click the **Server Admin** shortcut on your desktop.
- To log on to Server Admin remotely, you need the server's DNS name or IP address, the web server port, and the server password. When you enter the default password, you're prompted to change it.

IMPORTANT: To ensure the security of your system, immediately change all default passwords. Use industry best practices for creating strong passwords.

Related Topics

About Streamvault user accounts on page 12

Logging on to a Streamvault appliance

The first time you start your Streamvault™ appliance, you're prompted to change the default Admin password. Also change the default Operator password. You can then log on as either an Operator or Admin user.

Before you begin

Learn which access rights the Operator and Admin accounts have.

What you should know

Log on as an Admin user to configure your appliance in the SV Control Panel.

IMPORTANT: Passwords must meet the following requirements:

- Minimum of 14 characters

  The minimum length is 10 characters for appliances with image versions that don't have the Streamvault service. For information about which appliances have the Streamvault service and which don't, see Appliances with hardening management capabilities on page 16.
- At least three characters from the following four categories:
  - Uppercase letters
  - Lowercase letters
  - Base 10 digits (0-9)
  - Non-alphanumeric characters (such as $, %, !)

Procedure

1. Power on the appliance.
2. Log on using the Admin username and default password that are printed on the appliance.
3. Enter a new Admin password.

   You're logged on as an Admin user.

   NOTE: Some models have only the Admin account by default.
4. Log off, and then log on using the Operator username and default password that are printed on the appliance.
5. Enter a new Operator password.

   You're logged in as an Operator user.
6. Continue the Operator session, or log out and log back in as an Admin user.

After you finish

Launch the initial setup of your appliance.

About the Streamvault service

The Streamvault service is a Windows service that enables users to configure a Streamvault™ appliance, such as applying hardening profiles.

The Streamvault service can apply the following hardening profiles on appliances:

- Microsoft security baselines
- Microsoft security baselines with the Center for Internet Security (CIS) Level 1 profile
- Microsoft security baselines with the CIS Level 2 profile
- Microsoft security baselines with the Security Technical Implementation Guide (STIG) profile

See About Streamvault hardening on page 16 for more information about the hardening profiles.

When an Admin user selects a hardening profile in the SV Control Panel, the Streamvault service applies the profile to the appliance.

Updates for the Streamvault service are periodically available and can be applied through the Genetec™ Update Service (GUS) or Genetec Technical Assistance Portal (GTAP). When an update is available, a notification appears in the SV Control Panel. Applying updates is optional but recommended to access new versions of the hardening profiles.

About Streamvault hardening

Hardening enhances the security of your Streamvault™ appliance by applying a specific set of security settings.

When you harden your appliance, you're optimizing it for more security, but potentially at the expense of some usability or performance. How much you harden your appliance depends on your threat model and the sensitivity of your information.

Hardening is applied on the *Security* page of the SV Control Panel. There are four predefined hardening profiles to choose from.

By default, all appliances are shipped with the Microsoft with CIS Level 2 hardening profile applied.

Hardening profile	Description
Microsoft (only)	This hardening profile applies Microsoft security baselines to your system. Microsoft security baselines are a group of Microsoft-recommended configuration settings that are based on feedback from Microsoft security engineering teams, product groups, partners, and customers. The Microsoft baselines that are deployed on Streamvault appliances are the Windows baseline and the Microsoft Edge baseline.
Microsoft with CIS Level 1	This hardening profile applies Microsoft security baselines and the Center for Internet Security (CIS) Level 1 (CIS L1) profile to your system. The CIS L1 provides essential security requirements that can be implemented on any system with little or no performance impact or reduced functionality.
Microsoft with CIS Level 2	This hardening profile applies Microsoft security baselines and the CIS L1 and Level 2 (L2) profiles to your system. The CIS L2 profile offers the highest level of security and is intended for organizations where security is of utmost importance. The strict security that this hardening profile brings can reduce system functionality and make remote server management more difficult.
Microsoft with STIG	This hardening profile applies Microsoft security baselines and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) to your system. DISA STIGs are based on National Institute of Standards and Technology (NIST) standards and provide advanced security protection for Windows systems for the U.S. Department of Defense.

NOTE: Hardening profiles are available only on appliances that have the *Streamvault service*. For more information, see About the Streamvault service on page 15.

Appliances with hardening management capabilities

Only those appliances with the Streamvault™ service have hardening management capabilities. The appliance type and image determine whether the Streamvault service is available.

The table below outlines which appliances have the Streamvault service and which ones don't.

Appliance type	Image versions with the Streamvault service	Image versions without the Streamvault service
All-in-one	• 11.2024.2	• 16 • 17 • 18 • 19
SVW	• 11.2024.2	• 0010.4 • 0011.2 • 0012.2 • 0013.2
SVA	• 11.2024.2	• 0010.4 • 0011.2 • 0012.2 • 0013.2
SVR	• 10.2021.2 • 11.2024.2	• 0012.2.X
Other Streamvault appliances	• WS.2022.1	• 2016.1.B • 2016.1.C • 2019.1 • 2019.4.C • 2022.1.C

NOTE: For information on finding the image version of your appliance, see Finding the system ID and image version of a Streamvault appliance on page 74.

2

Getting started with SV Control Panel

Getting started introduces the SV Control Panel and provides information about how to set up your Streamvault appliance.

This section includes the following topics:

About the SV Control Panel

The SV Control Panel is a user interface application that you can use to configure your Streamvault™ appliance to work with Security Center access control and video surveillance.

CAUTION: Configuration changes that you make in the SV Control Panel will overwrite configuration changes made outside of the SV Control Panel, including custom Windows settings.

The SV Control Panel can be run in the following ways:

- Expansion mode for setups running on an expansion server.
- Client mode for setups running on Workstation appliances.
- Directory mode for setups running on the primary server.

The SV Control Panel includes the following features:

- *Streamvault Control Panel setup* wizard to help you set up your appliance quickly.
- *Streamvault Control Panel activation* wizard to help you activate your appliance.
- *Security Center installer assistant* that you can use to configure Security Center.
- *Streamvault Control Panel Backup* and *Streamvault Control Panel Restore* wizards to help you create backups of your Directory database and configurations and restore these files to your system if necessary.
- The Genetec™ Update Service (GUS) that regularly checks for software updates.
- Shortcuts to commonly used tasks in Config Tool and Security Desk.
- Links to the Genetec Technical Assistance Portal (GTAP) and product documentation.
- The option to choose the operation mode for the Cylance antivirus software provided with your Streamvault™ appliance. The options are listed on the *Security* configuration page.
- The ability to create more Archiver roles and partitions for setups on expansion servers.

NOTE: This guide is applicable to SV Control Panel version 3.0, which you can download from GTAP.

SV Control Panel version 3.0 is compatible with appliances that don't have the Streamvault service. However, these appliances won't have access to the hardening profiles.

Setting up your appliance in the SV Control Panel

The first time you log on to your Streamvault™ appliance, the SV Control Panel opens the *Streamvault Control Panel setup* wizard to guide you through the initial setup.

Before you begin

Connect the appliance to the internet.

What you should know

- Settings applied in the wizard can be changed later on the *Configuration* page of the SV Control Panel.
- For an Archiver, Analytics, Workstation, or any other appliance that is a Security Center expansion server, you aren’t prompted to change any user passwords.

Procedure

1 Start your appliance.

The SV Control Panel starts with the *Streamvault Control Panel setup* wizard open.

NOTE: The SV Control Panel only opens automatically the first time that the appliance starts. In subsequent restarts, users must log on using their Admin credentials and start the SV Control Panel.

2 On the *Introduction* page, click **Next**.

3 On the *Network* page, configure the IP connection settings:

a) If you use DHCP to obtain an IP automatically (default) and the IP address is missing, click **Refresh** ( ) to get a new IP address. Then click **Retry**.

b) If the **Status** field displays something other than "Connected to the internet", click **Retry**.

c) When the **Status** field displays "Connected to internet", click **Next**.

4 On the *Computer setup* page, complete the fields in the *General information* and *Regional settings* sections.

5 To change the user interface to a different language:

a) From **Product language**, choose your language.

b) Restart the SV Control Panel.

c) When the *Streamvault Control Panel setup* wizard reopens, click **Next** on the *Computer setup* page.

6 On the *Configure CylancePROTECT* page, choose a communication mode:

- **Online (recommended):** When online, the CylancePROTECT Agent communicates with Genetec to report new threats, update its agent, and send data to help improve its mathematical models. This option offers the highest level of protection.
- **Disconnected:** The disconnected mode is for an appliance without an internet connection. In this mode, CylancePROTECT cannot connect or send information to Genetec management services in the cloud. Your appliance is protected against most threats. Maintenance and updates are available through the Genetec™ Update Service (GUS).
- **Turn off:** Select this mode to permanently uninstall CylancePROTECT from your appliance. Your appliance will use Microsoft Defender for threat protection and detection. We do not recommend turning off CylancePROTECT if the appliance cannot receive virus definition updates for Microsoft Defender.

7 Click **Enable quarantine management** to add extra capabilities to the Cylance icon in the taskbar, including the **Delete Quarantined** option to delete files that Cylance has quarantined.

8 On the *Credentials* page, click **Modify password** to configure passwords for the following applications:

- **Security Center (Admin user):** The admin user's password for Security Desk, Config Tool, and Genetec™ Update Service.
- **Server Admin:** The password for the Genetec™ Server Admin application.

If your appliance is a Security Center expansion server, you aren't prompted to change any passwords. Select **Skip this step** if you don't want to set new passwords.

9 On the *Hardening* page, select one of the following hardening profiles:

- **Microsoft (only):** This hardening profile applies Microsoft security baselines to your system. Microsoft security baselines are a group of Microsoft-recommended configuration settings that are based on feedback from Microsoft security engineering teams, product groups, partners, and customers.
- **Microsoft with CIS Level 1:** This hardening profile applies Microsoft security baselines and the Center for Internet Security (CIS) Level 1 (CIS L1) profile to your system. The CIS L1 provides essential security requirements that can be implemented on any system with little or no performance impact or reduced functionality.
- **Microsoft with CIS Level 2:** This hardening profile applies Microsoft security baselines and the CIS L1 and Level 2 (L2) profiles to your system. The CIS L2 profile offers the highest level of security and is intended for organizations where security is of utmost importance.

  NOTE: The strict security that this hardening profile brings can reduce system functionality and make remote server management more difficult.
- **Microsoft with STIG:** This hardening profile applies Microsoft security baselines and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) to your system. DISA STIGs are based on National Institute of Standards and Technology (NIST) standards and provide advanced security protection for Windows systems for the U.S. Department of Defense.

NOTE: The *Hardening* page is available only for appliances with the Streamvault service.

10 On the *System Availability Monitor* page, choose a data collection method:

- **Do not collect data:** The System Availability Monitor Agent is installed but doesn't collect any data.
- **Data will be collected anonymously:** No activation code is required. Health data is sent to a dedicated Health Monitoring Service where the entity names are disguised and untraceable. This data is used only by Genetec Inc. for statistics and can't be accessed through GTAP.
- **Data will be collected and linked to my system:** An activation code is required. The health data that is collected is linked to a system that is registered with an active System Maintenance Agreement (SMA).

11 Read the confidentiality agreement, select the **I accept the terms in the confidentiality agreement** checkbox, and click **Apply**.

12 On the *Conclusion* page, click **Close**.

The **Start the activation wizard after setup** option is selected by default. If you clear it, you're reminded to activate the product.

After you finish

Activate your appliance before use.

Activating your Security Center license on an appliance

The *Streamvault Control Panel activation* wizard helps you activate your Security Center license on your Streamvault™ appliance.

Before you begin

- Connect your appliance to the internet.
- Make sure you have the System ID and password that was sent to you after you purchased your license.

What you should know

- This task only applies to appliances with an internet connection. For an appliance without internet, manually activate your Security Center license from Server Admin.
- You only need to activate the Security Center license on the appliance that hosts the Directory role, not on expansion server or workstation appliances.

Procedure

1 From the SV Control Panel, click **The system is not activated. Click here to activate.**

The *Streamvault Control Panel activation* wizard opens.

NOTE: If you see the message Internet access is required for activation, your appliance is currently not connected to the internet. Either connect your appliance now, or manually activate your license from Server Admin.

2 On the *Activation* page, click **System ID** and click **Next**.

3 On the *System ID* page, enter your System ID and password and click **Next**.

4 On the *Summary* page, verify that the System ID is correct and click **Activate**.

The *Result* page opens and indicates that activation was successful.

5 Click **Next**.

6 (Optional) On the *Updates* page, do one of the following:

- If no updates are available, click **Open Security Center installer assistant**.
- If updates are available, click **View updates** to open the Genetec™ Update Service and install the updates.
- If the update check failed because the Directory is unresponsive, click **Open Server Admin** and make sure that the Directory is ready.

NOTE: If the Genetec Update Service was not ready, the update check might fail. You see the message Unable to check for updates at this time. We'll try again later.

7 On the *Additional features* page, enable or disable Synergis™ Softwire and Genetec™ Mobile.

These features are only displayed if they are installed on your appliance. The Genetec Mobile feature is only available for Security Center 5.8 and earlier.

8 Close the *Streamvault Control Panel activation* wizard.

After you finish

- (Optional) Activate the System Availability Monitor agent.
- Configure your Security Center settings using the Security Center installer assistant

Related Topics

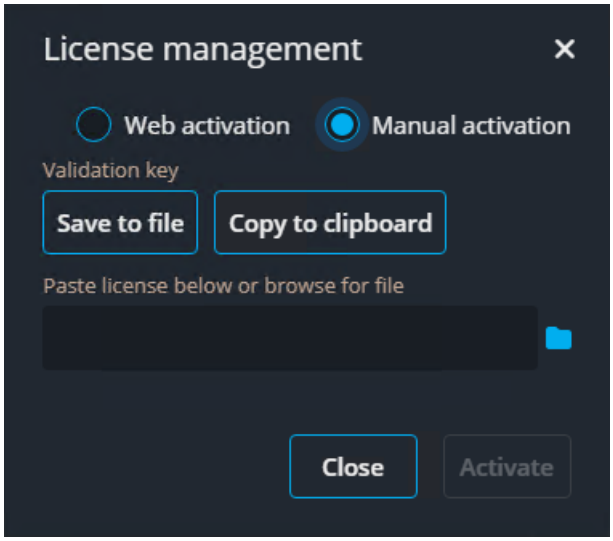
Activating a license manually from Server Admin on page 24
About page of the SV Control Panel on page 69

Activating a license manually from Server Admin

If your Streamvault™ appliance doesn't have internet access, you must activate your Security Center license manually from Server Admin.

Procedure

1 Save the validation key:
   a) From your appliance, open the SV Control Panel.
   b) From the homepage, click the **Server Admin** icon.
   c) Log on to Server Admin.
      If the Server Admin password is different from the Windows admin password, log on to Server Admin using the credentials specified in the *Streamvault Control Panel setup* wizard.
   d) On the *License* page, click **Modify**.
   e) In the *License management* dialog box, select **Manual activation** > **Save to file**.
      The default name for the file is *validation.vk*.



   f) Copy the *validation.vk* file to a USB key.
   g) Eject the USB key from the computer.

2 Get the license from GTAP:
   a) On another computer that has internet access, connect the USB key.
   b) Log in to GTAP.
   c) On the *GTAP login* page, enter the System ID and password assigned to you when you purchased your license, and then click **Login**.
   d) From the *System Information* page, click **Activate license** in the *License information* section.
   e) In the dialog box that opens, paste the validation key or browse for the file.
   f) In the *Activation* dialog box, browse to the *validation.vk* file on the USB key, and then click **Submit**.
      The message *Your license has successfully been activated* is displayed.
   g) Click **Download License**, and then save the license key.
      The default file name is your System ID, followed by *_Directory_License.lic*.
   h) Copy the *_Directory_License.lic* file to the USB key.
   i) Eject the USB key from the computer.

3 Activate your license:
   a) On your appliance, connect the USB key.
   b) Return to Server Admin.
   c) On the *License* page, click **Modify**.
   d) In the *License management* dialog box, select **Manual activation**.
   e) Paste your license information from the *License.lic* file (open with a text editor), or browse for the *License.lic* file, and then click **Open**.
   f) Click **Activate**.

Related Topics

Activating your Security Center license on an appliance on page 22

Activating System Availability Monitor

To monitor your system availability and health issues on GTAP, you can set System Availability Monitor to collect data about your appliance, and send it to Health Monitoring Services.

Before you begin

To collect and report health information about your appliance, you must generate an activation code on GTAP. For information on how to do so, see Generating activation codes for the System Availability Monitor Agent on the TechDoc Hub.

Procedure

1 Open the SV Control Panel.

2 On the *Configuration* page, click **Configure** in the *System Availability Monitor*.

3 In the *Genetec System Availability Monitor Agent* window, click **Modify**.

4 Verify that the **Data will be collected and linked to my system** checkbox is selected.

5 In the **Activation code** field, type the code for your appliance.

6 Click **OK**.

Enabling Security Center video and access control features

The *Security Center installer assistant* wizard guides you through setting up the main features of video management and access control.

What you should know

Settings that you apply in the assistant can be changed later in Config Tool.

Applies to: Appliances that host the Directory role, such as all-in-one appliances.

Procedure

1 Log on as an Admin user.

TIP: If your Security Center password is different from the Windows admin password, log on to Security Center using the password credentials specified in the *Streamvault Control Panel setup* wizard.

The Security Center installer assistant opens.

2 After reading the *Intro* page, click **Next**.

3 On the *Available features* page, choose the features you want and click **Next**.

Basic features are enabled by default. You can enable and disable features later on the *Features* page in the **General settings** view of the *System* task.

NOTE: If your license doesn't support a feature, the feature doesn't appear in the list.

4 On the *Camera security* page, specify the default username and password that are used for all your cameras, and then click **Next**.

TIP: For added security, select **Use HTTPS**.

5 On the *Camera quality settings* page, configure the following options:

- **Resolution:**
  - **High**: 1280x720 and higher
  - **Standard**: More than 320x240 and less than 1280x720
  - **Low**: 320x240 and lower
  - **Default**: Manufacturer's default settings

  The camera always uses the highest resolution that it can support from the chosen category. If the camera doesn't support any resolutions from the chosen category, it uses the highest resolution that it can support from the next category. For example, if the camera can't support a High resolution, it uses the highest resolution it can support from the Standard group.

Settings on this page can be modified later from the *Camera default settings* page of the Archiver role.

6 On the *Recording settings* page, select the default recording settings to apply to all cameras:

- **Off:** Recording is off.
- **Continuous:** Cameras record continuously. This is the default setting.
- **On motion/Manual:** Cameras record when triggered by an action (such as Start recording, Add bookmark, or Trigger alarm), by motion detection, or manually by a user.
- **Manual:** Cameras record when triggered by an action (such as Start recording, Add bookmark, or Trigger alarm), or manually by a user.

  NOTE: When the **Manual** setting is used, then motion does not trigger any recording.
- **Custom:** You can set a schedule for when recording occurs.

7 Click **Next**.

8 On the *Access control unit security* page, specify the default username and password for all your access control units, and click **Next**.

9 On the *Cardholders* page, select how you want to add your credentials (cards) and cardholders.
   a) Select whether you want to add cardholders (when the Security Center installer assistant closes) through the *Cardholder management* task or by using the Import tool.
   b) Click **Next**.

10 On the *Users* page, add more users to your system:
   a) Enter the username.
   b) Select the **User Type**:
      - **Operator:** An operator can use the *Monitoring* task, view video, and manage visitors in Security Desk.
      - **Reporting:** A reporting user can use the Security Desk application and run the most basic reporting tasks, excluding the tasks for AutoVu™ ALPR. A user who only has reporting privileges can't view any video, control any physical devices, or report incidents.
      - **Investigator:** An investigator can use the *Monitoring* task, view video, control PTZ cameras, record and export video, add bookmarks and incidents, use investigation tasks, manage alarms and visitors, override door unlock schedules, save tasks, and so on.
      - **Supervisor:** A supervisor can use the *Monitoring* task, view video, control PTZ cameras, record and export video, add bookmarks and incidents, use investigation tasks, manage alarms and visitors, override door unlock schedules, save tasks, and so on. A supervisor can also use maintenance tasks, manage cardholders and credentials, modify custom fields, set threat levels, block cameras, and perform people counting.
      - **Provisioning:** A provisioning user has most of the configuration privileges, except for the following: managing roles, macros, users, user groups, custom events, Activity trails, threat levels, and audio files. The provisioning user is typically a system installer.
      - **Basic AutoVu Operator:** This user type is for operators who use AutoVu ALPR. The Basic AutoVu user can use ALPR tasks, configure ALPR entities, create ALPR rules, monitor ALPR events, and so on.
      - **Patroller User:** This user type is for Genetec Patroller™ users who use AutoVu ALPR. The Patroller user can use ALPR tasks, configure ALPR entities, create ALPR rules, monitor ALPR events, and so on. A Patroller user doesn't have access to other Security Center applications, for example, Config Tool, and Security Desk. The Patroller user can't modify reports or change the Patroller password.

11 Enter and confirm the **Password**, and then click **Add**.
   The new user is added to the list of users on the right of the dialog box. To delete a user, select a user from the list, and click ✖.
   You change user profiles in the **Users** view of the *User Management* task. For information, see Security Center Administrator Guide on the TechDoc Hub.

12 Click **Next**.

13 Confirm that the information on the *Summary* page is correct, and then click **Apply**, or click **Back** to fix any errors.

14 On the *Conclusion* page, click **Restart**.
   Config Tool restarts to apply your settings.
   NOTE: The **Open the unit enrollment tool after wizard closes** option is selected by default. You can clear this option and open the Unit enrollment tool later by clicking the **Enroll cameras and controllers** shortcut on the SV Control Panel *Home* page.

After you finish

Add units to your system by using the Unit enrollment tool.

Related Topics

Configuring default camera settings on page 32
Creating custom recording schedules on page 34
Homepage of the SV Control Panel on page 61

About the Unit enrollment tool

Unit enrollment is a tool that you can use to discover IP units (video and access control) connected to your network, based on their manufacturer and network properties (discovery port, IP address range, password, and so on). After you discovered a unit, you can add it to your system.

- The Unit enrollment tool opens automatically after the *Security Center installer assistant* unless you cleared the **Open the unit enrollment tool after the wizard** option.
- When adding access control units, only HID and Synergis™ units can be enrolled with Unit enrollment tool. For complete details on how to enroll Synergis units, see the *Synergis™ Appliance Configuration Guide*.

Opening the Unit enrollment tool

There are three ways to open the Unit enrollment tool.

Procedure

- Do one of the following:
  - From the SV Control Panel homepage, click **Enroll cameras and controllers**.
  - From the SV Control Panel homepage, click the **Config Tool** icon, and then click **Tasks** > **Unit enrollment**.
  - From the SV Control Panel homepage, click the **Config Tool** icon, and then click the **Add unit status** icon in the Config Tool notification tray.

Configuring unit enrollment settings

You can use the **Settings and manufacturers** button in the Unit enrollment tool to specify which manufacturers to include when searching for new units. You can also configure the discovery settings for units, and specify username and passwords for units so they can be enrolled easily.

Procedure

1 From the homepage, click **Tools** > **Unit enrollment**.

2 In the *Unit enrollment* dialog box, click **Settings and manufacturers** ().

3 Use the **Refuse basic authentication** option to enable or disable basic authentication (video units only). This is useful if you turned off basic authentication in the Security Center InstallShield, but you need to turn it back on to perform a firmware upgrade or to enroll a camera that supports only basic authentication. To turn basic authentication back on, you must turn the **Refuse basic authentication** option to **OFF**.

NOTE: This option is available only to users with Administrator privileges.

4 Click **Add manufacturer** () to add a manufacturer to the list of units to be discovered.

To delete a manufacturer from the list, select it and click .

5 Configure the individual settings for any manufacturers that you added. To do this, select the manufacturer and click .

IMPORTANT: You must enter the correct username and password for the unit to enroll properly.

6 (Optional) Remove units from the list of ignored units (see Removing units from list of ignored units on page 31).

7 Click **Save**.

Adding units

Once new units have been discovered, you can use the Unit enrollment tool to add them to your system.

Procedure

1 From the homepage, click **Tools** > **Unit enrollment**.

2 There are three ways to add newly discovered units:

- Add all the new discovered units at the same time by clicking the **Add all** () button at the lower right side of the dialog box.
- Click a single unit in the list, then click **Add** in the **Status** column
- Right-click a single unit from the list and click **Add or Add Unit**.

  When a video unit does not have the correct username and password, the **Status** for the unit will be listed as **Bad logon** and you will be prompted to enter the correct information when you add the unit. If you want to use the same username and password for all the cameras on your system, select the **Save as default authentication for all manufacturers** option.

You can also add a unit manually, by clicking the **Manual add** button at the bottom of the *Unit enrollment tool* dialog box.

NOTE:

- For video units, if the added camera is an encoder with multiple streams available, each stream is added with the *Camera - n* string appended to the camera name, *n* representing the stream number. For an IP camera with only one stream available, the camera name is not modified.
- If you are adding a SharpV, by default, the camera units include a self-signed certificate that uses the common name of the SharpV (for example, SharpV12345). To add the SharpV to the Archiver, you must generate a new certificate (signed or self-signed) that uses the camera's IP address instead of the common name.

Clearing added units

You can clear units that have already been added to your system so they are not displayed every time you use the Unit enrollment tool to discover units on your system.

What you should know

The **Clear completed** option in the Unit enrollment tool is permanent, it cannot be reversed.

Procedure

1 Add the desired discovered units to your system, see Adding units on page 30.

2 Once the units have been added, click **Clear completed**.

Any unit that has **Added** displayed in the **Status** column will be cleared from the list of discovered units.

Ignoring units

You can choose to ignore units so they don't appear in the list of discovered units of the Unit enrollment tool.

Procedure

1 From the homepage, click **Tools** > **Unit enrollment**.

The Unit enrollment tool opens with the list of units that have been discovered on the system.

2 Right-click the unit you want to ignore, and select **Ignore**.

The unit is removed from the list and will be ignored when the Unit enrollment tool discovers new units. For information about removing a unit from the list of ignored units, see Removing units from list of ignored units on page 31.

Removing units from list of ignored units

You can remove a unit from the list of ignored units so it's not ignored when a discovery is performed by the Unit enrollment tool.

Procedure

1 From the homepage, click **Tools** > **Unit enrollment**.

2 In the upper right corner of the *Unit enrollment* dialog box, click **Settings and Manufacturers** ( ).

3 Click **Ignored units** and click **Remove all ignored units**, or you can select a single unit and click the **Remove ignored unit** button ( ).

Configuring default camera settings

From the *Camera default settings*, you can modify the default recording and video quality settings applied to all cameras controlled by the Archiver. Initially, these settings are configured on the *Camera quality settings* page in the Security Center installer assistant.

What you should know

You can also apply video and recording settings for a camera in Config Tool using the **Video and Recording** tab of the unit. Settings made for an individual camera take precedence over the settings that are applied in the Security Center installer assistant or on the *Camera default settings* page.

Procedure

1 From the Config Tool homepage, open the *Video* task.

2 Select the Archiver role, and then click the **Camera default settings** tab.

3 Under **Video quality (Same across all archivers)**, configure the following:

- **Resolution:**
  - **High**: 1280x720 and higher
  - **Standard**: More than 320x240 and less than 1280x720
  - **Low**: 320x240 and lower
  - **Default**: Manufacturer's default settings

  The camera always uses the highest resolution that it can support from the chosen category. If the camera doesn't support any resolutions from the chosen category, it uses the highest resolution that it can support from the next category. For example, if the camera can't support a High resolution, it uses the highest resolution it can support from the Standard group.

4 Under **Recording**, click to add a schedule.

Available schedules include:

- Schedules that were created using the **Schedules** view in the *System* task.
- A custom schedule, if one was created in the Security Center installer assistant.

5 From the **Mode** drop-down, select a mode for the recording schedule:

- **Off:** Recording is off.
- **Continuous:** Cameras record continuously. This is the default setting.
- **On motion/Manual:** Cameras record when triggered by an action (such as Start recording, Add bookmark, or Trigger alarm), by motion detection, or manually by a user.
- **Manual:** Cameras record when triggered by an action (such as Start recording, Add bookmark, or Trigger alarm), or manually by a user.

  NOTE: When the **Manual** setting is used, then motion does not trigger any recording.
- **Custom:** You can set a schedule for when recording occurs.

6 Configure the following options:

- **Record audio:** Turn this option on when you want to record audio along with video. A microphone entity must be attached to your cameras for this option to work.
- **Redundant archiving:** Turn this option on when you want both primary and secondary servers to archive video at the same time. This setting is only effective when failover is configured.
- **Automatic cleanup:** Turn this option on when you want to delete video after a specified number of days. Video is deleted whether the Archiver storage is full or not.
- **Time to record before an event:** Use the slider to set the number of seconds that you want to be recorded before an event. This buffer is saved whenever the recording starts, ensuring that whatever prompted the recording is also captured on video.
- **Time to record after a motion:** Set the number of seconds that you want the recording to continue after a motion event. During this time, the user can't stop the recording.
- **Default manual recording length:** Set the number of minutes that you want to record when a user starts the recording. The user can stop the recording at any time before the duration expires. This value is also used by the Start recording action, when the default recording length is selected.

7 Click **Apply**.

8 If you want to apply the new settings to all existing cameras, click **Yes**.

Related Topics

Enabling Security Center video and access control features on page 27

Creating custom recording schedules

Create custom recording schedules from the Security Center installer assistant to have cameras record in different recording modes for a specific time range.

Procedure

1 On the *Recording settings* page, click + under **Recording schedule**.

2 Enter a name for the new schedule.

3 From the **Recording mode** list, select one of the following:

- **Off:** Recording is off.
- **Continuous:** Cameras record continuously. This is the default setting.
- **On motion/Manual:** Cameras record when triggered by an action (such as Start recording, Add bookmark, or Trigger alarm), by motion detection, or manually by a user.
- **Manual:** Cameras record when triggered by an action (such as Start recording, Add bookmark, or Trigger alarm), or manually by a user.

  NOTE: When the **Manual** setting is used, then motion does not trigger any recording.
- **Custom:** You can set a schedule for when recording occurs.

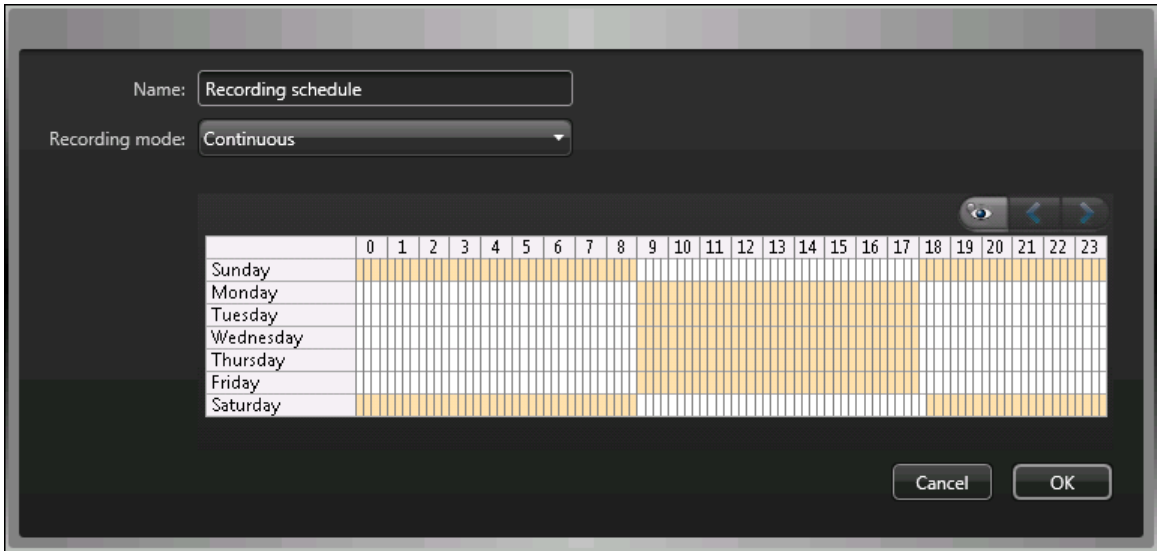
4 For each day of the week, specify the time range for recording:

- Click and drag to select a block of time.
- Right-click and drag to clear a block of time.
- Use the cursor keys to scroll through the 24-hour timeline.

TIP: To switch to high-resolution mode, where each block represents 1 minute, click .

Example

The following example shows a schedule where recording occurs continuously from 6:00 pm to 9:00 am on weekends and from 9:00 am to 5:00 pm on weekdays.



Related Topics

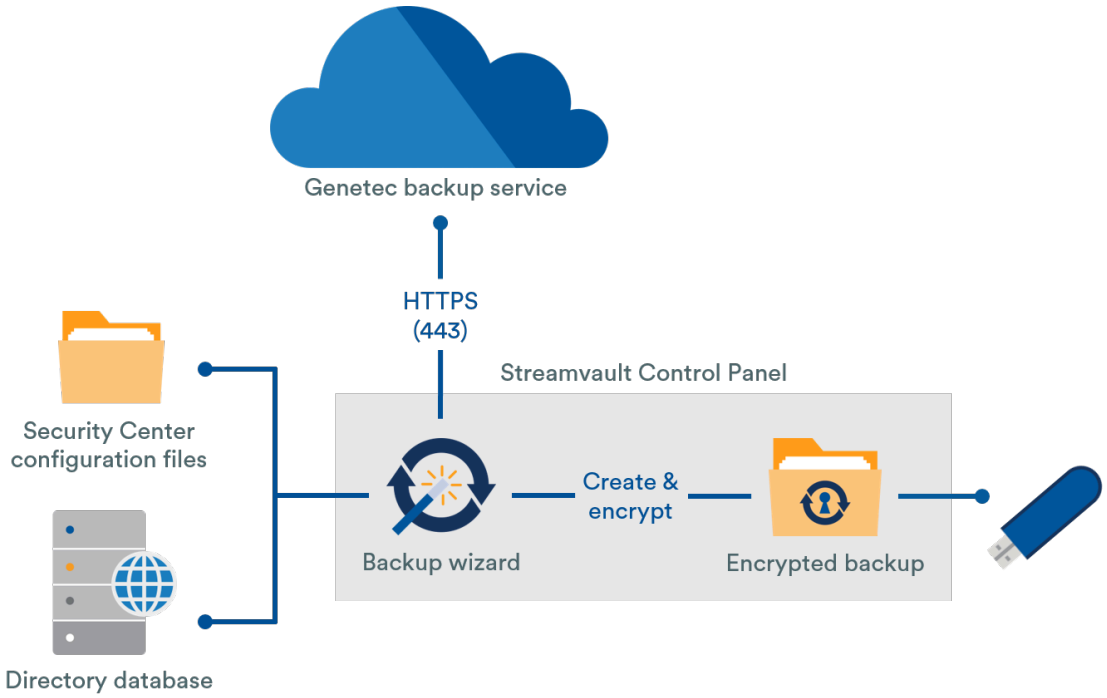
Enabling Security Center video and access control features on page 27

About backup and restore

Using the SV Control Panel, you can securely back up your Directory database and configuration files. Later, you can restore them to the same System ID in the event of a system failure or hardware upgrade.

How backup and restore works in the SV Control Panel

You create backups of your Directory database and configuration files and store them in the cloud or locally. The following architecture diagram shows how backup works in the SV Control Panel:



Benefits of backup and restore

- Easily back up your files to the cloud or locally using the *Backup* wizard. If you are backing up files to the cloud, the five most recent backups are kept.
- Easily restore any of the five cloud backups or any of your local backups to the same System ID using the *Restore* wizard.
- All backup files can be encrypted.
- The system locks after five failed attempts to log on.
- You don't need to be enrolled in the Genetec™ Advantage program to use this feature.

Limitations of backup and restore

- A backup excludes your license files, video archives, or other databases.
- You can't restore a backup on an earlier version of Security Center. For example, you can't restore a backup from a Security Center 5.10 system to a Security Center 5.9 system.
- You can't restore the configuration files if you're restoring across major versions of Security Center. For example, you can't restore the configuration files from a Security Center 5.9 system backup to a Security Center 5.10 system.

Related Topics

Backing up your Directory database on page 36
Restoring your Directory database on page 37

Backing up your Directory database

You can use backup and restore to safely back up your Directory database and configuration files. Backup and restore makes configuring your system easier after a hardware upgrade and can restore your configurations after a system failure.

Before you begin

Make sure of the following:

- Security Center 5.9 or later is installed.
- Genetec™ Server is running.
- You have a valid and active license.

What you should know

- Easily back up your files to the cloud or locally using the *Backup* wizard. If you are backing up files to the cloud, the five most recent backups are kept.
- Only administrators can perform a backup, and all backups to the cloud must be authenticated.

Procedure

1 In the SV Control Panel, click the **Configuration** tab.

2 Under *Backup/Restore Directory and configurations*, click **Backup wizard** > **Next**.

3 On the *Backup method* page, select either **Cloud** or **Local**, and then click **Next**.

- If you selected **Cloud**, do the following:
  a. On the *Authentication* page, enter either your System ID or GTAP credentials to authenticate the backup.
     NOTE: After you've entered your credentials the first time, you won't be asked again for future backups.
  b. On the *Security* page, select one of the following two options:
     - **Let Genetec manage my security:** You don't need to provide a password. The backup cloud service from Genetec Inc. encrypts your data.
     - **Use my own password:** Create and remember your own password to use later for the encryption of your backup files.
       IMPORTANT: If you lose or forget your password, Genetec Inc. can't recover the lost password.
- If you selected **Local**, do the following:
  a. On the *Destination folder* page, enter a name for the backup and navigate to the folder where you want to store the backup.
  b. On the *Security* page, create a password to encrypt your backup file. You can also select **Do not encrypt my backup**, although it's not recommended.

4 Follow the rest of the steps in the wizard to complete your backup.

Related Topics

About backup and restore on page 35
Restoring your Directory database on page 37

Restoring your Directory database

If you backed up your Directory database and configuration files by using backup and restore in the SV Control Panel, you can restore your backup files to the same System ID. Backup files can be restored in the event of a system failure or hardware upgrade.

Before you begin

Make sure of the following:

- Security Center 5.9 or later is installed.
- Genetec™ Server is running.
- You have a valid and active license.

What you should know

- If you backed up your files to the cloud, you can restore any of the last five backups to the same System ID.
- If you backed up your files locally, you can restore any of your backups to the same System ID.
- If you created your own password for your encrypted backup files during the backup process, you need it to restore your files.

Procedure

1 In the SV Control Panel, click the **Configuration** tab.

2 Under *Backup/Restore Directory and configurations*, click **Restore wizard** > **Next**.

3 On the *Restore method* page, select either **Cloud** or **Local**.

If you selected **Cloud**, on the *Authentication* page, enter either your System ID or GTAP credentials, depending on which one you used to authenticate the backup. If you use your GTAP credentials, an activation code is sent to your email.

4 On the *Backup selection* page, select the file you want to restore to your system.

5 On the *Restore* page, if you chose to create a password during the backup process, you must enter your password here.

6 Follow the rest of the steps in the wizard to complete the restore process.

Related Topics

Backing up your Directory database on page 36
About backup and restore on page 35

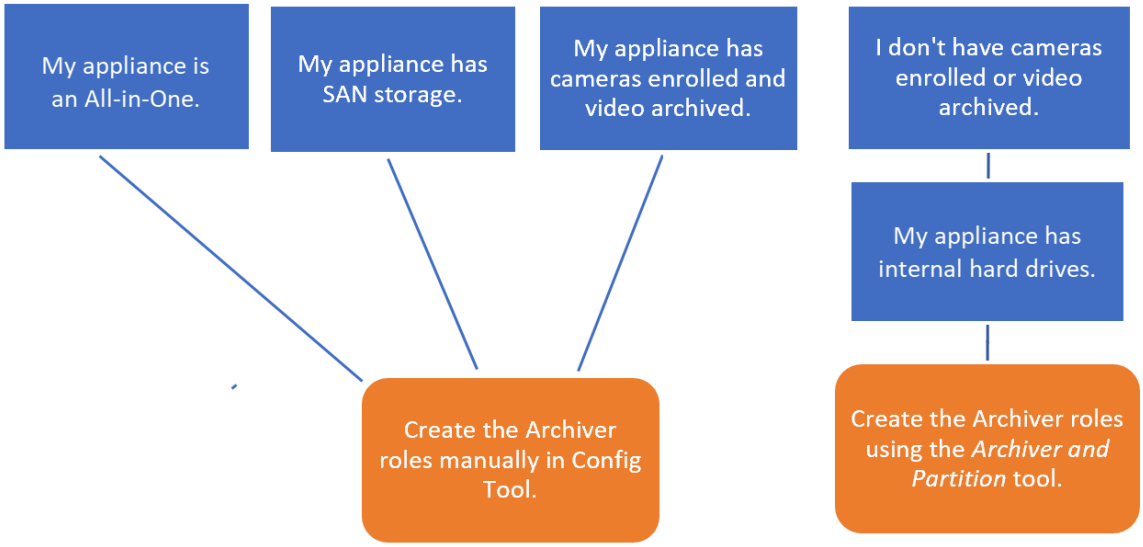
Choosing the method for creating Archiver roles and partitions

To set up your appliance for the expected number of cameras and bandwidth usage, you need to create enough Archiver roles. Depending on the type and state of your appliance, you can choose between two methods.

- Using the Archiver Roles and Partitions tool.
- Manually creating partitions and Archiver roles.

Choosing the method for your situation

Use the following decision tree to help you decide which method to use:



About the Archiver Roles and Partitions tool

You can access the Archiver Roles and Partitions tool in the SV Control Panel. The tool calculates how many Archiver roles you need based on the number of cameras that you plan to deploy and their expected bandwidth.

This tool is only available on Streamvault™ models that have an internal hard drive. If you're setting up an external storage device, such as SAN on a Streamvault™ SV-7000EX series appliance, follow the steps in Adding partitions and Archiver roles manually on page 40.

When the tool creates partitions, all local volumes except C: are erased and existing Archiver roles and enrolled cameras are removed from Security Center. So, if your appliance has cameras and recorded video that you want to keep, manually add the partitions and Archiver roles.

Adding Archiver roles in the SV Control Panel

Use the Archiver Roles and Partitions tool to add enough Archiver roles to support the expected video traffic. This tool is available on Archiver appliances from the Streamvault™ 1000, 2000, and 4000 series.

Before you begin

- Choose the appropriate method for creating Archiver roles and partitions.
- Back up the important data on the drive that you plan to partition.

  CAUTION: The Archiver Roles and Partitions tool can delete existing data, including the Archiver role configuration and all files on the D: drive.

Procedure

1 In the SV Control Panel, click the **Configuration** tab.

2 Under *Archiver roles and partitions*, click **Configure**.

The *Archiver Roles and Partitions* dialog box opens.

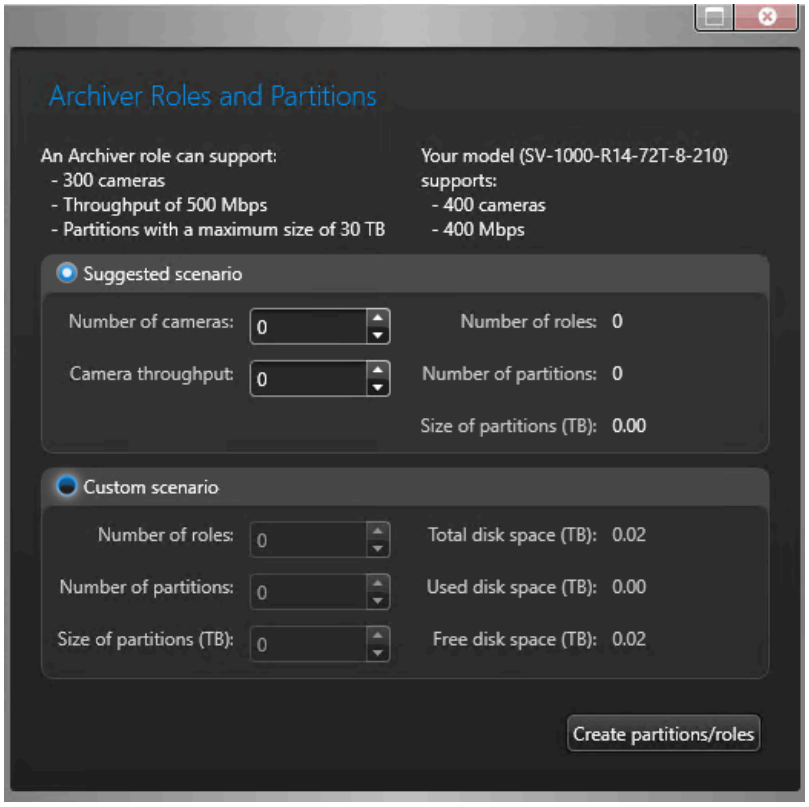
3 To configure the number of Archiver roles and partitions, select one of the following options:

- To let the tool calculate the number of roles, the number of partitions, and the partition size you need, select **Suggested scenario**. Enter the number of cameras that you expect to deploy, and the expected throughput of each camera.
- To specify the number of Archiver roles and partitions to create, select **Custom scenario**. Enter the number of Archiver roles, the number of partitions, and the partition size.

  The number of partitions must be a multiple of the number of Archiver roles.

CAUTION: Files on the drive you partition are deleted.

4 Click **Create partitions and roles**.



5 In the *Warning* window, select the checkbox to confirm that you want to proceed.

6 Click **OK**.

The *Result* window opens and displays the name and locations of the Archiver roles and partitions. Each Archiver role is automatically assigned a drive letter.

Adding partitions and Archiver roles manually

To set up your Streamvault™ SV-7000EX or SV-300E All-in-One appliance for the first time, you must manually create partitions. You can also manually add Archiver roles to an appliance that already has data on it, so the data is not lost.

Before you begin

Choose a method for creating partitions on your appliance.

What you should know

Formatting a volume deletes the data on the partition. To preserve data, shrink the volume and then create new volumes.

Procedure

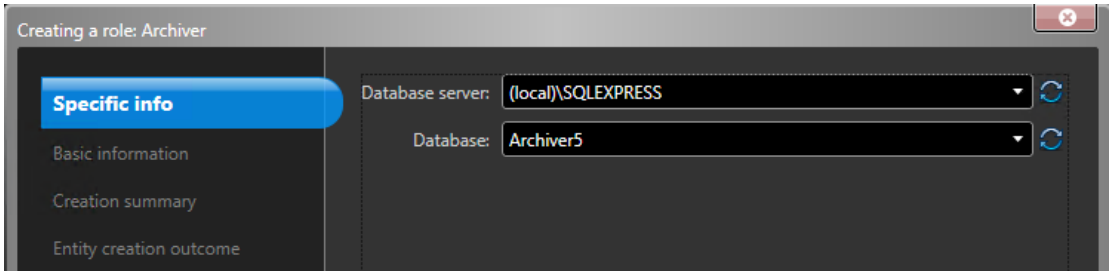
1 If the appliance already has cameras enrolled, video archived, or access control data, do the following:

a) Back up the Directory database using the SV Control Panel.

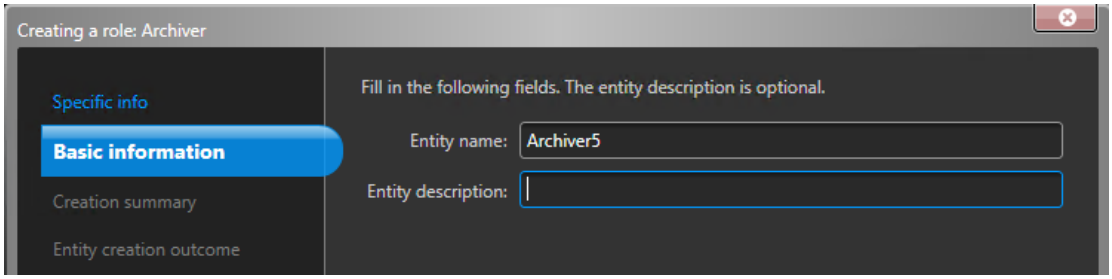
b) Generate a *Camera configuration* report to take a snapshot of your current camera configuration. For information, see Viewing camera settings on the TechDoc Hub.

2 Create the volumes that you need for the Archiver roles you plan to create on the appliance.
   - On appliances that connect with SAN storage, such as SV-7000EX series appliances, create a logical unit number (LUN) for each Archiver role.
   - On appliances that have internal storage drives, such as SV-1000E, SV-2000E, and SV-4000E, use the Windows *Disk Management* tool to set up the volumes.

3 In Security Center, create an Archiver role:
   a) From the Config Tool homepage, open the *System* task and click the **Roles** view.
   b) Click **Add an Entity** and select **Archiver**.
      The Archiver role configuration wizard opens.
   c) On the *Specific info* page, enter a name for the Archiver role **database** and click **Next**.
      Each Archiver role must have a dedicated database.

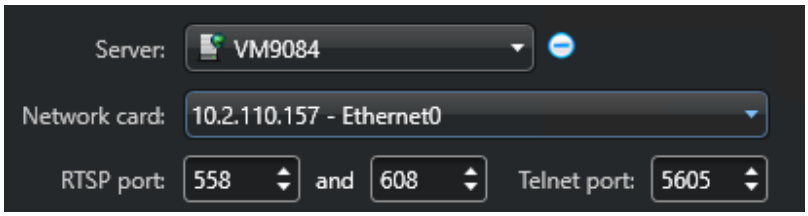


   d) In the **Basic information** section, enter the **Entity name** and click **Next**.
      It is best practice for the Archiver role database name to match the entity name.



   e) Verify that the information on the *Creation Summary* page is correct and click **Create**.

4 Configure the Archiver role.
   a) In the entity browser, select your new Archiver role and click **Resources**.
   b) Click ⊕ to expand the *Server* section and select a network interface card (NIC) from the **Network card** list.
      All Archiver roles must use the same NIC.



   c) Under *Recording*, select or create a **Disk group** or **Network Location** for the Archiver role.
      Each Archiver role needs a dedicated recording location. If Archiver A writes to disks A, B, and C, then Archiver B should write to disks D, E, and F. A role can own multiple partitions, but two roles should never use the same partition.
   d) Click **Apply**.

5 Repeat steps 3 and 4 to create each Archiver role.

6 Add your cameras to their designated Archiver role:

a) From the Config Tool homepage , open the *Video* task.

b) In the entity browser, select the Archiver role that you want to assign the camera to, and click **Video Unit** ().

c) In the dialog box that opens, enter the required information regarding the camera and click **OK**.

NOTE: It takes a few seconds to add the cameras. If the role is unable to add a camera in the given time, a failed status is indicated, and the camera is removed.

d) Click **Apply**.

3

Getting started with Streamvault Maintenance plugin

Getting started introduces the Streamvault Maintenance plugin and provides information about how to set up the plugin.

This section includes the following topics:

About the Streamvault Maintenance plugin

The Streamvault™ Maintenance plugin is used to monitor the health of your Streamvault™ appliances and ensure you receive notifications when problems occur.

NOTE: This guide is applicable to the Streamvault Maintenance plugin 2.0.

The Streamvault Maintenance plugin includes the following components:

- Streamvault role: Plugin role used to run either the hardware monitor or manager entity. One role is required for each Streamvault appliance that you need to monitor.
- *Streamvault™ hardware monitor*: Entity used to define the alert configurations for each Streamvault appliance.
- *Streamvault™ manager*: Entity used to bulk-control configurations for a group of Streamvault appliances. Only one Streamvault manager instance can be created.
- *Streamvault™ hardware*: Report task in Security Center used to view a list of health issues affecting your Streamvault appliances.

The plugin entity configurations consist of the following settings:

- **Alert configurations**: used to define the types of **Events**, **Severity** levels, and **Notification** types that affect alerts addressing the health statuses of your Streamvault servers.
- **Email recipients**: used to select which users and user groups receive email notifications.
- **Remote management credentials**: used to control the creation of user profiles in iDRAC.
- **Integrated Dell Remote Access Controller (iDRAC) integration** (for Streamvault models that support iDRAC): used to exercise more precise control over credential management. This feature can be found on the **Management** tab of the plugin.

  For more information about iDRAC, see https://www.dell.com/en-us/lp/dt/open-manage-idrac.

  IMPORTANT:

  - For systems with iDRAC-enabled servers, iDRAC firmware must be at version 6.0 or later.
  - For iDRAC-supported devices, the Streamvault Maintenance plugin accesses health data using an internal connection, as long as Dell's iDRAC Service Module (iSM) software is installed. iSM is installed by default on models that support iDRAC.

    If iSM isn't available, the plugin uses out-of-band communication with iDRAC. In this case, a network connection must exist between the iDRAC dedicated port and at least one LAN port if port sharing isn't used. The dedicated iDRAC port is disabled by default. For more information, refer to the following: https://www.dell.com/support/kbdoc/en-ca/000177212/dell-poweredge-how-to-configure-the-idrac9-and-the-lifecycle-controller-network-ip.

Downloading and installing the plugin

To integrate the Streamvault™ Maintenance plugin into Security Center, you must install the plugin on a Directory server, the Streamvault™ servers you want to monitor, and on all client workstations from which you want to configure the plugin.

Before you begin

Make sure that a compatible version of Security Center is installed. For information, see Supported plugins in Security Center on the TechDoc Hub.

What you should know

- **BEST PRACTICE:** Install the Streamvault role on every server that you need to monitor.
- **IMPORTANT:** Ensure each server's iDRAC module is connected to your network and can communicate with the host system. By default, the iDRAC module shares the same LAN port as the host system and is configured to get an IP address by using DHCP.
- **IMPORTANT:** Before proceeding, ensure that the iDRAC module is updated to firmware 6.00 or later, and that the server BIOS is updated to the latest version.
- The plugin is supported only on servers running the Security Center server software.
- **NOTE:** The Streamvault Maintenance plugin comes pre-installed on all compatible Streamvault servers. Because of this, most users only need to create the roles and entities in Security Center. If your server was shipped before the plugin was made available, or if it was uninstalled, follow these steps to install.

Procedure

1 Open the GTAP Product Download page.

2 Under **Download Finder**, select your version of Security Center.

3 From the *Genetec Plugins* section, download the package for your product.

4 Run the .exe file, and then unzip the file.

By default, the file is unzipped to *C:\Genetec*.

5 Open the extracted folder, right-click the *setup.exe* file, and click **Run as administrator**.

6 Follow the installation instructions.

7 On the *Installation Wizard Completed* page, click **Finish**.

IMPORTANT: The **Restart Genetec™ Server** option is selected by default. You can clear this option if you don't want to restart the Genetec™ Server immediately. However, you must restart the Genetec Server to complete the installation.

8 Close, and then open, any instances of Config Tool and Security Desk.

Genetec Streamvault privileges

To use the *Hardware monitor* and *Manager* tasks associated with the Streamvault™ appliance, user accounts must be assigned the required privileges.

Configuring user privileges for Streamvault

Default privileges are assigned to some user groups, such as administrators.

In the Config Tool *User management* task, you can configure or modify the user or user group privileges on the *Privileges* page of the user or user group.

To learn more about the privilege hierarchy, privilege inheritance, and assigning privileges, see the Security Center Administrator Guide and the Security Center Hardening Guide on the TechDoc Hub on the TechDoc Hub.

NOTE: For a list of all available Security Center privileges, see the Security Center privileges spreadsheet. You can sort and filter this list as needed.

Streamvault plugin role privileges

Streamvault plugin role privileges grant access to tasks associated with Streamvault *Hardware monitor* and *Manager*.

By default, administrators have all privileges. If you create a user account from one of the other privilege templates, the user account requires the following Streamvault plugin role privileges for Config Tool in Streamvault.

Subcategory of privileges	Includes privileges to	Actions that can be performed
Hardware monitor	Modify hardware monitors	• Modify alert configurations • Modify email recipients • Modify remote management credentials • Change port settings
	Add hardware monitors	Create a new hardware monitor entity and assign it to a Streamvault server
	Delete hardware monitors	Delete an existing hardware monitor entity
	View hardware monitors	View a hardware monitor configuration
Manager	Modify manager	• Bulk modify alert configurations • Bulk modify email recipients
	Add manager	Create the manager entity and assign it to a Streamvault server
	Delete manager	Delete the manager entity
	View manager	View the manager configuration

Creating the plugin role

Before you can configure and use the plugin, you must create the Streamvault™ Maintenance plugin role in Config Tool.

Before you begin

Download and install the plugin.

What you should know

The Streamvault Maintenance plugin contains two plugin roles:

- Streamvault™ hardware monitor: The Streamvault™ hardware monitor entity is used to monitor the health of your Streamvault™ appliances and ensure you receive notifications when problems occur. One Streamvault™ hardware monitor per Streamvault™ appliance is required.
- Streamvault™ manager: The Streamvault™ manager entity is used to control the alert configurations for a group of Streamvault™ Agent entities. Only one Streamvault™ manager is allowed per system.
- **NOTE:** If the Directory servers are virtual machines or non-Streamvault servers, create a role for these servers only if you wish to use the manager entity.

Procedure

1 From the Config Tool homepage, open the *Plugins* task.

2 In the *Plugins* task, click **Add an entity** (), and select **Plugin**.

The plugin creation wizard opens.

3 On the *Specific info* page, select the server on which the plugin role is hosted and the plugin type, and then click **Next**.

If you don't use expansion servers in your system, the **Server** option isn't displayed.

4 On the *Basic information* page, specify the role information:

a) Enter the **Entity name**.

b) Enter the **Entity description**.

c) Select the **Partition** for the plugin role.

If you don't use partitions in your system, the **Partition** option isn't displayed. Partitions are logical groupings used to control the visibility of entities. Only users who are members of that partition can view or modify the role.

d) Click **Next**.

5 On the *Creation summary* page, review the information, and then click **Create**, or **Back** to make changes.

After the plugin role is created, the following message is displayed: The operation was successful.

6 Click **Close**.

After you finish

- Configure the Streamvault hardware monitoring entity.
- Configure the Streamvault manager entity.

Configuring a Streamvault hardware monitor entity

You can configure a Streamvault™ hardware monitor entity to monitor the health of a Streamvault™ appliance and set up notifications to be raised when problems occur.

Before you begin

- Enroll your Streamvault appliances.
- Create the Streamvault plugin role.

  IMPORTANT: A Streamvault hardware monitor is automatically created on each Streamvault server that's hosting a Streamvault role. If the hardware monitor entity isn't present in your system after you've created the role, you must create the hardware monitor manually.

What you should know

The configuration options are different depending on whether you have iDRAC-enabled servers or other non-iDRAC servers.

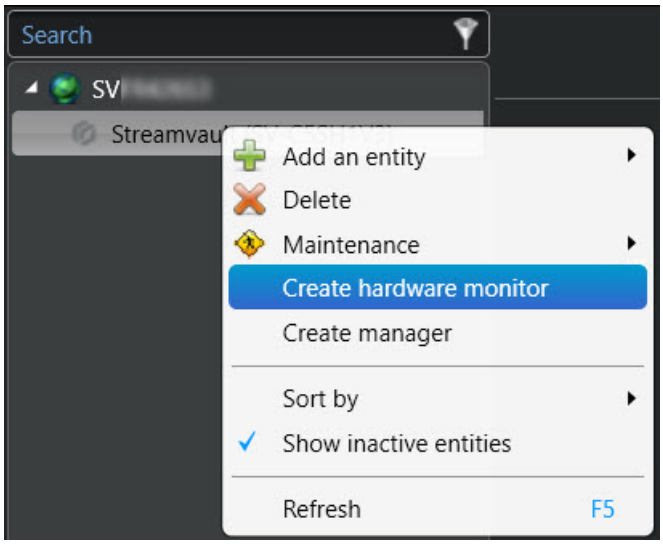
- Configuring an iDRAC-enabled server.
- Configuring a non-iDRAC server.

Procedure

To configure an iDRAC-enabled server:

1 In Config Tool, navigate to the *Plugins* task and select the Streamvault plugin role.

2 Right-click the Streamvault plugin role and click **Create hardware monitor**.



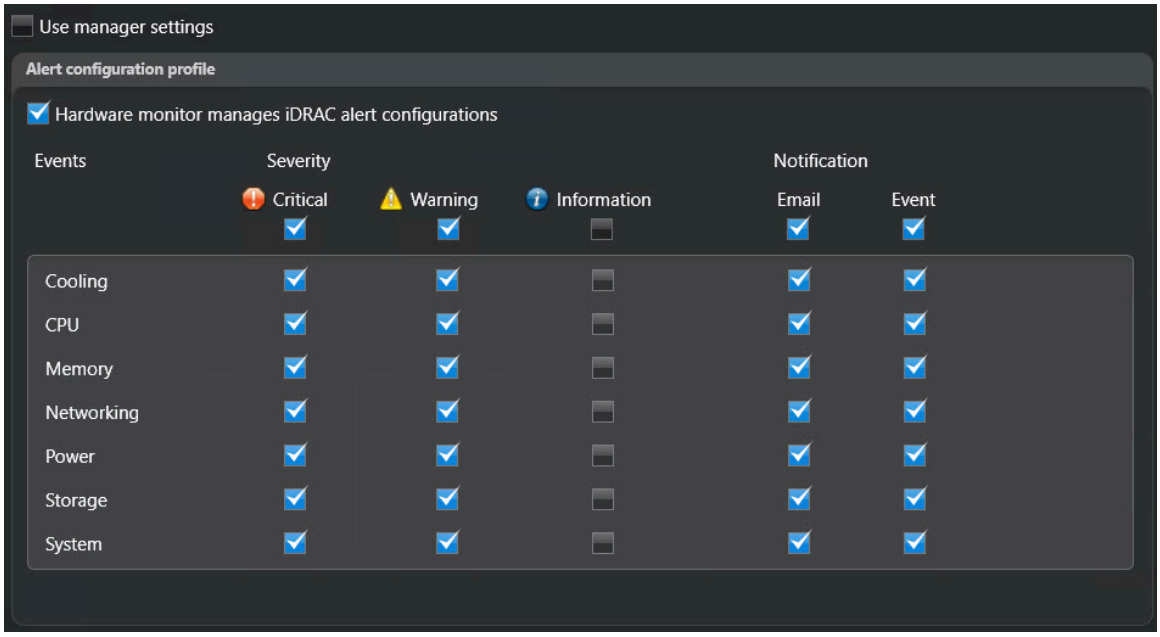
3 On the **Identity** tab, enter a name for the Streamvault hardware monitor in the **Name** field.

4 Select the **General** tab.

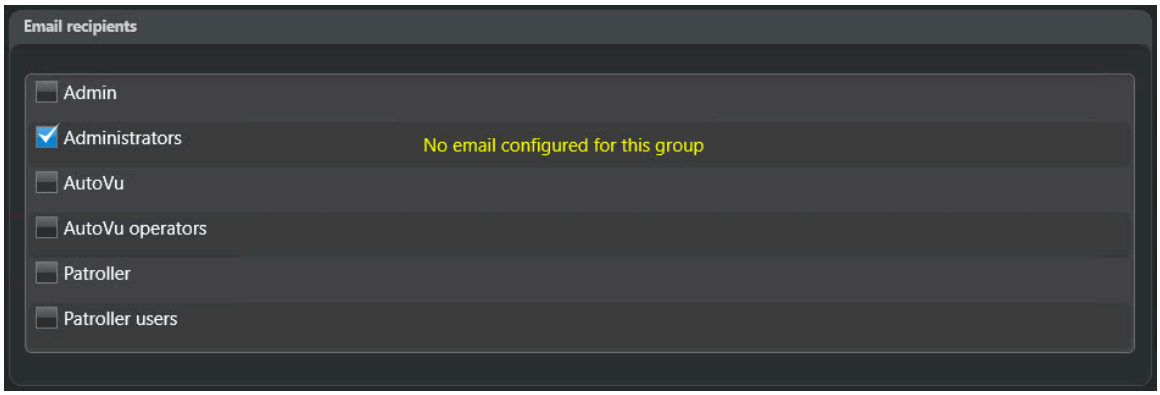
5 (Optional) If you created a Streamvault™ manager entity for your system, select the **Use manager settings** checkbox to use the alert configuration profile settings of the Streamvault manager.

6 In the *Alert configuration profile* section, select the **Hardware monitor manages iDRAC alert configurations** checkbox to manage alert configurations through the Streamvault hardware monitor.

7 Select the checkboxes that correlate with the **Events**, **Severity** levels, and **Notification** types that you want to include for this Streamvault hardware monitor.



8 In the *Email recipients* section, choose which users and user groups receive email notifications when a condition in the *Alert configuration profile* section is met.

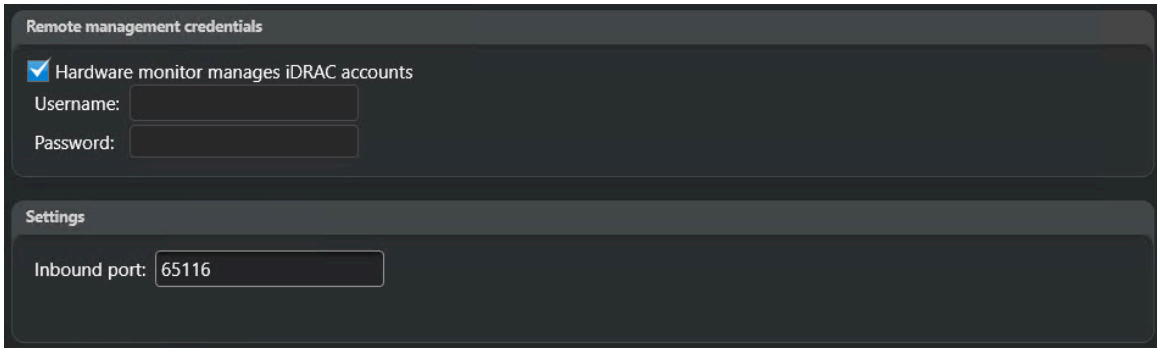


9 In the *Remote management credentials* section, do one of the following:

- Select the **Hardware monitor manages iDRAC accounts** checkbox to manage credentials directly through the plugin.
- Clear the **Hardware monitor manages iDRAC accounts** checkbox to use iDRAC to control user and password creation.

10 (Optional) If you cleared the **Hardware monitor manages iDRAC accounts** checkbox, navigate to the **Management** tab and configure credentials directly in iDRAC.

11 (Optional) In the *Settings* section, you can change the default **Inbound port** from 65115 to your preferred choice. For more information, see Default ports used by Streamvault on page 4.

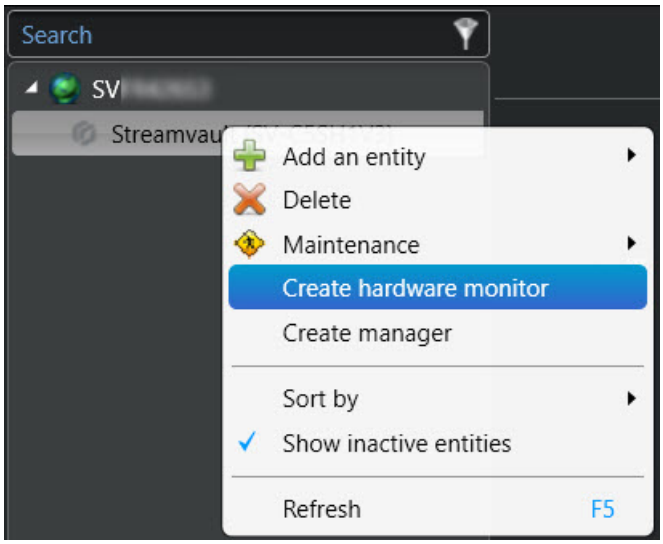


12 Click **Apply**.

To configure a non-iDRAC server:

1 In Config Tool, navigate to the *Plugins* task and select the Streamvault plugin role.

2 Right-click the Streamvault plugin role and click **Create hardware monitor**.



3 On the **Identity** tab, enter a name for the Streamvault hardware monitor in the **Name** field.

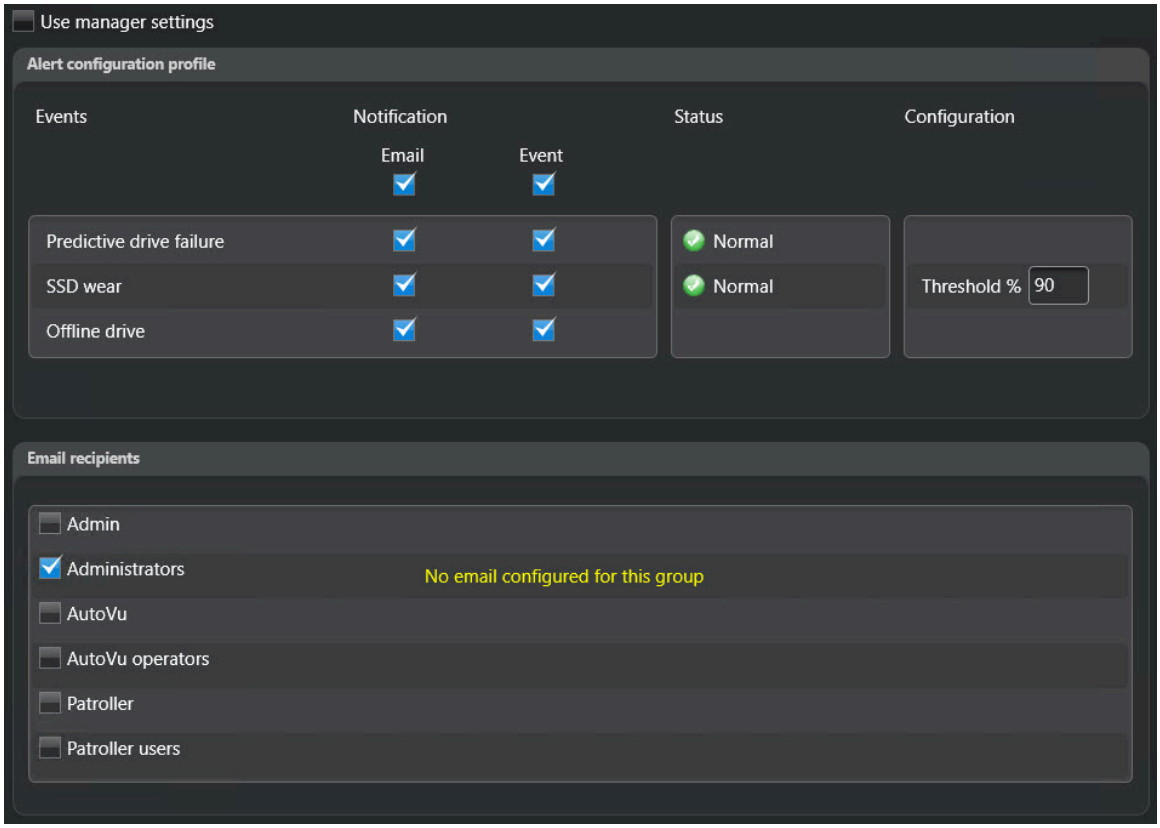
4 Select the **General** tab.

5 (Optional) If you created a Streamvault manager entity for your system, select the **Use manager settings** checkbox to use the alert configuration profile settings of the Streamvault manager.

6 In the *Alert configuration profile* section, select the checkboxes that correlate with the **Events** and **Notification** types that you want to apply to the Streamvault Maintenance plugin instances controlled by the Streamvault manager.

7 Under **Configuration**, set the wear **Threshold %** of the solid-state drive (SSD) at which you want to receive a notification to inform you to replace the SSD soon.

8 In the *Email recipients* section, choose which users and user groups receive email notifications when a condition in the *Alert configuration profile* section is met.



9 Click **Apply**.

Related Topics

About the Management tab on page 55

Configuring a Streamvault manager entity

You can configure a Streamvault™ manager entity to control the alert configurations of a group of Streamvault™ hardware monitors from a single location. You can also set up notifications to be raised when problems occur. Using the Streamvault manager entity is optional.

Before you begin

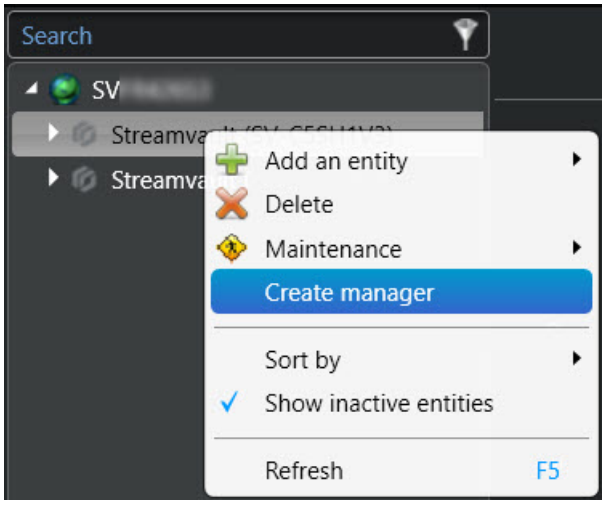
- Enroll your Streamvault™ devices.
- Create the Streamvault plugin role.

NOTE: The Streamvault manager entity can run on any Streamvault or non-Streamvault server in your Security Center system. Only one Streamvault manager entity can be added to the system.

Procedure

1 In Config Tool, navigate to the *Plugins* task and select the Streamvault plugin role.

2 Right-click the Streamvault plugin role and click **Create manager**.



3 Select the Streamvault manager entity and click the **General** tab.

The following sections are displayed:

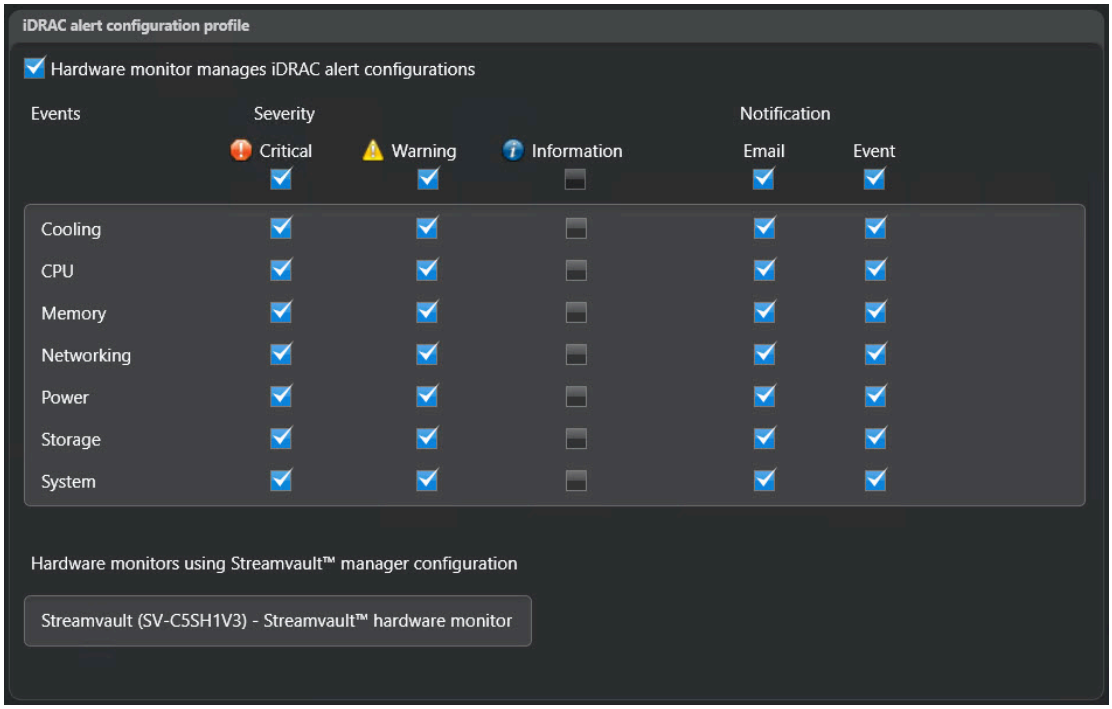
- The *iDRAC alert configuration profile* section manages iDRAC-enabled servers in your system.
- The *Non-iDRAC alert configuration profile* section is used to manage other non-iDRAC servers in the system.

Both sections are always shown, regardless of whether you have an iDRAC or non-iDRAC system.

4 (If applicable) In the *iDRAC alert configuration profile* section, configure the following:

a) To manage iDRAC alert configurations through the Streamvault hardware monitor of the selected server, select the **Hardware monitor manages iDRAC alert configurations** checkbox.

b) Select the checkboxes that correlate with the **Events**, **Severity** levels, and **Notification** types that you want to apply to the Streamvault Maintenance plugin instances controlled by the Streamvault manager.

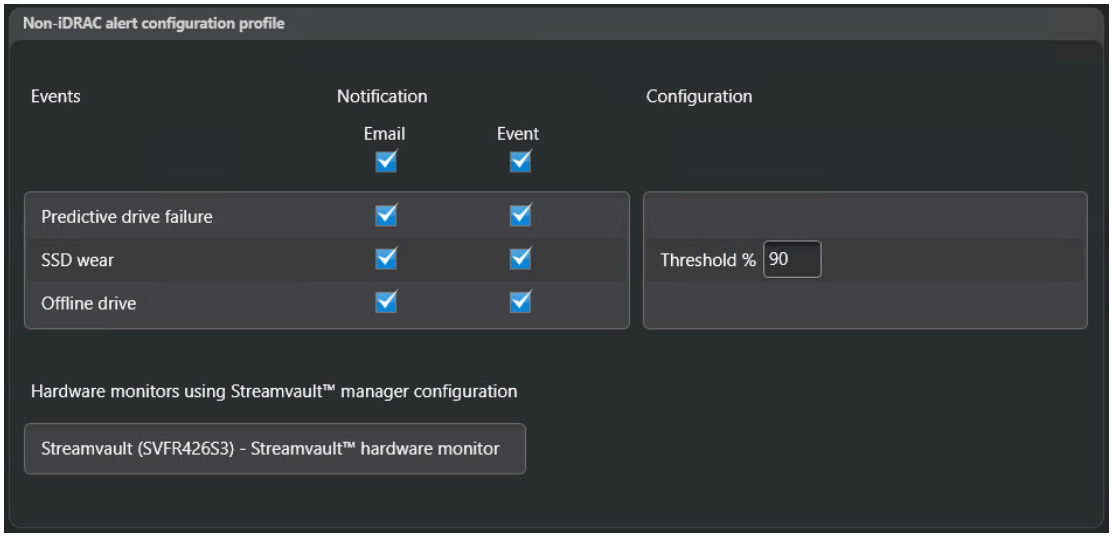


NOTE: Hardware monitors that have their configurations set by the Streamvault manager are listed under **Hardware monitors using Streamvault™ manager configuration**. Hardware monitors that use their own configurations are listed under **Hardware monitors using custom configuration**.

5 (If applicable) In the *Non-iDRAC alert configuration profile* section, configure the following:

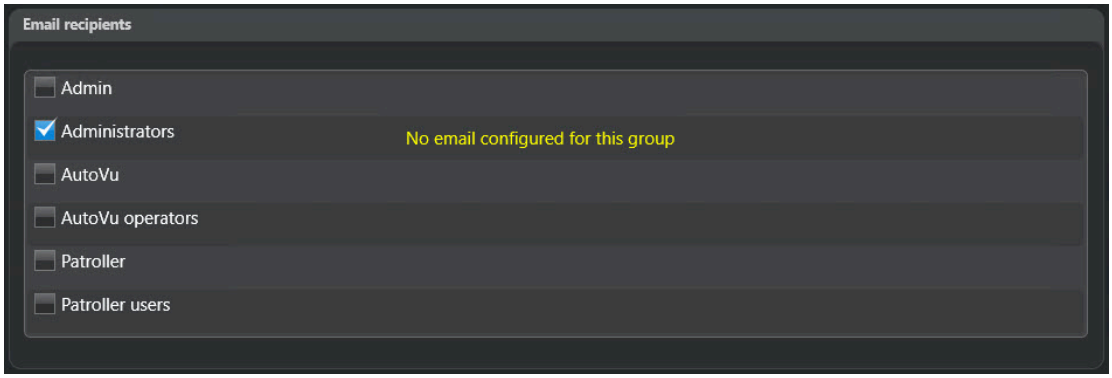
a) Select the checkboxes that correlate with the **Events** and **Notification** types that you want to apply to the Streamvault Maintenance plugin instances controlled by the Streamvault manager.

b) Under **Configuration**, set the wear **Threshold %** of the solid-state drive (SSD) at which you want to receive a notification to inform you to replace the SSD soon.



NOTE: Hardware monitors that have their configurations set by the Streamvault manager are listed under **Hardware monitors using Streamvault™ manager configuration**. Hardware monitors that use their own configurations are listed under **Hardware monitors using custom configuration**.

6 In the *Email recipients* section, choose which users and user groups receive email notifications when a condition in the **iDRAC alert configuration profile** or **Non-iDRAC alert configuration profile** section is met.



7 Click **Apply**.

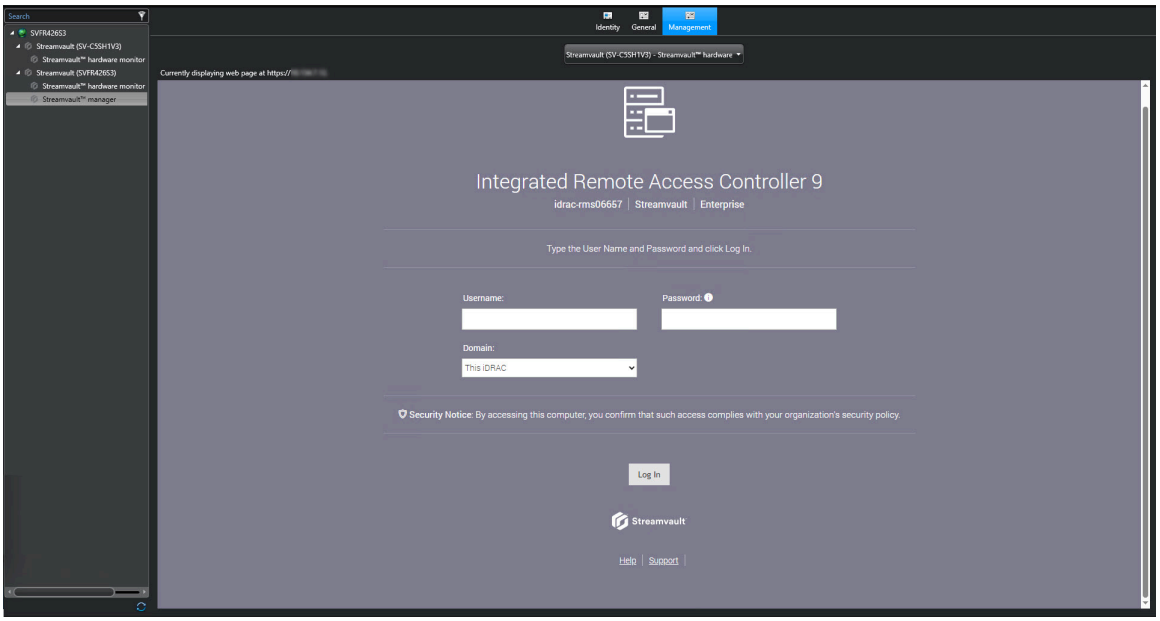
About the Management tab

The **Management** tab displays an iDRAC web page through which you can configure and manage your iDRAC server credentials. You can also find more information about your iDRAC server and configure other options that aren't available through the Streamvault™ plugin user interface.

You can access the **Management** tab through the Streamvault™ hardware monitor of any iDRAC-enabled server or through the Streamvault™ manager.

If you access the **Management** tab through the Streamvault manager, a drop-down is displayed at the top of the page. You can use it to switch from one iDRAC server to another instead of having to manually switch from one hardware monitor to another. Each iDRAC server has its own iDRAC web page.

For login information, click **Help** at the bottom of the web page.



NOTE: To access the iDRAC web page, you need a network connection between the client system that runs Config Tool and the IP address of the iDRAC server. If a network connection is unavailable, use the Config Tool page directly from the Streamvault appliance through a remote desktop or local console session.

If your system doesn't have any iDRAC servers, the **Management** tab is empty. A message states that there are no Streamvault hardware monitors with iDRAC management capabilities available.

NOTE: If the iDRAC web page doesn't load, click another tab and then go back to the **Management** tab.

Related Topics

Configuring a Streamvault hardware monitor entity on page 48
Configuring a Streamvault manager entity on page 52

Reviewing Streamvault appliance health

Use the Streamvault™ Hardware task to view a list of health issues affecting your Streamvault appliances.

Procedure

1 From the homepage, open the *Streamvault hardware* task.

2 In the **Time range** query filter, define the time period you want the report to include.

3 Click **Generate report**.
The unit properties are listed in the report pane.

Report pane columns for the Streamvault hardware task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Streamvault™ hardware task.

- **Image:** Icon representing the issue type.
- **Severity:** Level of severity associated with the issue.
- **Timestamp:** Date and time when the issue occurred.
- **Source:** Streamvault appliance affected by the issue.
- **MessageID:** Identifying alphanumeric sequence associated with the reported issue.
- **Message:** Description of the issue.
- **Description:** Description of what is causing the issue.

NOTE: For more information about creating reports, see Reporting task workspace overview on the TechDoc Hub.

Creating event-to-actions for Streamvault health events

Using an event-to-action, you can trigger actions to occur when a Streamvault™ hardware issue is detected.

Before you begin

- Create the Streamvault Maintenance plugin role.
- Configure a Streamvault hardware monitor entity.

Procedure

1 From the Config Tool homepage, click the *Automation* task and click the **Actions** view.

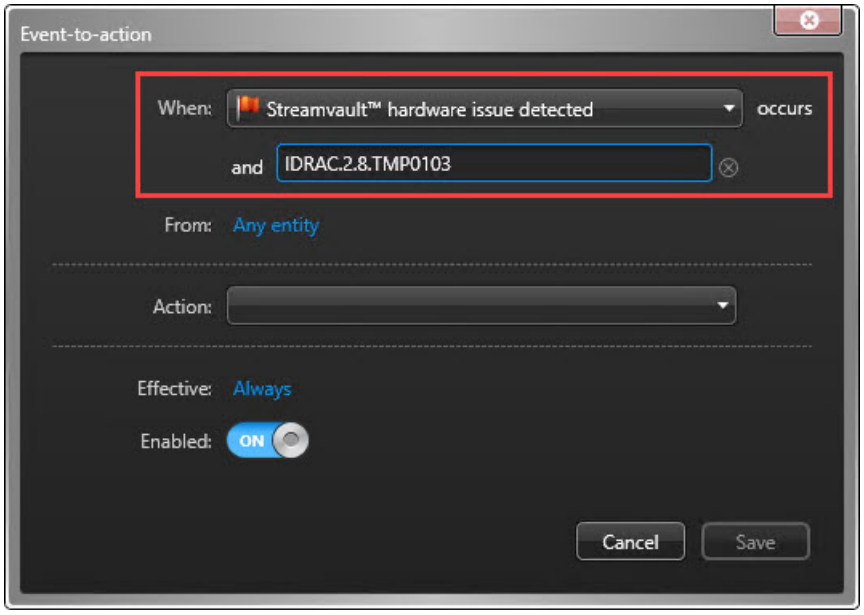
2 Click **Add an item** ( ).

3 Configure your event-to-action:

a) From the **When** drop-down, select **Streamvault hardware issue detected**.

b) Click **Specify a condition** and enter the iDRAC code error. You can also enter the full ID to prevent any false triggers.

For example, in the screenshot below, the error code is TMP0103 and the full ID is IDRAC.2.8.TMP0103.



c) (Optional) In the **From** option, select your Streamvault™ plugin or hardware monitor.

NOTE: Since the Streamvault plugin uses custom events that are meaningful only to itself, there's no need to assign a source.

If you select the Streamvault plugin as the source entity, then if the plugin role is ever deleted, all the linked automation rules are deleted. If no source entity is specified and the role is deleted, the automation rules persist.

d) From the **Action** drop-down, select an action type and configure its parameters.

e) (Optional) In the **Effective** option, click **Always**, and select a schedule when this event-to-action is active.

If the event occurs outside of the defined schedule, then the action isn't triggered.

4 Ensure the event-to-action is enabled.

5 Click **Save**.

NOTE: For a complete list of iDRAC error codes, see https://developer.dell.com/apis/2978/versions/5.xx/docs/Error%20Codes/EEMIRegistry.md.

4

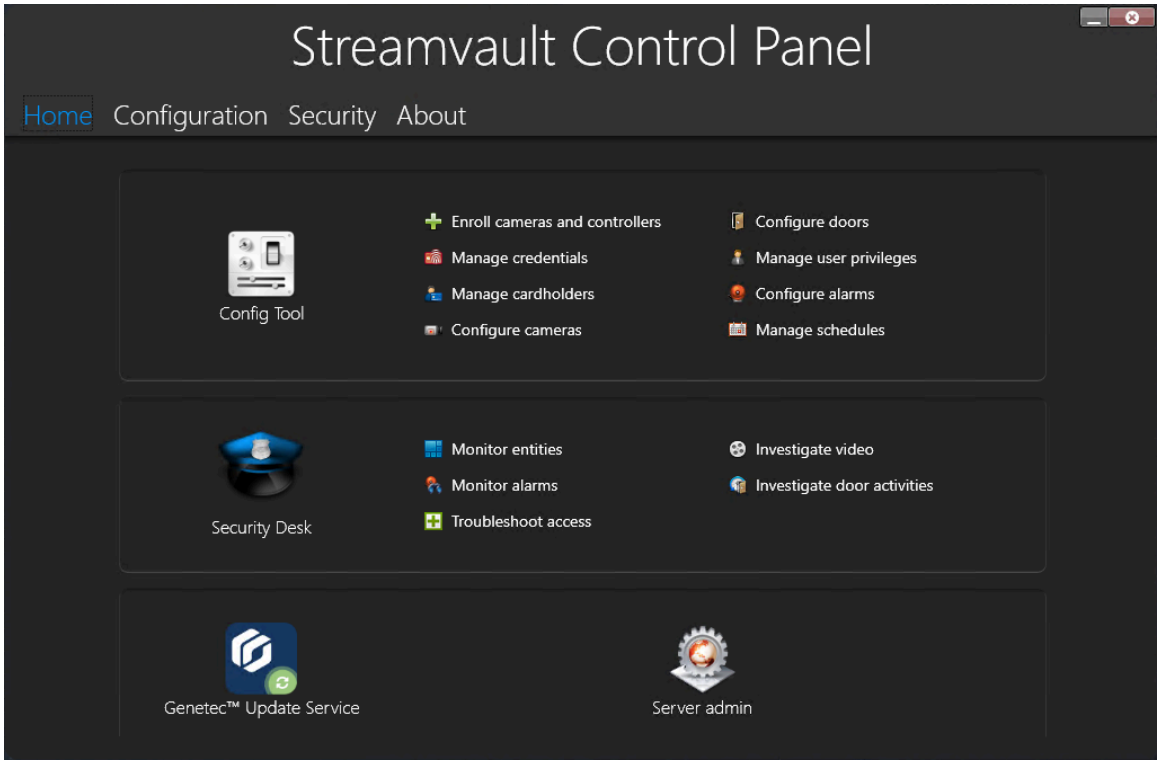
SV Control Panel reference

These reference pages help you understand the SV Control Panel.

This section includes the following topics:

Homepage of the SV Control Panel

Use the homepage of the SV Control Panel to access the basic tasks that are required to configure and use your system. You can click the interface icons to access the Config Tool, Security Desk, Server Admin, or Genetec™ Update Service applications.



Alternatively, you can click the Config Tool shortcuts or Security Desk shortcuts to open associated tasks.

For systems running in Client mode, the Server Admin shortcut is unavailable. Likewise, the Config Tool and Security Desk shortcuts are limited.

NOTE: Note: If your system isn't activated, a red banner appears to notify you. Click **The system is not activated. Click here to activate it.** to open the Streamvault™ Control Panel activation wizard.

Config Tool shortcuts

Use the shortcuts to open the main tasks in the Config Tool application. The shortcuts that are available depend on the license options that you have.

Shortcut	Action
Config Tool	Opens Config Tool.
Enroll cameras and controllers	Opens the Unit enrollment tool, where you can enroll your cameras and controllers.
Manage credentials	Opens the *Credential management* task, where you can manage user credentials.
Manage cardholders	Opens the *Cardholder management* task, where you can manage cardholders.
Configure cameras	Opens the *Video* task, where you can add and manage cameras.

Shortcut	Action
Configure doors	Opens the *Area view* task, where you can add and manage doors.
Manage user privileges	Opens the *User management* task, where you can add and manage user privileges.
Configure alarms	Opens the *Alarms* task, where you can configure alarms.
Manage schedules	Opens the *System* task, where you can create and manage schedules.

Security Desk shortcuts

Use the shortcuts to open the main tasks in the Security Desk application. The shortcuts that are available depend on the license options that you have.

Shortcut	Action
Security Desk	Opens Security Desk.
Monitor entities	Opens the *Monitoring* task, where you can monitor system events in real-time.
Monitor alarms	Opens the *Alarm monitoring* task, where you can monitor and respond to active alarms, and view past alarms.
Troubleshoot access	Opens the Access troubleshooter tool, which allows you to diagnose and access configuration problems. **NOTE:** This shortcut is unavailable for systems running in Client mode.
Investigate video	Opens the *Archives* task, where you can search for video archives. **NOTE:** This shortcut is unavailable for systems running in Client mode.
Investigate door activities	Opens the *Door activities* task, where you can investigate events at selected doors. **NOTE:** This shortcut is unavailable for systems running in Client mode.

Genetec Update Service shortcut

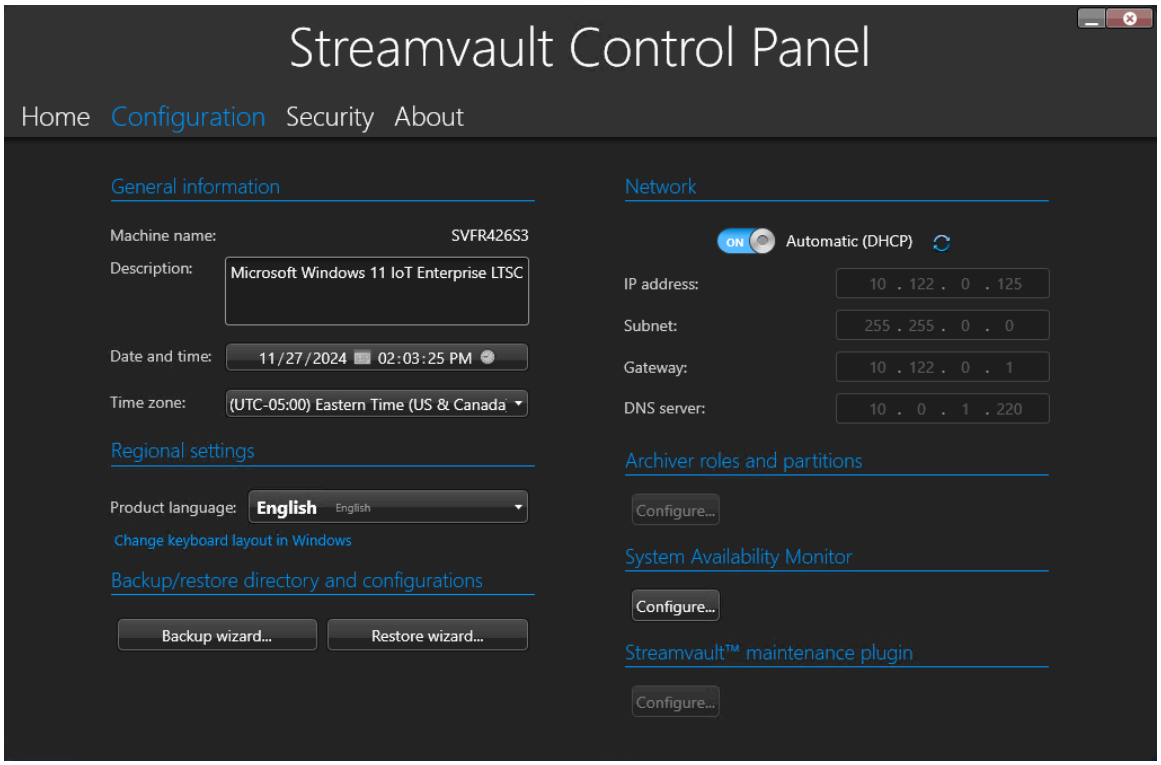
Use the Genetec Update Service to help ensure that the software components on your appliance are up to date.

Server Admin shortcut

Use the Server Admin application to manually apply a license, or view and change the configuration of the server.

Configuration page of the SV Control Panel

Use the *Configuration* page of the Streamvault™ Control Panel to modify general settings such as the *regional settings*, *network settings*, and *System Availability Monitor settings*.



For systems running on an expansion server or in Client mode, the *System Availability Monitor* and *Backup/restore directory and configurations* sections are unavailable.

General information settings

Use the *General information* section to change general settings, such as the name of your Streamvault appliance.

- **Machine name:** Displays the name of the SV machine.
- **Description:** Enter a meaningful description to help identify the machine.
- **Date and time:** Click in the field to configure the date and time values displayed on the machine. Alternatively, you can click the calendar or clock icon in the field to configure the settings.
- **Time zone:** Select a time zone from the drop-down.

Regional settings

Use the *Regional settings* section to change the language settings of your system keyboard layout.

- **Product language:** Select a language from the list to change the language of Config Tool and Security Desk.

  IMPORTANT: For changes to take effect, you must restart your Security Center applications.
- **Change keyboard layout in Windows:** Click this option to open the Windows *Language & region* settings page to change the layout of your keyboard.

  IMPORTANT: For changes to take effect, you must restart your computer.

NOTE: The SV Control Panel is available in English, French, and Spanish.

Backup and restore

Use the *Backup/Restore Directory and configurations* section to access the *Backup* wizard and *Restore* wizard.

Backup and restore is an SV Control Panel feature. It allows you to securely back up your Directory database and configuration files, and later restore them to the same System ID. Backup and restore can be used in the event of a system failure or hardware upgrade. This feature doesn't back up your license file, video archives, or other databases.

This section is unavailable for systems running on an expansion server or in Client mode.

- **Backup wizard:** Click **Backup wizard** to create a backup of your Directory database and configuration files.
- **Restore Wizard:** Click **Restore Wizard** to restore a backup of your Directory database and configuration files to your system.

IMPORTANT: You need to open the required port to ensure that the *Backup/Restore Directory and configurations* feature can communicate with the SV Control Panel. For more information, see Default ports used by Streamvault on page 4.

Network settings

Use the *Network* section to change network settings such as the IP address of your Streamvault appliance.

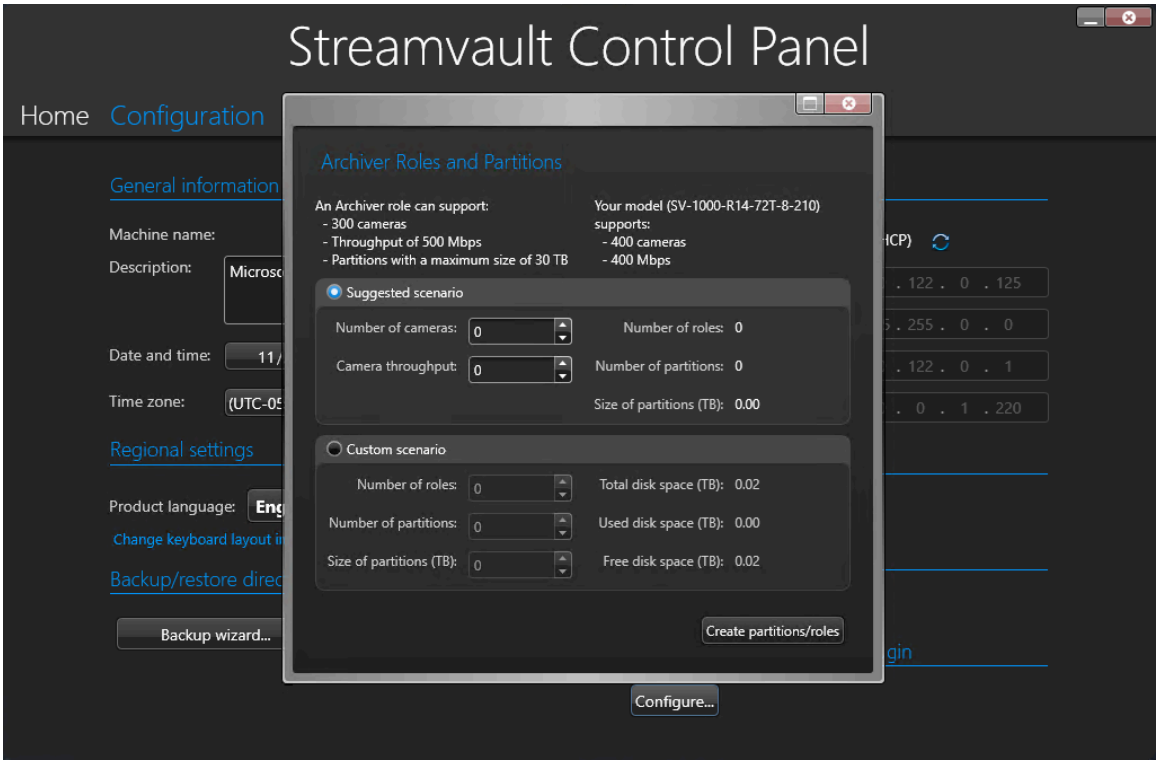
- **Automatic (DHCP):** By default, Dynamic Host Configuration Protocol (DHCP) is used to automatically assign the IP address, Subnet, Gateway, and DNS server. Turn this option off if you don't want the IP address assigned dynamically by your DHCP server.

  Click **Refresh** () to refresh your DHCP settings and obtain a new IP address.
- **IP address:** The IP address of the machine.
- **Subnet:** The subnet mask of the machine.
- **Gateway:** The IP address of the gateway.
- **DNS server:** The IP address of the DNS server.

Archiver roles and partitions

Use the *Archiver roles and partitions* section to configure systems that require more than the maximum number of cameras and throughput supported by a single Archiver.

This section is available for systems running Security Center 5.9 and later on an expansion server.



- **An Archiver role can support:** Displays the maximum number of cameras, amount of throughput, and partition size supported by a single Archiver role.
- **Your model supports:** Displays the maximum number of cameras and amount of throughput supported by your Streamvault appliance model.
- **Suggested scenario:** Automatically calculates the number of roles, partitions, and partition size needed for your desired number of cameras and throughput.
- **Custom scenario:** Choose the number of roles, partitions, partition size desired for your systems configuration.

For more information on using this feature, see Adding Archiver roles in the SV Control Panel on page 39.

System Availability Monitor settings

Use the *System Availability Monitor* section to configure the settings for the System Availability Monitor Agent on your Streamvault appliance. For example, setting the data collection method and activating the Agent.

You can also check the following:

- If the appliance is communicating with Security Center
- When the last check point occurred
- What recent errors and warnings were reported in the Applications and Services logs

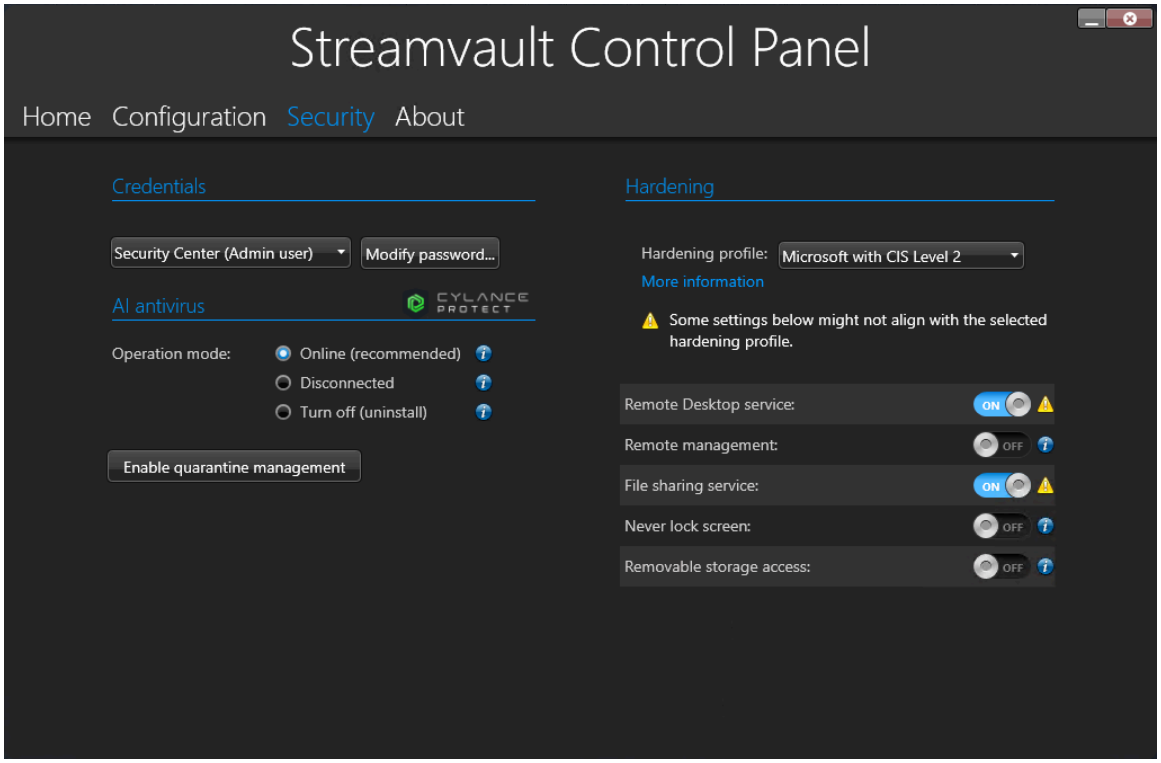
This section is unavailable for systems running on an expansion server or in Client mode.

Streamvault Maintenance plugin settings

Use the *Streamvault maintenance plugin* section to enroll the plugin in Security Center, if it hasn't already been enrolled.

Security page of the SV Control Panel

Use the *Security* page to modify user passwords, choose the communication mode between the CylancePROTECT Agent and Genetec™, and apply hardening profiles and system security settings to your Streamvault™ appliance.



Password settings

Use the *Credentials* section of the *Security* page to change user account passwords for your Streamvault appliance.

NOTE: Different password options are available to the current user on both a main and expansion server. On an expansion server, the admin can only change the Windows passwords, not the passwords of the Security Center applications.

Define a password for each user type:

- **Security Center (Admin user):** The admin user's password for Security Desk, Config Tool, and Genetec™ Update Service.
- **Server Admin:** The password for the Genetec™ Server Admin application.
- **Windows operator:** Click **Modify password** to change the operator's password for Windows.

Antivirus settings

Use the *AI antivirus* section to choose the mode in which the CylancePROTECT Agent communicates with Genetec.

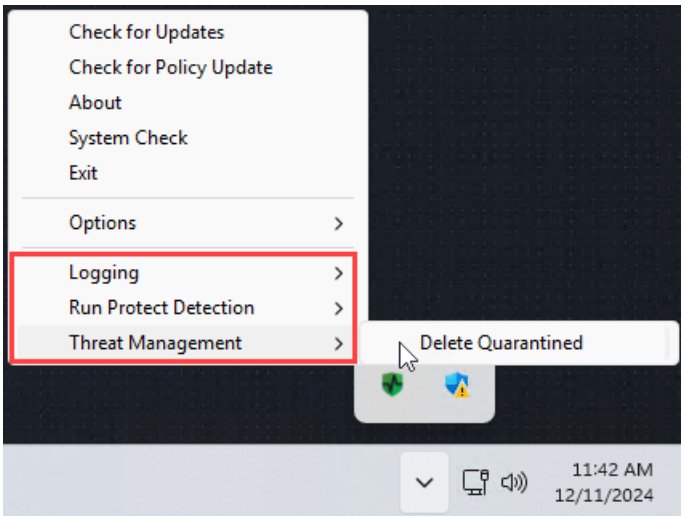
CylancePROTECT is the AI-powered antivirus software used for threat protection and detection.

You can choose from the following operation modes:

- **Online (recommended):** When online, the CylancePROTECT Agent communicates with Genetec to report new threats, update its agent, and send data to help improve its mathematical models. This option offers the highest level of protection.
- **Disconnected:** The disconnected mode is for an appliance without an internet connection. In this mode, CylancePROTECT cannot connect or send information to Genetec management services in the cloud. Your appliance is protected against most threats. Maintenance and updates are available through the Genetec™ Update Service (GUS).
- **Turn off:** Select this mode to permanently uninstall CylancePROTECT from your appliance. Your appliance will use Microsoft Defender for threat protection and detection. We do not recommend turning off CylancePROTECT if the appliance cannot receive virus definition updates for Microsoft Defender.

CAUTION: Switching between options may require a computer reboot, causing downtime for the system.

Click **Enable quarantine management** to add **Threat Management** to the right-click menu of the Cylance icon in the Windows taskbar. This option allows you to delete quarantined items. **Logging** and **Run Protect Detection** are also added to the right-click menu. These options allow you to access logs and trigger scans, respectively.



Hardening settings

Use the *Hardening* section to choose a hardening profile and set system security settings for your Streamvault appliance.

NOTE: The hardening profiles are available only on appliances that have the *Streamvault service*. For more information, see About the Streamvault service on page 15.

There are four predefined hardening profiles:

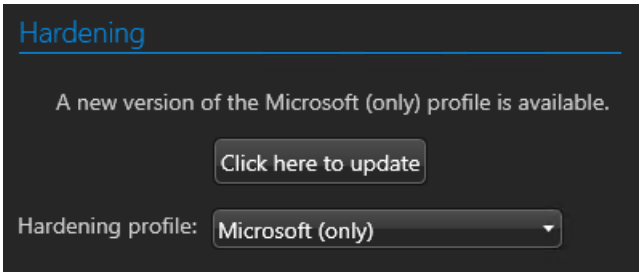
- **Microsoft (only):** This hardening profile applies Microsoft security baselines to your system. Microsoft security baselines are a group of Microsoft-recommended configuration settings that are based on feedback from Microsoft security engineering teams, product groups, partners, and customers.
- **Microsoft with CIS Level 1:** This hardening profile applies Microsoft security baselines and the Center for Internet Security (CIS) Level 1 (CIS L1) profile to your system. The CIS L1 provides essential security requirements that can be implemented on any system with little or no performance impact or reduced functionality.
- **Microsoft with CIS Level 2:** This hardening profile applies Microsoft security baselines and the CIS L1 and Level 2 (L2) profiles to your system. The CIS L2 profile offers the highest level of security and is intended for organizations where security is of utmost importance.

  NOTE: The strict security that this hardening profile brings can reduce system functionality and make remote server management more difficult.

- **Microsoft with STIG:** This hardening profile applies Microsoft security baselines and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) to your system. DISA STIGs are based on National Institute of Standards and Technology (NIST) standards and provide advanced security protection for Windows systems for the U.S. Department of Defense.

NOTE: By default, all appliances are shipped with the Microsoft with CIS Level 2 hardening profile applied.

When a new version of your selected hardening profile is available, a **Click here to update** button appears. Click the button to apply the update.



In addition to the hardening profiles, the following system security settings can be set:

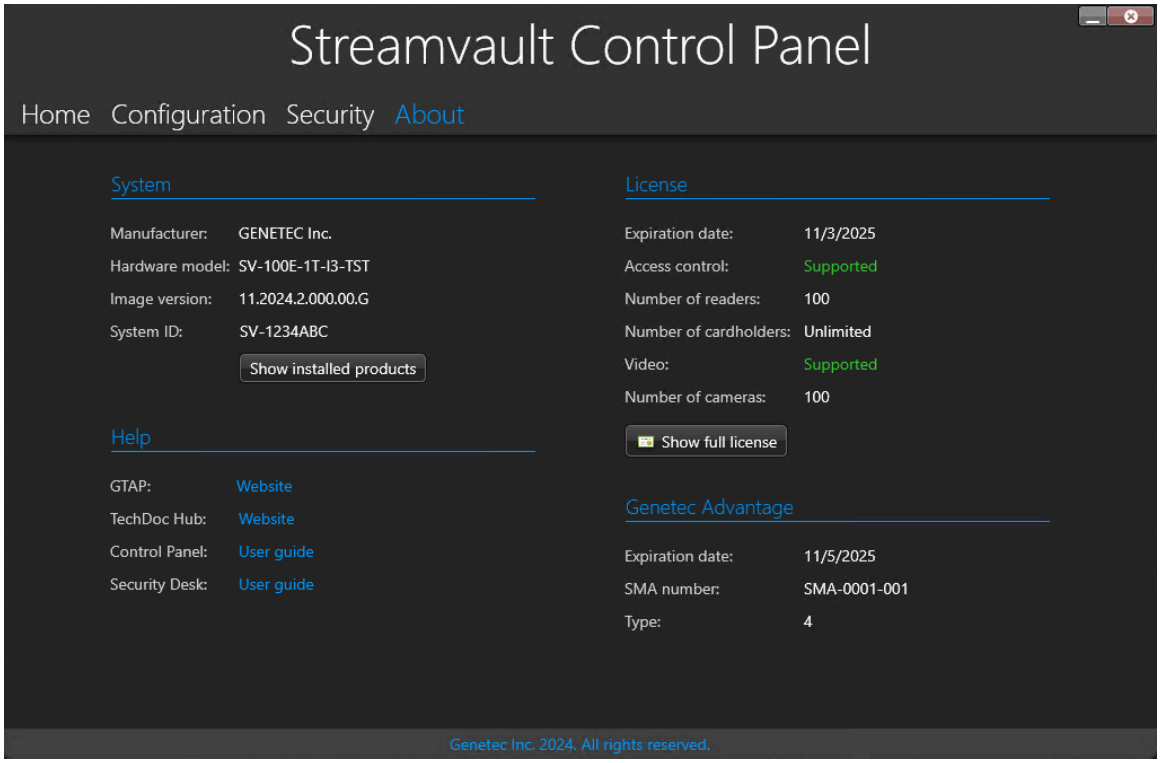
- **Remote Desktop service:** Allow people in your network to log on to the appliance by using a *Remote Desktop* application. To prevent malicious software from affecting the device, this option has been turned off by default.
- **Remote management:** Enable remote support for Microsoft management tools such as Windows Admin Center, Microsoft Server Manager, and Remote PowerShell.
- **File sharing service:** Allow people in your network to share files and folders that are on the appliance. To prevent malicious software from affecting the device, this option has been turned off by default.
- **Never lock screen:** If this option is turned on, Windows will keep a user logged in, even after 15 minutes of inactivity.
- **Removable storage access:** Enable access to a connected USB key or USB hard disk from Windows.

  NOTE: Users with administrative privileges automatically have removable storage access.

About page of the SV Control Panel

Use the *About* page to view useful information if you require assistance with your Streamvault™ appliance. The *About* page includes system information, links to the Genetec™ Technical Assistance Portal (GTAP) and product documentation, license information, and Software Maintenance Agreement (SMA) information.

For systems that run on an expansion server or are in Client mode, only the *System* and *Help* sections are available.



System information

Use the *System* section to view information about the system.

- **Manufacturer:** Displays the hardware manufacturer.
- **Hardware model:** Displays the hardware model.
- **Image version:** Displays the software image version.
- **System ID:** Displays the system ID number.
- **Show installed products:** Click to display the software version of the Genetec components installed on the appliance.

Help information

Use the *Help* section to access useful links to the GTAP and product documentation.

- **GTAP:** Click the link to open GTAP and support forums.
  NOTE: You must have a valid username and password to sign in to GTAP.
- **TechDoc Hub:** Click the link to open the Genetec TechDoc Hub.
- **Control Panel:** Click the link to open the *Streamvault Appliance User Guide*, which contains SV Control Panel information.
- **Security Desk:** Click the link to open the *Security Center User Guide*.

License information

Use the *License* section to view information about the license. The information that is displayed varies depending on your license options.

- **Expiration date:** Displays when your Security Center license expires.
- **Access control:** Displays whether or not access control features are supported.
- **Number of readers:** Displays how many readers are supported on your system.
- **Number of cardholders:** Displays how many cardholders are supported on your system.
- **Video:** Displays whether or not video features are supported.
- **Number of cameras:** Displays how many cameras are supported on your system.
- **Show full license:** Click to display more license information.

This section is unavailable for systems running on an expansion server or in Client mode.

Genetec Advantage information

Use the *Genetec Advantage* section to view information about the SMA.

- **Expiration date:** Displays the expiration date of the Software Maintenance Agreement.
- **SMA number:** Display the SMA number.
- **Type:** Displays the SMA type.

This section is unavailable for systems running on an expansion server or in Client mode.

5

Additional resources

This section includes the following topics:

Product warranty for your Streamvault appliance

Your Streamvault™ appliance is covered by a 3-year standard hardware and software warranty, with an optional 2-year extension.

For a detailed description of the terms and conditions of the Genetec™ product warranty, refer to the Genetec™ Product Warranty Overview.

Re-imaging a Streamvault appliance

To re-image a Streamvault™ appliance, you need its Microsoft Certificate of Authenticity (COA) to determine which image can be used with the appliance. Each Streamvault appliance has a COA label affixed to it, which indicates the edition of Windows running on the appliance.

Refer to the Streamvault Release Notes for a list of images that are compatible with your appliance, based on its Windows edition. Do not use your software image if your appliance runs a different edition of Windows than the one indicated in the release notes.

The following is an example of a typical COA label with Windows edition and certificate information stamped. Products that contain embedded versions of Microsoft software have a COA label.

NOTE: Each Streamvault image is designed to work with its respective version of Security Center, as indicated in the Streamvault Release Notes. Downgrading Security Center to an earlier version might require reducing the hardening level of the appliance.

For an overview of product availability, support, and available services, see the Product Lifecycle page on GTAP.

Finding the system ID and image version of a Streamvault appliance

When contacting the Genetec™ Technical Assistance Center (GTAC), you need the System ID and the image version of the Genetec™ software installed on the appliance.

Before you begin

Log on to Windows as Administrator.

What you should know

In addition to the system ID and image version, GTAC might request the certification number and serial number. To find this information, look for a label on the Streamvault™ appliance.

Procedure

1 From the Windows desktop, open **Genetec™ SV Control Panel**.

2 If prompted, enter the password for the Admin user.

3 Click **About**.

4 In the *System* section, take note of the **System ID** and **Image version**.

Related Topics

Performing a factory reset on a Streamvault All-in-one appliance on page 78
Performing a factory reset on a Streamvault workstation or server appliance on page 87

Allowing file sharing on a Streamvault appliance

To share the files and folders on your appliance with people in your network, you must enable file sharing in the SV Control Panel.

Before you begin

On the appliance, log on to Windows as the Admin user.

What you should know

- For maximum security, file sharing is disabled by default.
- The remote computers and your appliance must be connected to the same IP network.

Procedure

1 On the *Security* page of the SV Control Panel, turn on the **File sharing service** option.

2 Click **Apply**.

3 To share a folder or file with people, right-click a folder or a file in Windows File Explorer and click **Share**.

Allowing Remote Desktop connections to a Streamvault appliance

To control an appliance from any computer or virtual machine on the network, you must first enable remote access on the appliance.

Before you begin

On the appliance, log on to Windows as the Admin user.

What you should know

- For maximum security, remote access is disabled by default.
- The appliance and remote computer must be connected to the same network.

Procedure

1 On the *Security* page of the SV Control Panel, turn on the **Remote Desktop service** option.

2 Click **Apply**.

Related Topics

Remote Desktop can’t connect to a Streamvault appliance on page 95

6

Troubleshooting

This section includes the following topics:

Performing a factory reset on a Streamvault All-in-one appliance

If the software on a Streamvault™ All-in-one appliance fails to start or stops working as expected, you can perform a factory reset using a USB key.

Before you begin

- Back up your Directly database in the SV Control Panel
- Have the correct license for the version of Security Center you want to restore or install.
- Have the System ID and password that was sent by email when you purchased the appliance. See Finding the system ID and image version of a Streamvault appliance on page 74.
- (Recommended) Connect your appliance to the internet using a wired Ethernet connection so that the system can validate connectivity.

  NOTE: The validation fails if no internet connection is available, but you can continue to use your appliance.

What you should know

A factory reset deletes and overwrites all data currently on the Windows drive (C:), including databases and logs. Video files on other drives aren't affected.

Procedure

1 Create a factory reset USB key that contains the software image.

2 Using the USB key, reset the image on your appliance.

After you finish

Reconfigure your appliance.

Related Topics

Finding the system ID and image version of a Streamvault appliance on page 74

Creating a factory reset USB key for a Streamvault All-in-one appliance

Before you can reset the image of a Streamvault™ All-in-one appliance, you must prepare a bootable USB key that contains the required Streamvault software image.

Before you begin

- Get a USB key with at least 32 GB of storage. Some USB keys are unable to boot the image; if this occurs, try using a different brand or model of key.

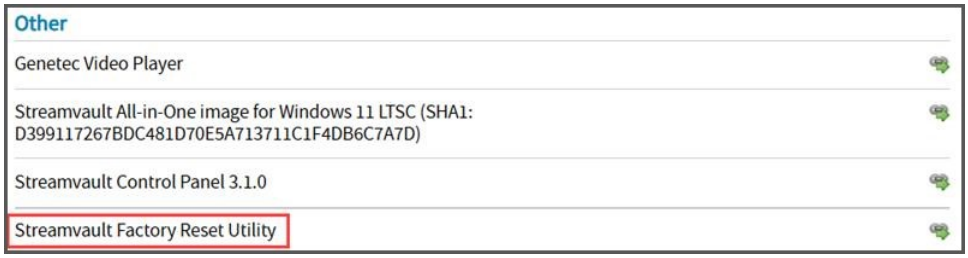
  CAUTION: All data on the USB key is deleted when you create a bootable drive.

Procedure

1 Contact Genetec™ Technical Assistance Center (GTAC) to get the recovery image.
The recovery image comes in one of the following three formats:
- A *.zip* file containing *.swm* files.
- A *.iso* file containing the *.swm* files and the *Streamvault factory reset utility* user interface, which you'll use to reset the software image.
- A *.iso* file containing the *Windows Setup* wizard, which you'll use to reset the software image.

2 If your recovery image is a *.zip* file, unzip the contents into any Windows folder.

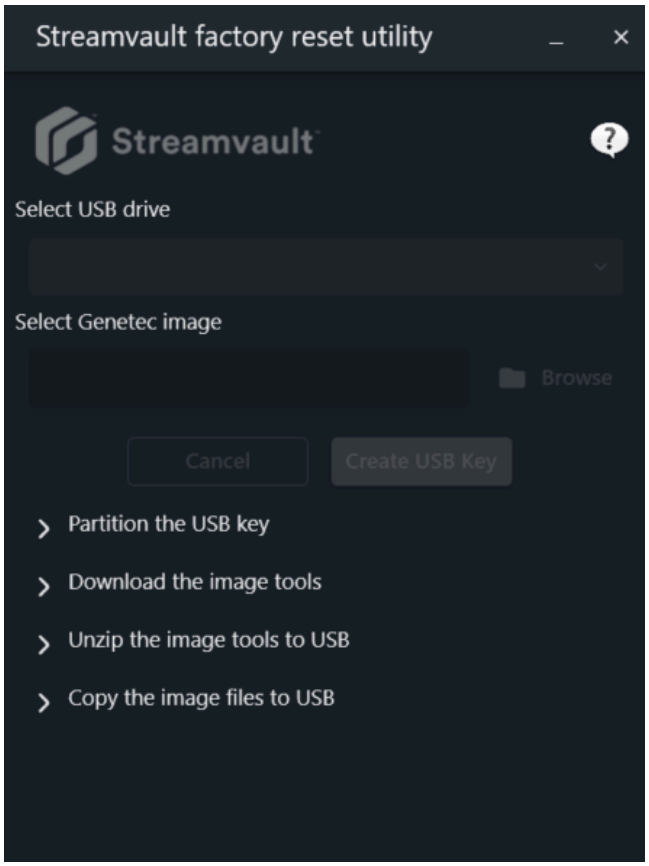
3 From the Product Download page on GTAP, download the *Streamvault factory reset utility* USB creator.
a) From the *Download Finder* list, select your version of Security Center.
b) From the *Other* list, download the *Streamvault Factory Reset Utility* package.



4 Insert the USB key into a USB port.

5 Open the *Streamvault factory reset utility* USB creator that you downloaded from the TechDoc Hub.

6 From the **Select USB drive** list, select a USB key that has at least 32 GB of storage.



7 In the *Select Genetec image* section, click **Browse** and select the *.swm* or *.iso* file you downloaded.
If you require a *.swm* file, select any one of the unzipped files from the *wim* folder.

8 Click **Create USB Key**.

The *Streamvault factory reset utility* starts to partition the USB key, download the image tools, and copy the image files.

When the download is complete, the following message is displayed: The USB key was created successfully.

Example

The following video shows you how to create a factory reset USB key with *.swm* files.

After you finish

Choose from the following:

- Reset the software image of your Streamvault All-in-one appliance.
- Reset the software image of your Streamvault workstation or server appliance.

Resetting the software image on an All-in-one appliance

After you have prepared a bootable USB key that has the required Streamvault™ software image, you can use it to reset the software image on a Streamvault All-in-one appliance.

Before you begin

- Make sure you have the USB key that contains the recovery software for your appliance.

What you should know

- Resetting takes approximately 20 - 30 minutes, during which several scripts run and the appliance restarts several times.
- Do not interrupt the reset process. Closing or shutting down the appliance manually might corrupt the recovery.

Procedure

To reset the software image:

1 Shut down the appliance.

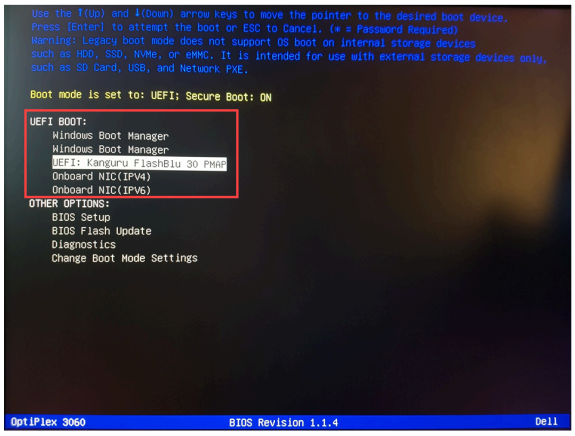
2 Insert the USB key that you created into a USB port.

3 Power on the appliance and press F12 repeatedly until the boot menu appears.

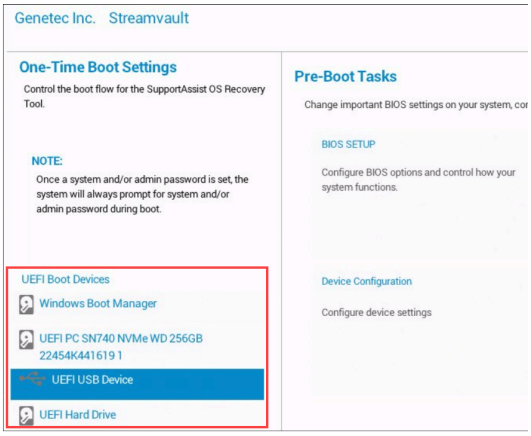
Depending on your appliance, either the UEFI Boot menu or the Streamvault One-time Boot menu opens.

4 Select the USB drive and press Enter.

NOTE: The look and feel of your boot menu might look different.



UEFI Boot menu



Streamvault One-time Boot menu

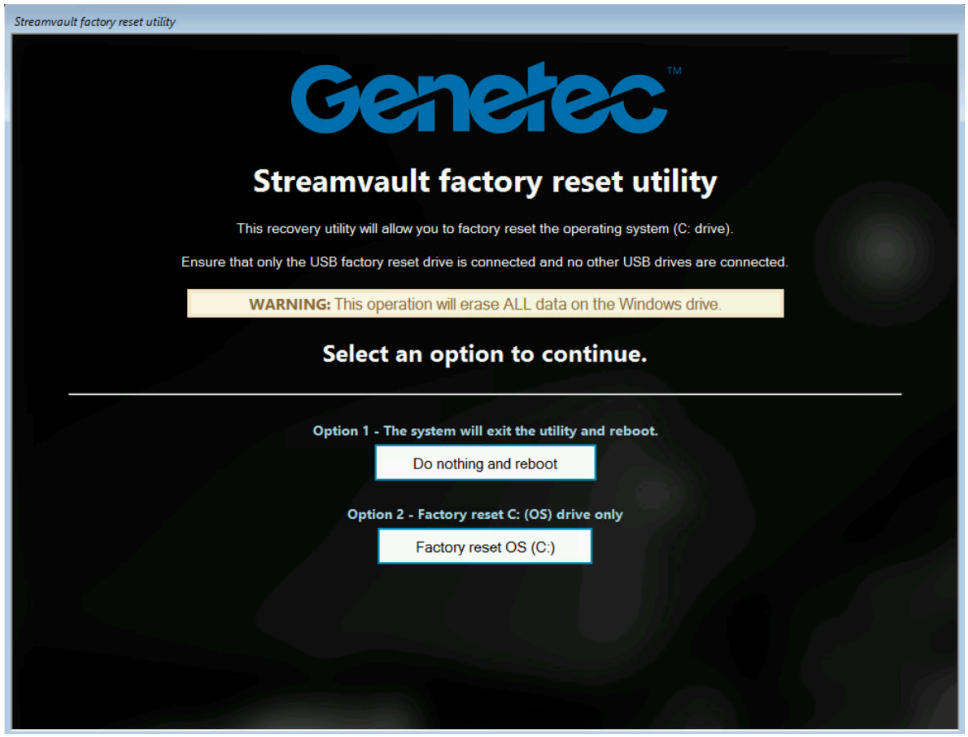
Depending on the software image, either the *Streamvault factory reset utility* or *Windows Setup* wizard opens.

5 Reset the software image using the tool that applies to your appliance:

- *Streamvault factory reset utility*
- *Windows Setup* wizard

To reset the software image using the Streamvault factory reset utility:

1 When the USB boots in recovery mode, select **Factory reset OS (C:)** to format and reinstall the appliance system drive.



2 When prompted, type `Yes` and press Enter. Wait for the factory reset to complete.

3 When the factory reset is complete, remove the USB key from the appliance, and press Enter to reboot.

4 In the *Genetec™ Product Validator* dialog box, enter the appliance's part number (Product No.) and Genetec™ serial number.

These numbers can be found on the Genetec label located on the top of the appliance. If there's no label, you can enter any text to continue.

The **Start** button appears.

5 Click **Start**.

One of the following status messages is displayed:

- **PASS:** The process was successful. Proceed to the next step.
- **PASS - No Transmission:** The process was successful; however, an internet connection wasn't available at the time. Proceed to the next step.
- **FAIL:** The process was unsuccessful. Contact the Genetec™ Technical Assistance Center (GTAC).

6 If you receive a PASS or PASS - No transmission message, close the *Genetec™ Product Validator* window.

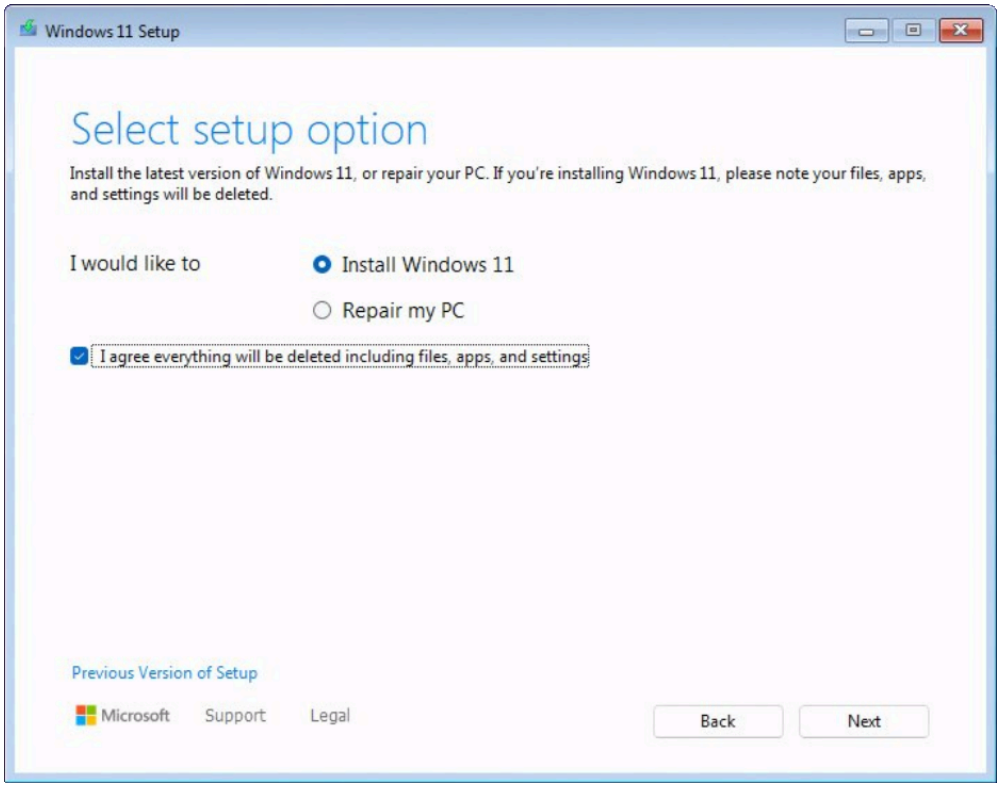
7 Wait for the background script to close, and then restart the appliance.

To reset the software image using the Windows Setup wizard:

1 On the *Select language settings* screen, select your preferred language and time settings and click **Next**.

2 On the *Select keyboard settings* screen, select your preferred keyboard and click **Next**.

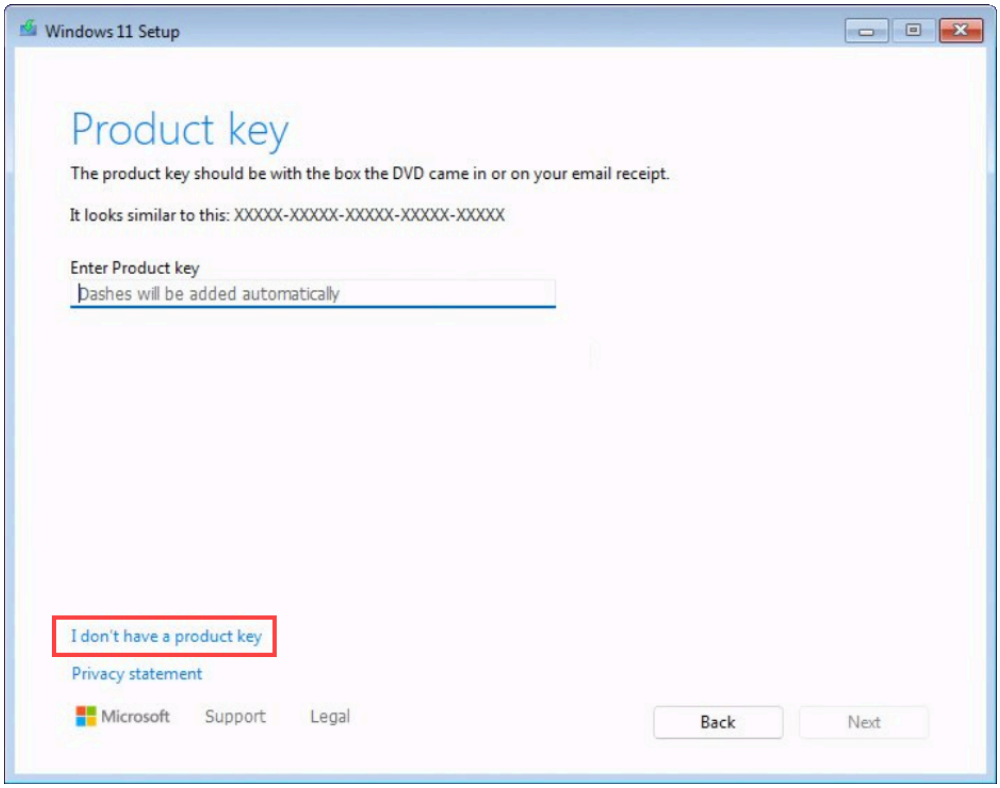
3 On the *Select setup option* screen, select **Install Windows X**, where X stands for the Windows version you're installing. Acknowledge that your files, apps, and settings will be deleted and click **Next**.



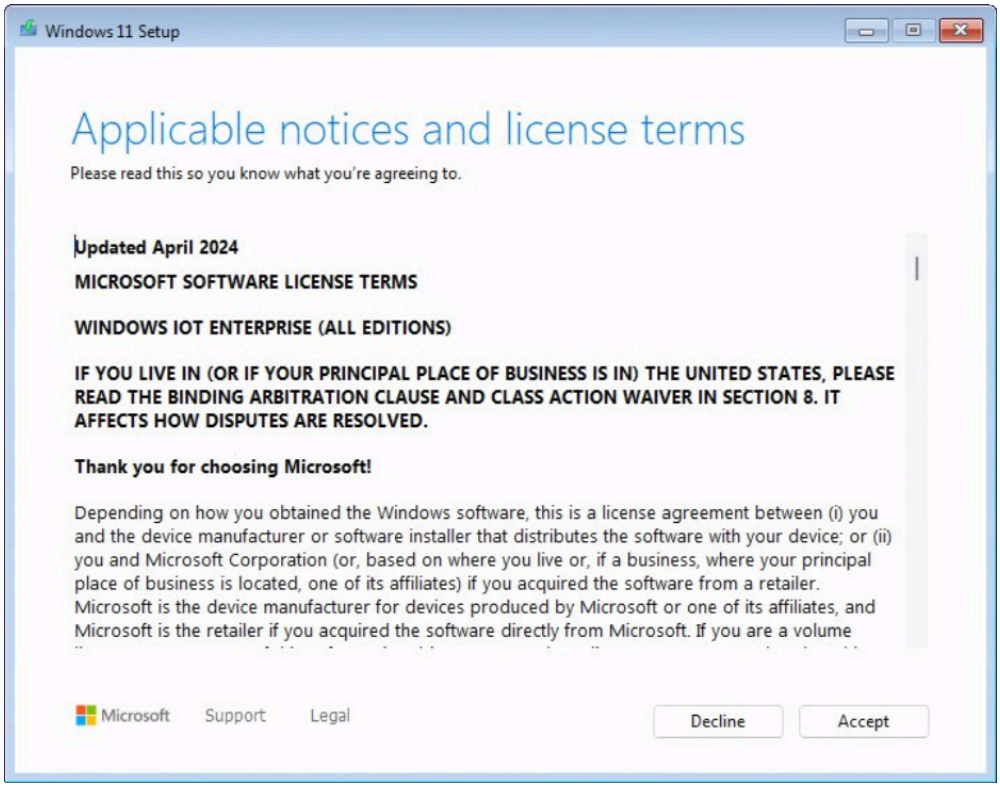
NOTE: The video archives stored on the secondary video disk aren't affected. Only the files on the OS disk are deleted.

4 On the *Product key* screen, do one of the following:

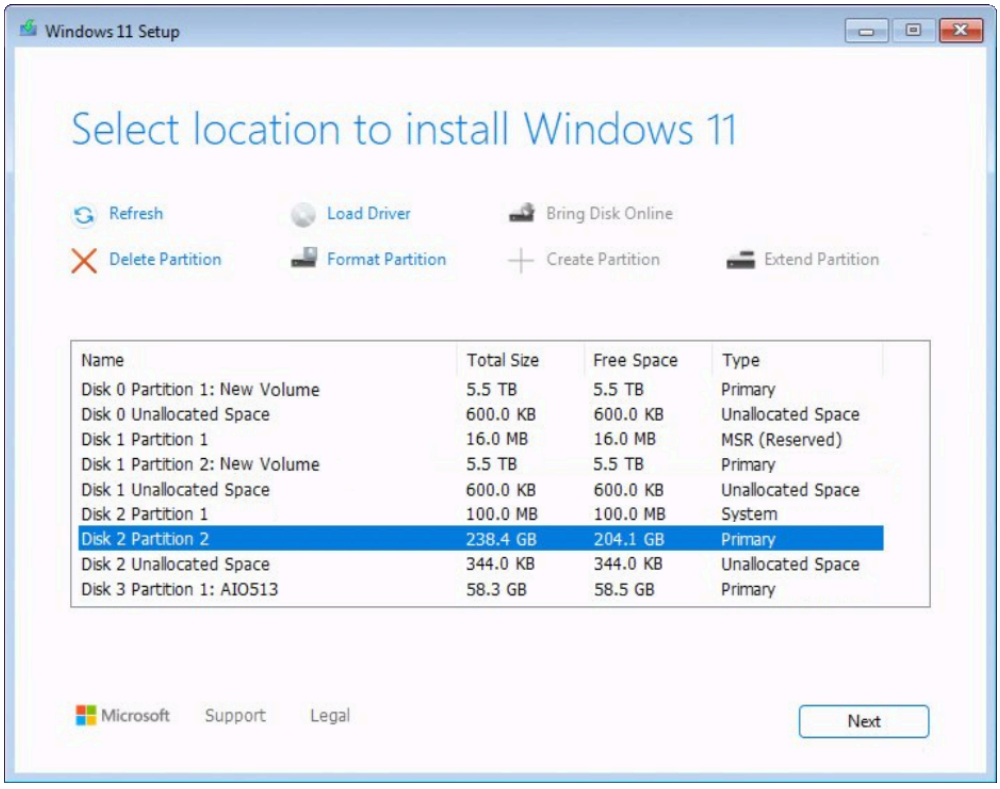
- If the appliance is connected to the internet, click **I don't have a product key** to continue. The appliance automatically retrieves its activation data from Microsoft.
- If the appliance isn't connected to the internet, enter the license key that is located on the Certificate of Authenticity (COA) label affixed on your appliance and click **Next**.



5 On the *Applicable notices and license terms* screen, read the license terms and click **Accept**.

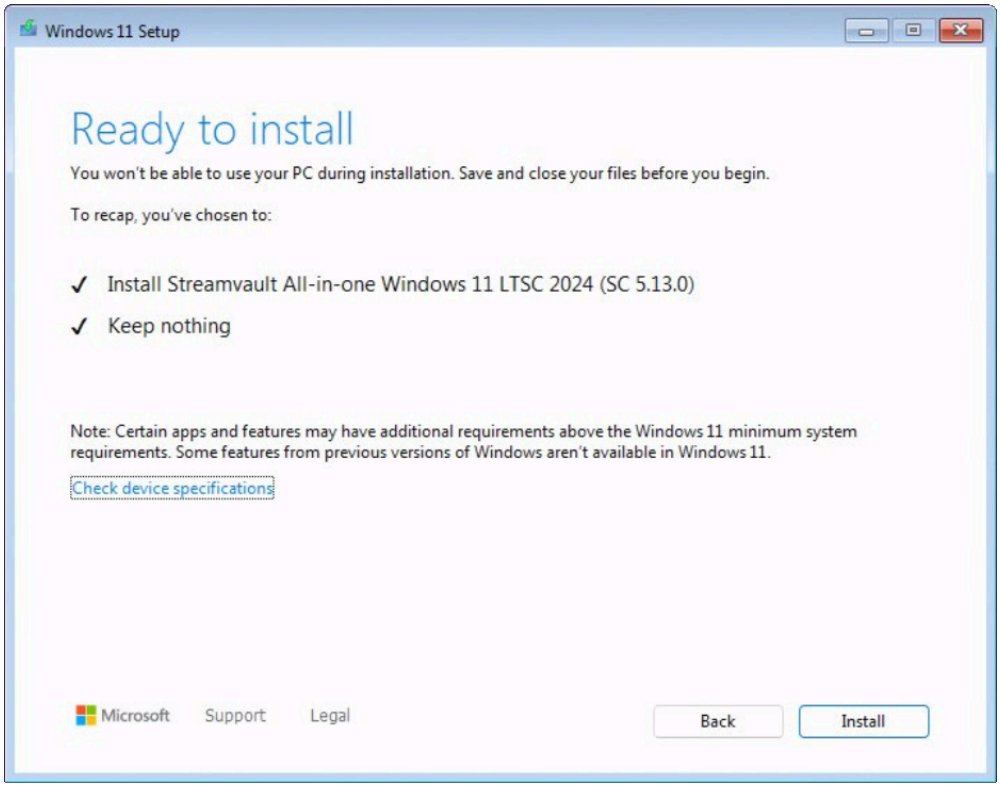


6 On the *Select location to install Windows X* screen, select the *Primary* partition on your OS disk. This partition is typically less than 1 TB in size. Click **Next**.



CAUTION: Do not select the primary partition of the video storage disk, as you'll overwrite all of your video storage.

7 On the *Ready to install* screen, click **Install**.



8 When the installation is complete, the system reboots to Windows and a script automatically runs to finalize the installation. When the script has finished running, restart the appliance.

Example

Watch this video to learn how to reset the software image on an all-in-one appliance using a bootable USB containing *.swm* files.

After you finish

- Log on to Windows using the default username and password that are on the sticker adhered to the appliance.
- Activate your Security Center license.
- If you backed up Security Center configurations before the factory reset, restore the configurations using the SV Control Panel.
- Reconfigure your appliance.

Performing a factory reset on a Streamvault workstation or server appliance

If the software on your Streamvault™ server or workstation fails to start or stops working as expected, you can perform a factory reset using a USB key.

Before you begin

- Back up all Security Center configuration using SV Control Panel. For more information, see Backing up your Directory database on page 36.
- Get a USB key with at least 32 GB of storage. Some USB keys are unable to boot the image; if this occurs, try using a different brand or model of key.

  CAUTION: All data on the USB key is deleted when you create a bootable drive.
- Have the correct license for the version of Security Center you want to restore or install.
- Have the System ID and password that was sent by email when you purchased the appliance.

What you should know

- **Applies to:** All models beginning with SVW, SVR, and SVA, and all servers with model numbers SV-1000E and above.
- For All-in-One appliances, see Performing a factory reset on a Streamvault All-in-one appliance on page 78.
- A factory reset deletes all the data currently on the System (OS) drive, but it doesn't affect the factory default RAID drive settings.
- The reset might fail if hard drives, RAID drives, or partitions on the appliance were changed from the factory default settings. In such a case, contact the Genetec™ Technical Assistance Center (GTAC).

Procedure

1 Create a factory reset USB key.

2 Using the USB key, reset the image on your appliance.

After you finish

Set up your appliance.

Related Topics

Finding the system ID and image version of a Streamvault appliance on page 74

Creating a factory reset USB key for a Streamvault workstation or server appliance

Before you can reset the image of a Streamvault™ workstation or server appliance, you must prepare a bootable USB key that contains the required Streamvault software image.

Before you begin

Get a USB key with at least 32 GB of storage. Some USB keys are unable to boot the image; if this occurs, try using a different brand or model of key.

CAUTION: All data on the USB key is deleted when you create a bootable drive.

Procedure

1 Contact Genetec™ Technical Assistance Center (GTAC) to get the recovery image.
The recovery image comes in one of the following three formats:

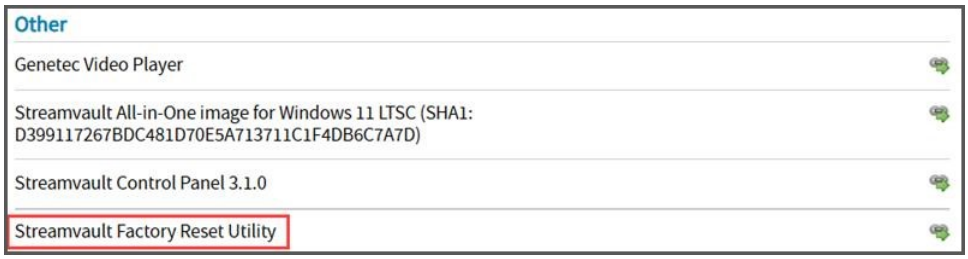
- A *.zip* file containing *.swm* files.
- A *.iso* file containing the *.swm* files and the *Streamvault factory reset utility* user interface, which you'll use to reset the software image.
- A *.iso* file containing the *Windows Setup* wizard, which you'll use to reset the software image.

2 If your recovery image is a *.zip* file, unzip the contents into any Windows folder.

3 From the Product Download page on GTAP, download the *Streamvault factory reset utility* USB creator.

a) From the *Download Finder* list, select your version of Security Center.

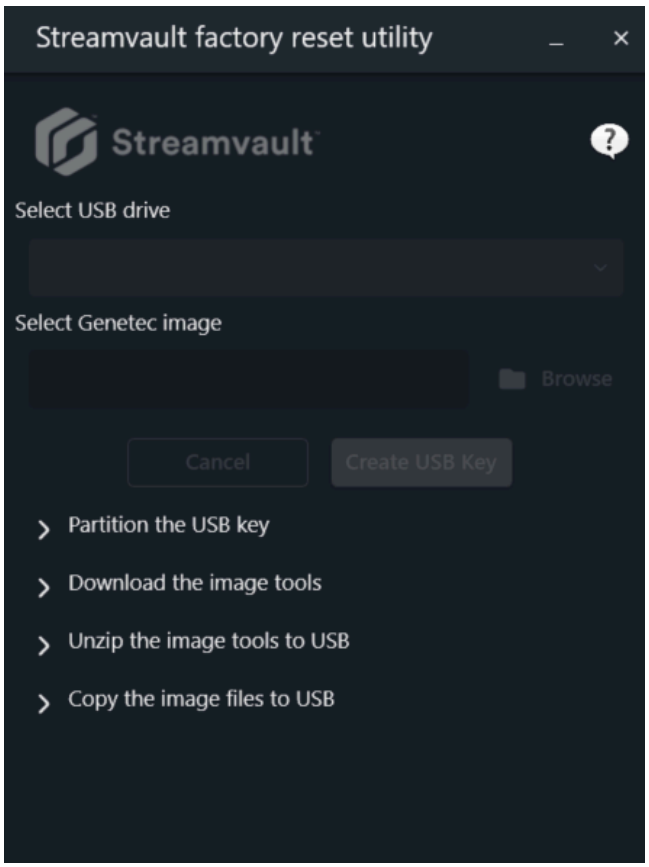
b) From the *Other* list, download the *Streamvault Factory Reset Utility* package.



4 Insert the USB key into a USB port.

5 Open the *Streamvault factory reset utility* USB creator.

6 From the **Select USB drive** list, select a USB key that has at least 32 GB of storage.



7 In the *Select Genetec image* section, click **Browse** and select the *.swm* or *.iso* file you downloaded.
If you require a *.swm* file, select the required image from the <*service tag number*> folder.

8 Click **Create USB Key**.
The *Streamvault factory reset utility* starts to partition the USB key, download the image tools, and copy the image files.

When the download is complete, the following message is displayed: The USB key was created successfully.

Example

The following video shows you how to create a factory reset USB key with *.swm* files.

After you finish

Choose from the following:

- Reset the software image of your Streamvault All-in-one appliance.
- Reset the software image of your Streamvault workstation or server appliance.

Resetting the software image on a Streamvault workstation or server appliance

After you have prepared a bootable USB key that has the required Streamvault™ software image, you can use it to reset the software image on a workstation or server appliance.

Before you begin

- Make sure you have the USB key that contains the recovery software for your appliance.

What you should know

- Resetting doesn't affect the factory default RAID drive settings.
- Resetting might fail if the hard drives, RAID drives, or partitions on the appliance have been changed from the factory default settings. In such a case, contact the Genetec™ Technical Assistance Center (GTAC).

Procedure

1 Shut down the appliance.

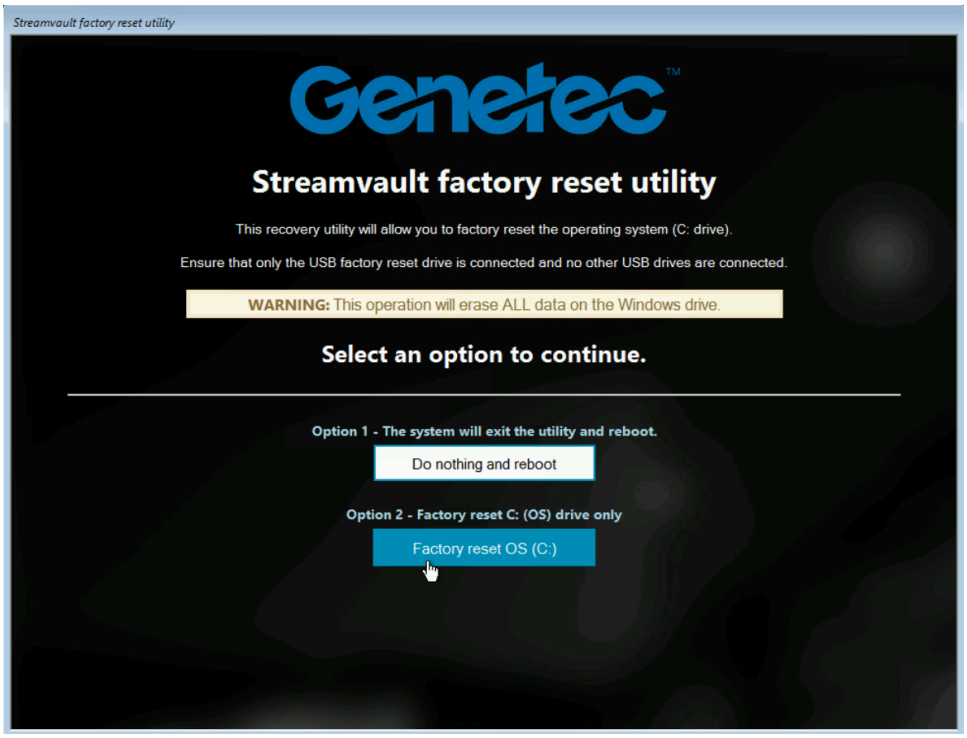
2 Insert the bootable USB key that you created into a USB port.

3 Power on the Streamvault appliance.

4 When prompted, press F12.
The *Boot Manager* opens. Click **One-shot UEFI Boot Menu**.

5 Select your USB drive, and then press Enter.
The *Streamvault factory reset utility* opens.

6 Click **Factory reset OS (C:)**.



A Command Prompt opens and the *Streamvault factory reset utility* analyzes the system to detect the system (OS) drive.

7 In the Command Prompt, type Yes to confirm that the correct hard drive was detected, and then press Enter to start the factory reset.

IMPORTANT: Do not interrupt, shut down, or reboot the workstation during the re-imaging process. It might take up to 20 minutes, depending on the speed of your USB key.

8 After the factory reset is complete, press Enter when prompted to reboot the workstation.

9 Remove the USB key from the USB port.

The workstation is now reset to its default state.

Example

Watch this video to learn how to reset the software image on a Streamvault workstation or server appliance.

After you finish

- Log on to Windows using the default username and password that are on the sticker adhered to the appliance.
- Activate your Security Center license.
- If you backed up Security Center configurations before the factory reset, restore the configurations using the SV Control Panel.
- Reconfigure your appliance.

Mercury EP controllers remain offline when TLS 1.1 is disabled

After enrolling a Mercury EP controller in Security Center, the unit doesn't come online.

You don't receive any errors or warnings about this issue.

Applies to:

- Streamvault™ SV-100E 16.3 and later
- Streamvault™ SV-300E 16.3 and later
- Streamvault™ SV-350E 16.3 and later

Cause

All Mercury EP controllers require the Transport Layer Security (TLS) 1.1 protocol to communicate with Security Center. However, the protocol is disabled on all Streamvault™ All-in-One appliances 16.3 and later.

Solution

Enable TLS 1.1.

Enabling Transport Layer Security (TLS)

The Transport Layer Security (TLS) 1.0 and 1.1 protocols have several major vulnerabilities, so they are disabled on Streamvault™ appliances. When a device enrolled in Security Center requires one of these protocols for communication, you must enable the protocol on your appliance.

What you should know

- TLS 1.1 is disabled in Streamvault software image 16.3 and later.
- TLS 1.0 is disabled in Streamvault software image 16.0 and later.
- Enable only the version of TLS that your device requires.
- Enable TLS on the server (incoming) and client (outgoing) nodes.
- For security reasons, the Internet Properties options are disabled on appliances. If your appliance has the Streamvault service, you can enable TLS from the Local Group Policy Editor. If your appliance doesn't have the Streamvault service, you can only enable TLS from the Windows Registry Editor.

Procedure

To enable TLS on an appliance with the Streamvault service:

1 Open Command Prompt as an administrator and run `gpedit.msc`.

The Local Group Policy Editor opens.

2 Go to **Computer Configuration** > **Administrative Templates** > **Streamvault** > **Genetec** > **Additional Templates**.

3 Enable TLS 1.*n* on the client, where *n* represents the minor version number:

a) Right-click on *\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n\Client\Enabled* and click **Edit**.

b) Set **Enabled** to 1 and click **Apply** > **OK**.

c) Right-click on *\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n\Client\DisabledByDefault* and click **Edit**.

d) Set **DisabledByDefault** to 0 and click **Apply** > **OK**.

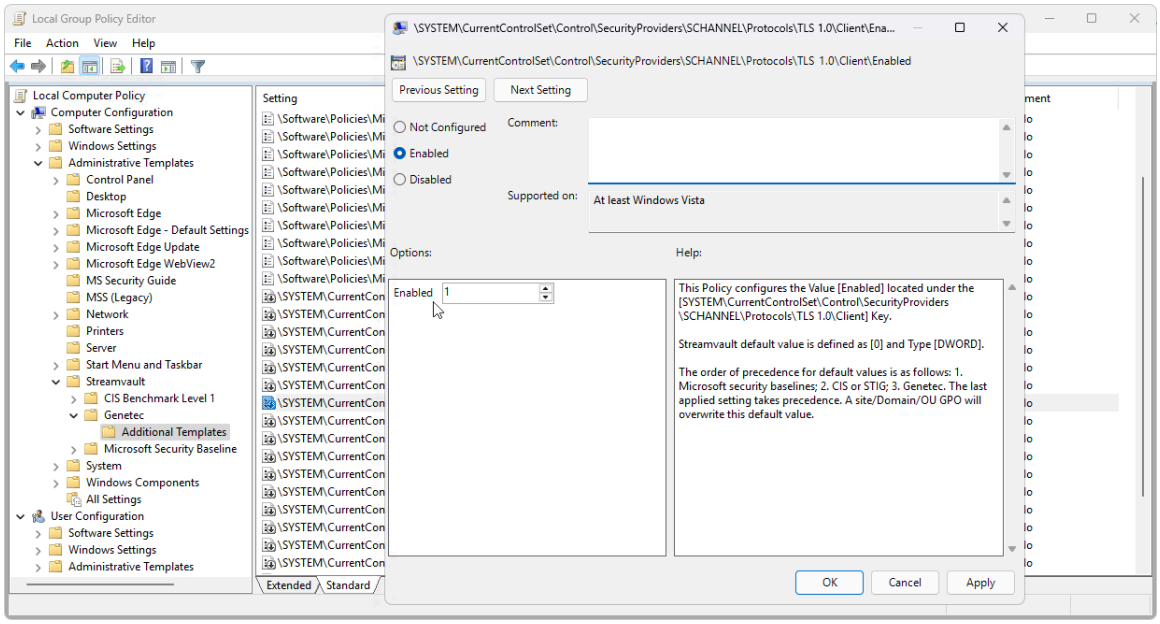
4 Enable TLS 1.*n* on the server:

a) Right-click on *\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n\Server\Enabled* and click **Edit**.

b) Set **Enabled** to 1 and click **Apply** > **OK**.

c) Right-click on *\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n\Server\DisabledByDefault* and click **Edit**.

d) Set **DisabledByDefault** to 0 and click **Apply** > **OK**.



5 Restart Windows.

To enable TLS on an appliance without the Streamvault service:

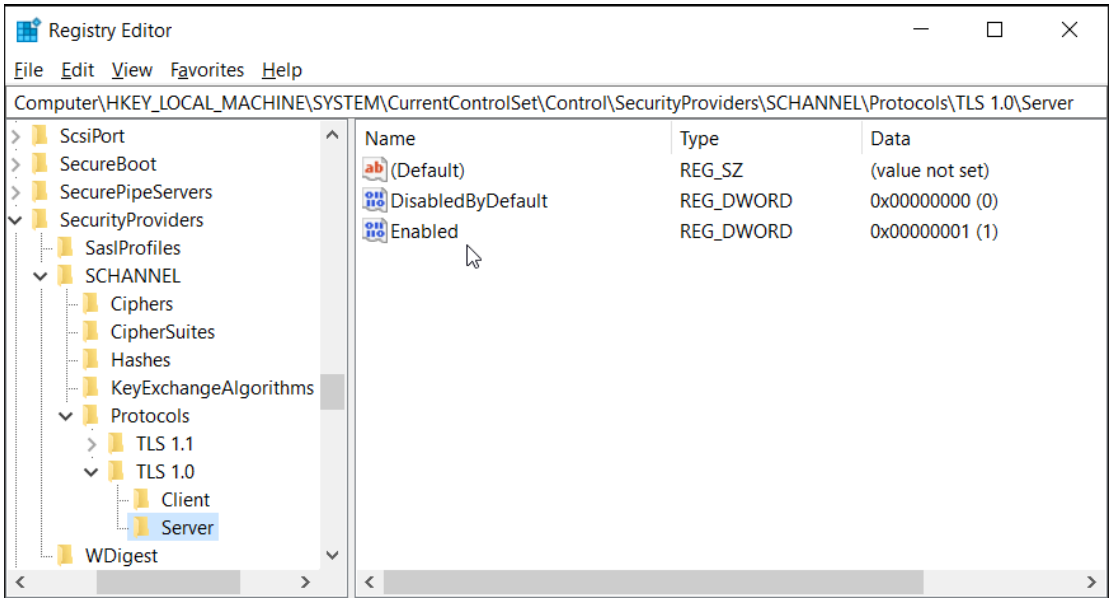
1 Open Windows Registry Editor.

2 Enable TLS 1.*n*, where *n* represents the minor version number:

a) Navigate to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n.*

b) Select the **Server** node, set **DisabledByDefault** to 0, and set **Enabled** to 1.

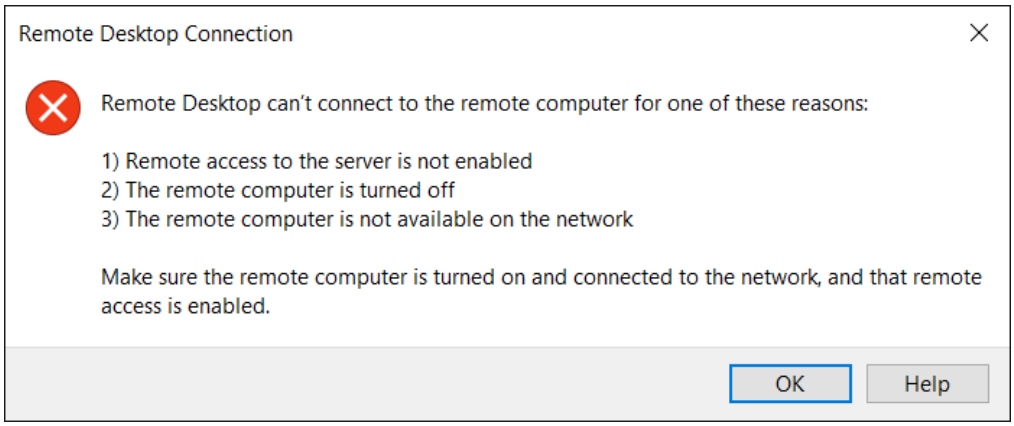
c) Select the **Client** node, set **DisabledByDefault** to 0, and set **Enabled** to 1.



3 Restart Windows.

Remote Desktop can’t connect to a Streamvault appliance

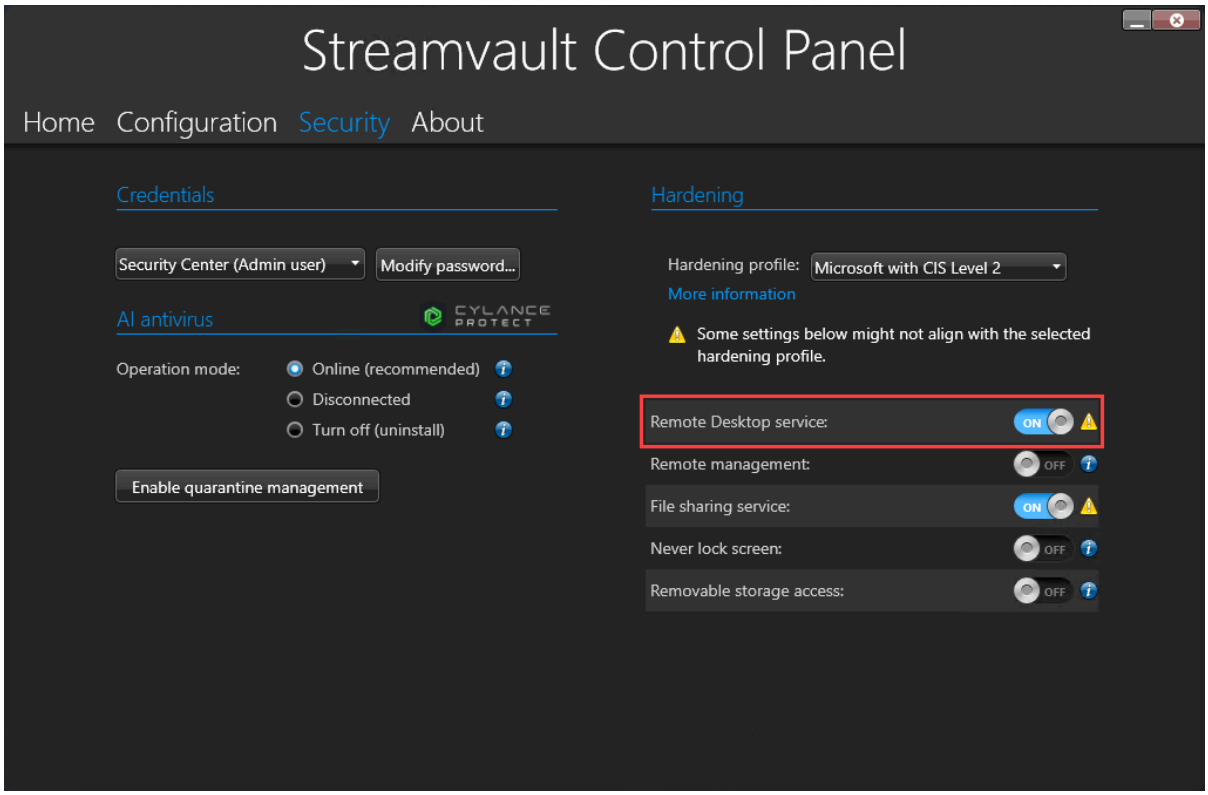
When you try to access a Streamvault™ appliance using Remote Desktop, you receive a message that Remote Desktop can't connect to the remote computer.



Remote Desktop service is disabled in the SV Control Panel

Description: To ensure maximum security, remote access is disabled by default on an appliance.

Solution: Enable remote access on the appliance. On the *Security* page of the SV Control Panel, turn on **Remote Desktop service**.



Remote Desktop isn't allowed in Windows

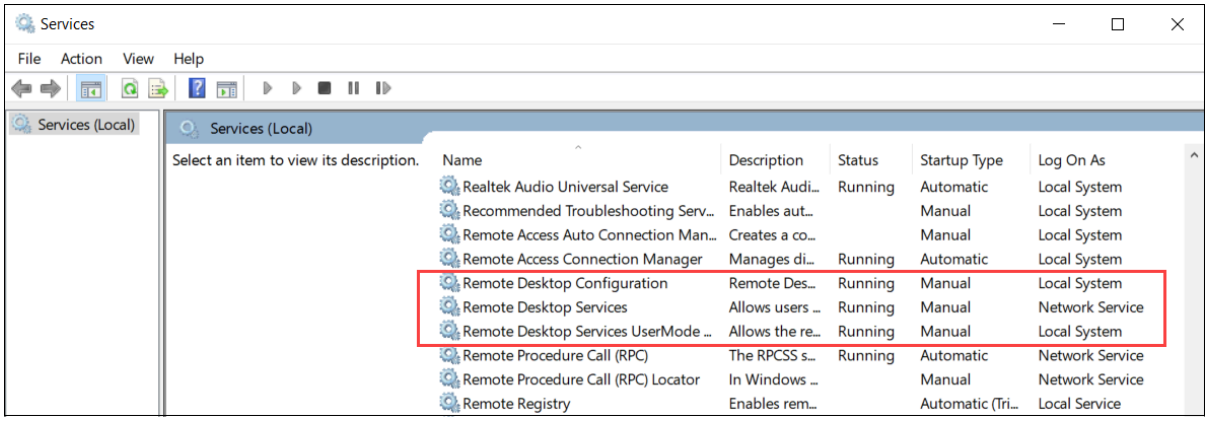
Description: Although **Remote Desktop service** is turned on in the SV Control Panel, this setting is currently not allowed in Windows.

Solution: Overwrite the Windows setting by turning off and then turning on the **Remote Desktop service** option.

Remote Desktop Services aren’t running

Description: The Remote Desktop Services were stopped in Windows.

Solution: Open the Windows Services console, ensure that **Remote Desktop Services** is logged on as a **Network Service** user, and ensure that the other Remote Desktop Services are running.

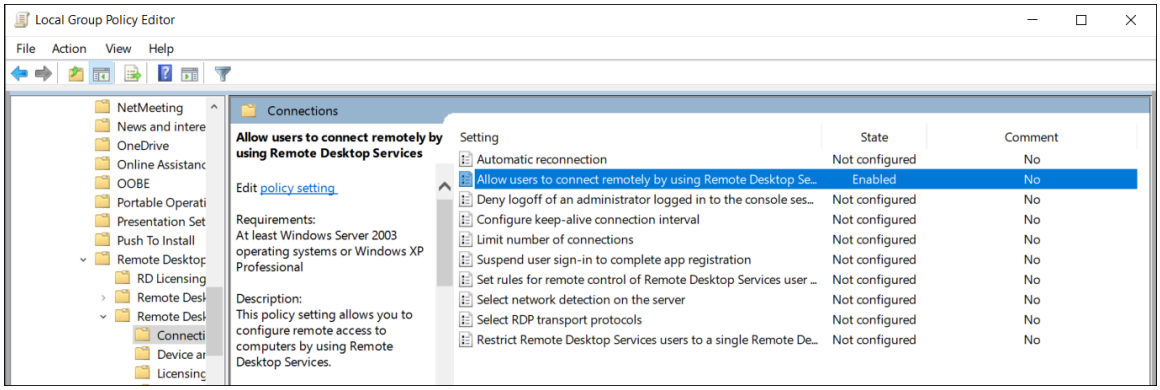


Remote Desktop Services are denied

Description: Windows is configured to deny access for remote users to Remote Desktop Services.

Solution: Allow remote user access to the appliance using Remote Desktop Services:

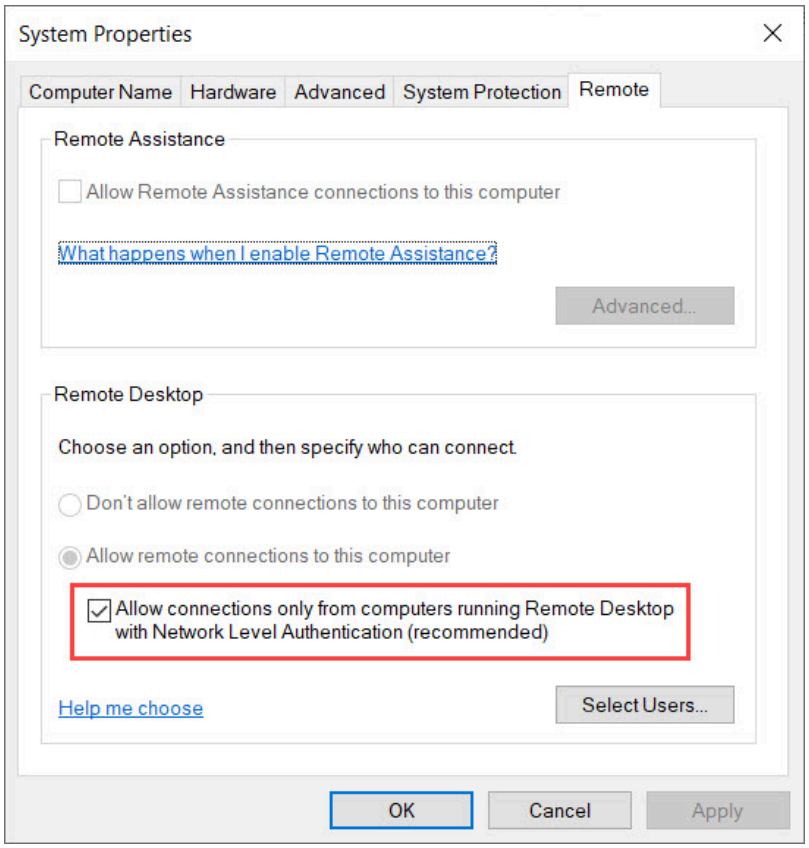
1. Open Command Prompt as an administrator and run `gpedit.msc`.
2. Go to **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections**.
3. Enable **Allow users to connect remotely by using Remote Desktop Services**.



4. In Command Prompt, run `gpupdate /force`.
5. From the Windows Control Panel, go to **System and Security** > **Allow remote access**.

   The *System Properties* window opens on the **Remote** tab.

6. In the *Remote Desktop* section, ensure that **Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)** is selected.



Local group policies deny remote access

Description: The Windows local group policies are configured to deny remote access to your appliance.

Solution: Configure the group policies on your appliance to allow remote access:

1. Open Command Prompt as an administrator and run `gpedit.msc`.
2. Go to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**.
3. Verify the following group policy settings:
   - **Allow log on through Remote Desktop Services** is set to **Administrators**.
   - **Deny access to this computer from the network** is set to **Guests**.
   - **Deny log on through Remote Desktop Services** is set to **Guests**.

NTLMv2 authentication is unsupported

Description: The appliance or the remote computer doesn't support NTLMv2 authentication.

NOTE: If all client computers support NTLMv2, Microsoft and several independent organizations strongly recommend the *Send NTLMv2 responses only* policy. Consult the Microsoft Network security: LAN Manager authentication level best practices and security considerations before changing your settings.

Solution: To ensure that your environment allows NTLMv2 authentication:

1. Open Command Prompt as an administrator and run `gpedit.msc`.

2. Go to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local policies** > **Security Options** > **Network security: LAN Manager authentication level**.
3. Set the policy to **Send LM & NTLM - use NTLMv2 session security if negotiated**.

Contact us

Solution: If Remote Desktop Connection is still unable to connect, contact the Genetec Technical Assistance Center (GTAC).

Related Topics

Allowing Remote Desktop connections to a Streamvault appliance on page 76

Removing restrictions from non-administrator user accounts

By default, non-administrator user accounts, including the Operator, have limited access to Streamvault™ Control Panel features. You can remove the restrictions from those accounts to give them more access to features.

Before you begin

- Only a person logged on as Admin can remove restrictions from non-administrator accounts.
- Restrictions can only be removed on systems with the Streamvault service.

Procedure

1 Open File Explorer and navigate to *C:\Windows\System32\GroupPolicyUsers*.

2 Delete the *S-1-5-32-545* folder and all its contents. This folder contains the restrictions for non-administrators.

3 Restart Windows.

Local accounts can't access Remote Desktop, file sharing service, and remote management

When the **Remote Desktop service**, **Remote management**, or **File sharing service** options are turned on in the SV Control Panel, local accounts still can't access the features.

This behavior applies to Windows Server products that have SV Control Panel 3.0 and later:

- Streamvault™ SV-1000E series
- Streamvault™ SV-2000E series
- Streamvault™ SV-4000EX series
- Streamvault™ SV-7000EX series

By default, Remote Desktop service, Remote management, and File sharing service are disabled for the local administrator and local accounts, such as Operator. With previous versions of the SV Control Panel, the local administrator and local accounts all got access to these features when they were turned on. As of SV Control Panel 3.0, only the local administrator is given access when the features are turned on.

This new behavior is controlled through the **Deny access to this computer from the network** security policy and complies with Microsoft's security baseline for Windows Server.

Enabling Smart Card related services

If you've upgraded to SV Control Panel 3.0 from an older version and want to enable Smart Card related services, you can do so through the Windows Services application.

What you should know

The **Enable Smart Cards support** option isn't available in SV Control Panel 3.0, as the Smart Card services are enabled by default.

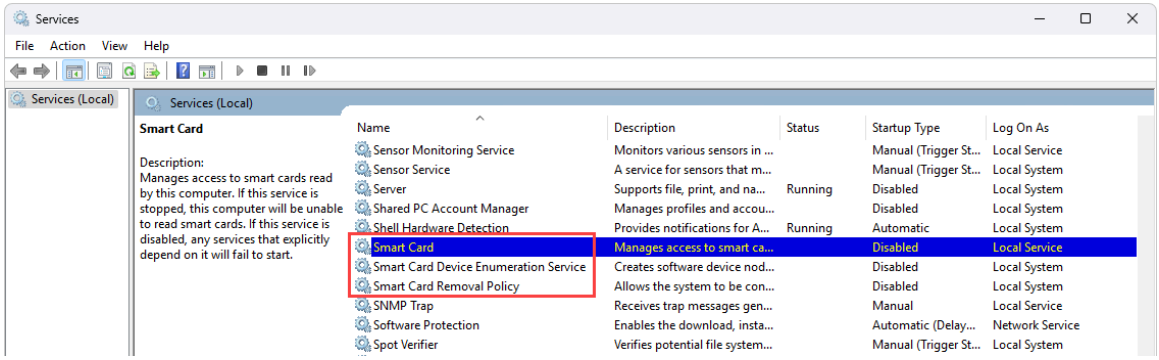
Procedure

1 In Windows, run *services.msc* to open the *Services* application.

2 Enable the **Smart Card** service.
   a) Right-click on the **Smart Card** service and select **Properties**.
      The *Properties* dialog box opens.
   b) On the **General** tab, locate the **Startup type** field, and select **Automatic**.
   c) Click **Apply** > **OK**.

3 Enable the **Smart Card Device Enumeration Service**.
   a) Right-click on **Smart Card Device Enumeration Service** and select **Properties**.
      The *Properties* dialog box opens.
   b) On the **General** tab, locate the **Startup type** field, and select **Manual**.
   c) Click **Apply** > **OK**.

4 Enable the **Smart Card Device Enumeration Service**.
   a) Right-click on the **Smart Card Removal Policy** service and select **Properties**.
      The *Properties* dialog box opens.
   b) On the **General** tab, locate the **Startup type** field, and select **Manual**.
   c) Click **Apply** > **OK**.



Enabling support for Mercury EP and LP firmware 1.x.x controllers

Before you can integrate Mercury EP or LP firmware 1.x.x controllers on your Streamvault™ appliance, you must enable an older SSL cipher suite.

What you should know

Depending on your integration, one of the following cipher suites must be added to allow the units to communicate with the appliance:

- **Mercury LP controller integration on firmware 1.31 and earlier:**
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_RSA_WITH_AES_128_GCM_SHA256
- **Mercury EP controller integration on firmware 1.29.7 and earlier:**
  - TLS_RSA_WITH_AES_256_CBC_SHA

Procedure

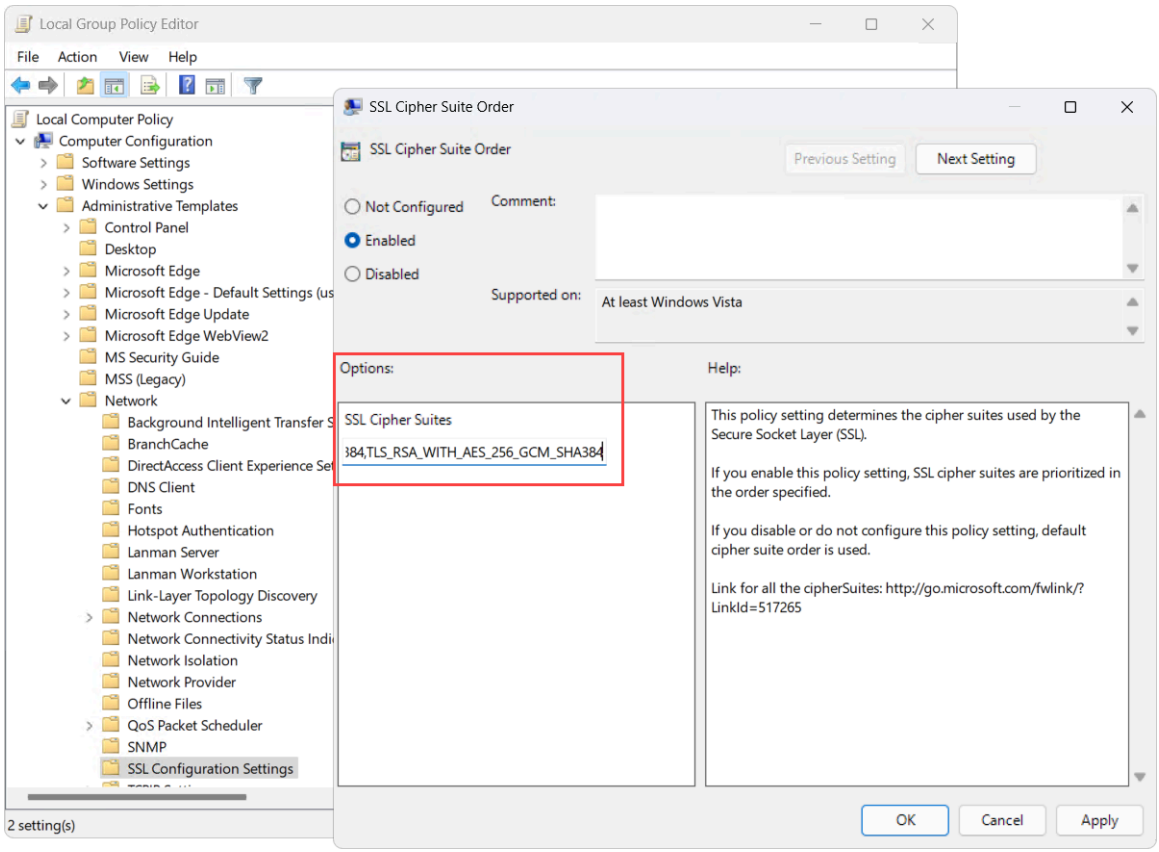
1 In Windows, run `gpedit.msc` to open the *Local Group Policy Editor*.

2 Navigate to **Computer Configuration** > **Administrative Templates** > **Network** > **SSL Configuration Settings**.

3 Double-click **SSL Cipher Suite Order**.

4 In the *Options* pane, in the **SSL Cipher Suites** field, add a comma to the end of the list followed by the cipher suite applicable to your integration. Don't add any spaces.

5 Click **OK** to save the Group Policy Object (GPO).



6 Restart the Softwire Service or reboot the appliance.

Enabling support for the Synergis IX integration

Before you can enroll Synergis™ IX controllers on your Streamvault™ appliance, you must add an extra SSL cipher suite.

What you should know

One of the following cipher suites must be added to enroll Synergis IX controllers on your Streamvault appliance:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Procedure

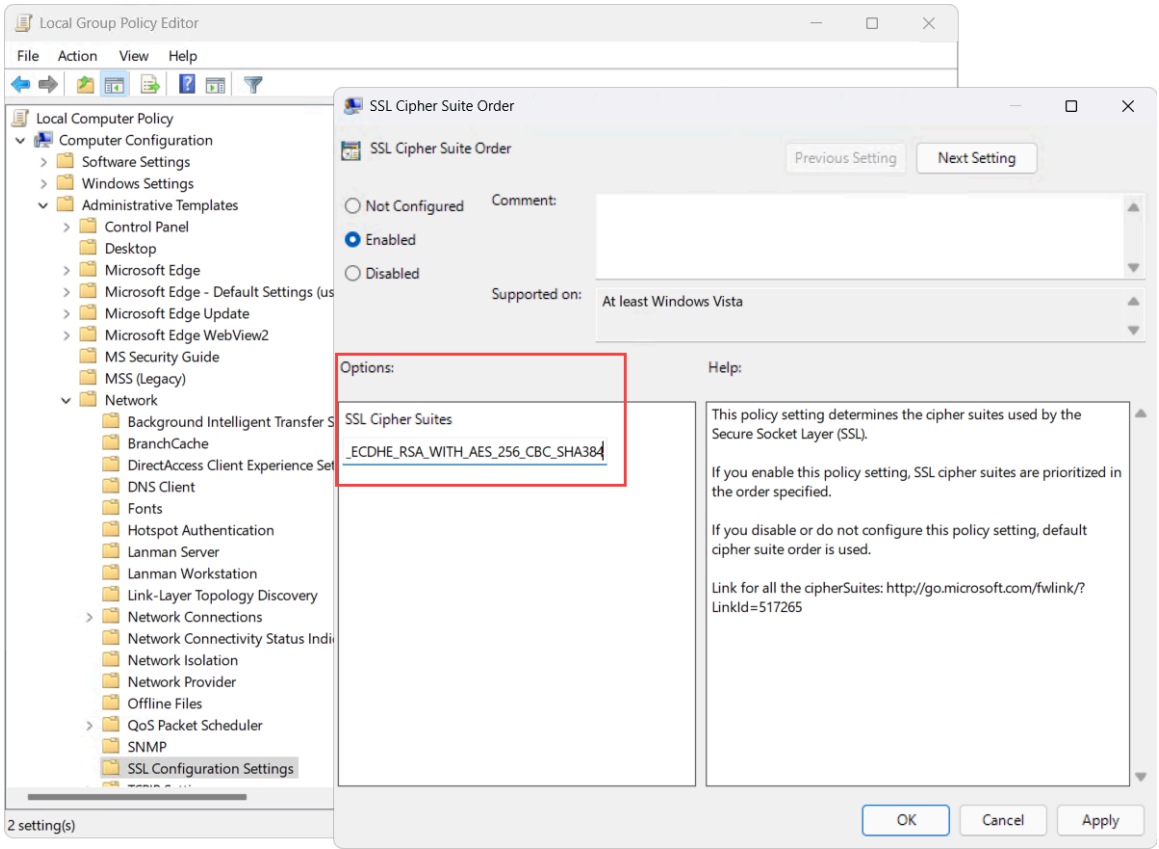
1 In Windows, run `gpedit.msc` to open the *Local Group Policy Editor*.

2 Navigate to **Computer Configuration** > **Administrative Templates** > **Network** > **SSL Configuration Settings**.

3 Double-click **SSL Cipher Suite Order**.

4 In the *Options* pane, in the **SSL Cipher Suites** field, add a comma to the end of the list followed by `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` or `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256`. Don't add any spaces.

5 Click **OK** to save the Group Policy Object (GPO).



6 Restart the Softwire Service or reboot the appliance.

7

Technical support

This section includes the following topics:

Contacting the Genetec Technical Assistance Center

The Genetec™ Technical Assistance Center (GTAC) is available to assist you with any software or hardware issues related to Streamvault™.

NOTE: For inquiries about Genetec™ Security Center software issues, technical assistance is offered through our regular technical assistance line. To find the GTAC phone number and business hours in your region, refer to the Genetec Technical Assistance Center *Contact us* page.

Useful information

When opening a support case, have the following information ready:

- Your Security Center license system ID. For more information, see How do I find my system ID?.
- Your Genetec serial number or the hardware service tag.
- Your Genetec code, which is found on the chassis (not applicable to all-in-one appliances). The code is required if you lose administrative access to the system and need a factory image.

- Your diagnostics TSR log file (if applicable).

Contacting GTAC by phone

Phone support for Streamvault™ issues is available to all customers during the business hours of their region.

For customers in North America, Europe, Middle East, and Africa:

1. Refer to the Genetec™ Technical Assistance Center (GTAC) *Contact us* page to find the GTAC phone number and business hours in your region.
2. Call the GTAC phone number and choose Option #2.

For customers in the Asia-Pacific region:

Support for the APAC region is provided through the Genetec Technical Assistance Portal (GTAP) through live chat and support cases. Operating hours are from Monday to Friday 8 am - 8 pm (local time).

For 24/7 emergency support outside of business hours:

1. Call the GTAC number for your region.
2. Enter your Genetec certification ID number.
3. Enter the Genetec Advantage contract number or Genetec Subscription number.
4. Select the product.
5. Leave a message including your name, phone number, and a description of the issue.

   The on-call engineer contacts you within 30 minutes.

IMPORTANT: 24/7 emergency support is available only to customers who have added this option to their Genetec Advantage contract. For more information, contact advantage@genetec.com.

Customers without Advantage coverage must open a case through the Genetec Technical Assistance Portal (GTAP).

Contacting GTAC through GTAP

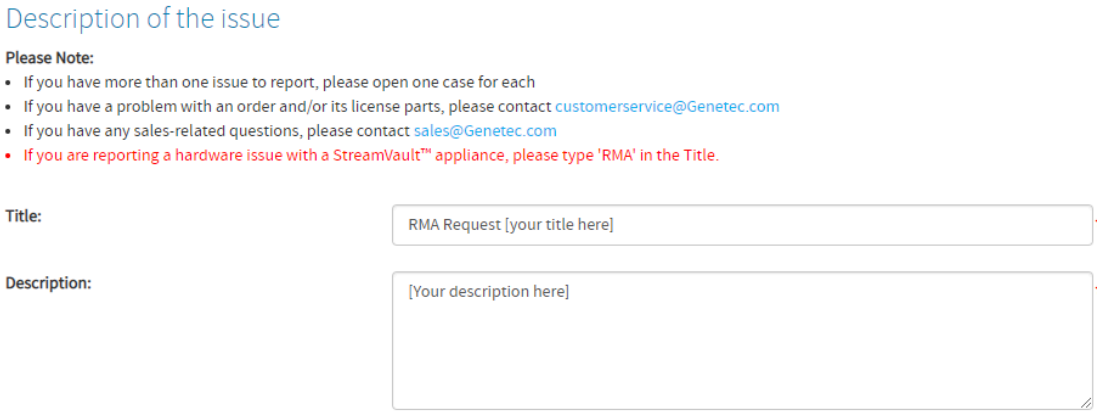
Support for Streamvault™ issues is available to all customers during the business hours of their region through online support cases on the Genetec™ Technical Assistance Portal (GTAP).

For customers without Genetec™ Advantage coverage, a case needs to be opened through the Genetec Technical Assistance Portal (GTAP). For more information on Genetec Advantage, contact advantage@genetec.com.

To submit a case through the online portal:

1. Navigate to Genetec Technical Assistance Portal.
2. Log in using your corporate email.
3. Click **+ Create Case**.

4. From the **System ID** list, select the affected system.
5. For hardware return or repairs, include **RMA Request** in the title so our team can easily identify these requests.



6. Include your product's serial number, Genetec code, and diagnostics TSR log file (if applicable).
7. Click **Submit case**.

   You'll receive a case confirmation by email with the estimated response time.

Contacting GTAC through live chat

Support for Streamvault™ issues is available for customers with Genetec™ Advantage coverage through live chat on the Genetec Technical Assistance Portal (GTAP). Customers can receive support during the business hours of their region.

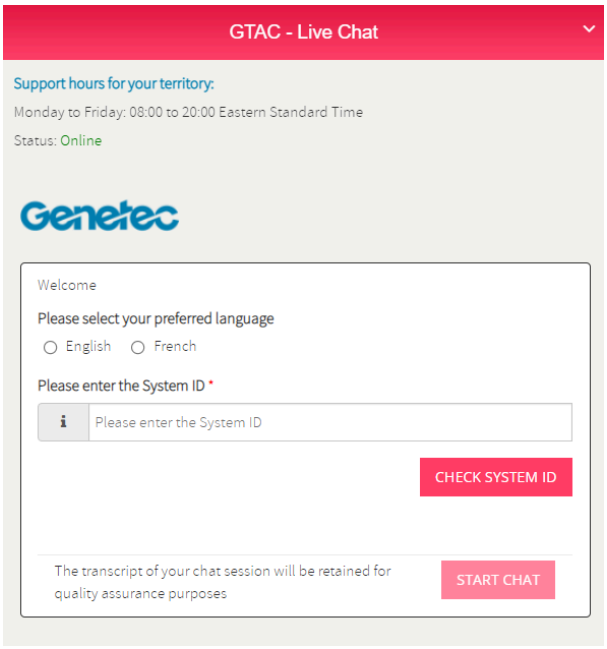
For customers without Genetec Advantage coverage, a case needs to be opened through Genetec Technical Assistance Portal (GTAP). For more information on Genetec Advantage, contact advantage@genetec.com.

To start a Live Chat:

1. Go to Genetec Technical Assistance Portal
2. Log in using your corporate email.
3. Click the **click to chat** button.

4. Choose your preferred language.

5. Enter the full system ID (`GSC-xxxxxx-xxxxxx`), then click **Check System ID**.
6. Choose whether you're chatting about a new or existing case.
7. Select the product.
8. Click **Start chat**.



9. To initiate an RMA, include the product's serial number, Genetec code, and diagnostics TSR log file (if applicable).

   Response time (available only during the business hours of your region): Usually within 5 minutes.

Software support

Streamvault™ Windows image software includes the latest version of Security Center software and control panel at the time of image creation. Support for the Windows image and Security Center software is handled separately.

Streamvault software

- Streamvault Windows image is covered under your Streamvault warranty for the entire lifecycle of the appliance.

  IMPORTANT: Upgrading the Windows operating system is not covered by your warranty. Upgrading the Windows operating system deletes the necessary drivers, hardening, and software installed with the image.
- The backup image provided for a Streamvault appliance re-imaging includes the original operating system and image provided with the appliance upon purchase.
- Streamvault Windows image is covered under your Streamvault warranty regardless of your Genetec™ Advantage status.

Security Center software

Issues with Security Center software are covered by the service-level agreement (SLA) and support procedures outlined in the following Genetec™ Lifecycle Management (GLM) document: Genetec Advantage Description.

Hardware support

HP and Dell ProSupport warranties are available through Genetec™. For any hardware issues, the Genetec™ Technical Assistance Center (GTAC) is your point of contact to diagnose the issue and coordinate with HP and Dell ProSupport.

Refer to the Genetec Hardware Warranty Overview for details about the Streamvault hardware warranties offered by Genetec.

Specifications for Streamvault

Refer to the following technical, mechanical, and environmental specifications when planning and deploying your Streamvault™ appliance.

Technical, mechanical, and environmental specifications

All-in-one appliances:

- SV-300E datasheet

Rackmount appliances:

- SV-1000E series datasheet
- SV-2000E series datasheet
- SV-4000E series datasheet

High-availability centralized storage:

- SV-7000EX series datasheet

Workstations:

- SVW-100E series datasheet
- SVW-300E series datasheet
- SVW-500E series datasheet

All-in-one Vehicle Monitoring appliances:

- SVR-300A series datasheet
- SVR-300AR series datasheet
- SVR-500A series datasheet

Streamvault support terms and conditions

The Genetec™ Standard and Extended hardware warranties are governed by the terms and conditions described in the Genetec Hardware Warranty Overview.

Glossary

manufacturing image

A manufacturing image is a Streamvault™ image that is shipped to customers when they purchase an appliance. The software versions installed on this image vary depending on the customer order.

recovery image

A recovery image is used for re-imaging Streamvault™ appliances. It's a fixed image with specific software versions pre-installed.

Streamvault factory reset utility

The Streamvault factory reset utility is a tool that allows you to reimage a Streamvault appliance to factory settings. The tool helps you create a bootable USB key with the required Streamvault software image.

Streamvault service

The Streamvault service is a Windows service that enables users to configure a Streamvault™ appliance, such as applying hardening profiles.

Streamvault™ hardware

Streamvault™ hardware is a report task in Security Center that you can use to view a list of health issues affecting your Streamvault™ appliances.

Streamvault™ hardware monitor

The Streamvault™ hardware monitor entity is used to monitor the health of your Streamvault™ appliances and ensure you receive notifications when problems occur. One Streamvault™ hardware monitor per Streamvault™ appliance is required.

Streamvault™ manager

The Streamvault™ manager entity is used to control the alert configurations for a group of Streamvault™ Agent entities. Only one Streamvault™ manager is allowed per system.

SV-1000E

The SV-1000E is a cost-effective rackmount security appliance designed for mid-sized security systems. It helps you move to a unified security system combining video surveillance, access control, automatic license plate recognition, communications, intrusion and analytics in a single appliance. The SV-1000E comes with Security Center, and the SV Control Panel pre-installed.

SV-100E

The SV-100E is a subcompact all-in-one appliance that comes with Microsoft Windows, Security Center, and the SV Control Panel pre-installed. The SV-100E is for small-scale, single server installations, and can support both cameras and access control readers.

SV-2000E

The SV-2000E is a rackmount security appliance that lets you easily deploy a unified system combining video surveillance, access control, automatic license plate recognition and communications. The SV-2000E comes with Security Center, and the SV Control Panel pre-installed.

SV-300E

The SV-300E is a compact, all-in-one turnkey appliance that comes with Microsoft Windows, Security Center, and the SV Control Panel preinstalled. With built-in analog encoder capture cards, you can use the appliance to quickly deploy a standalone video surveillance or access control system, or a unified system.

SV-350E

The SV-350E is an all-in-one, turnkey security appliance that helps you move to a unified system combining video surveillance, access control, intrusion detection, and communications. It comes with Microsoft Windows, Security Center, and the SV Control Panel pre-installed. It offers RAID 5 for critical video storage.

SV-4000E

The SV-4000E is a rackmount security appliance that delivers enterprise-grade performance and reliability. Its certified hardware configurations and out-of-the-box hardening against cyber threats simplifies the design and deployment of a new security system. The SV-4000E comes with Security Center, and the SV Control Panel pre-installed.

SV-7000E

The SV-7000E is a rackmount security appliance designed for applications combining a large number of high resolution cameras, users and events. The SV-7000E comes with Security Center, and the SV Control Panel pre-installed.

SVA-100E

The SVA-100E is a compact appliance you can use to easily enhance your security system with KiwiVision™ video analytics. The design is optimized for you to apply more analytics streams to your video surveillance system, whether that is a single or multiple analytic stream, per camera.

SV appliance

Streamvault™ is a turnkey appliance that comes with an embedded operating system and Security Center pre-installed. You can use Streamvault™ appliances to quickly deploy a unified or standalone video surveillance and access control system.

SV Control Panel

SV Control Panel is a user interface application that you can use to configure your Streamvault™ appliance to work with Security Center access control and video surveillance.

SVW-300E

The SVW-300E workstation is a turnkey solution designed for monitoring small and medium-sized security systems with support for multiple displays. The SVW-300E comes with Security Center pre-installed.

SVW-500E

The SVW-500E workstation is a high-performance solution designed for users who need the ability to view cameras with a very high-resolution on 4K monitors and video walls. The SVW-500E comes with Security Center pre-installed.

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.

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