Streamvault™ Appliance User Guide

Click here for the most recent version of this document.

Document last updated: November 3, 2023

Legal notices

Genetec Inc. distributes this document with software that includes an end-user license agreement and is furnished under license and may be used only in accordance with the terms of the license agreement. The contents of this document are protected under copyright law.

The contents of this guide are furnished for informational use only and are subject to change without notice. Genetec Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

This publication may not be copied, modified, or reproduced in any form or for any purpose, nor can any derivative works be created therefrom without Genetec Inc.'s prior written consent.

Genetec Inc. reserves the right to revise and improve its products as it sees fit. This document describes the state of a product at the time of document's last revision, and may not reflect the product at all times in the future.

In no event shall Genetec Inc. be liable to any person or entity with respect to any loss or damage that is incidental to or consequential upon the instructions found in this document or the computer software and hardware products described herein.

Genetec™, AutoVu™, AutoVu MLC™, Citywise™, Community Connect, Curb Sense™, Federation™, Flexreader™, Genetec Airport Sense™, Genetec Citigraf™, Genetec Clearance™, Genetec ClearID™, Genetec Mission Control™, Genetec Motoscan™, Genetec Patroller™, Genetec Retail Sense™, Genetec Traffic Sense™, KiwiVision™, KiwiSecurity™, Omnicast™, Privacy Protector™, Sipelia™, Stratocast™, Streamvault™, Synergis™, Valcri™, their respective logos, as well as the Mobius Strip Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.

Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

Patent pending. Genetec Security Center, Omnicast, AutoVu, Stratocast, Citigraf, Clearance, and other Genetec products are the subject of pending patent applications, and may be the subject of issued patents, in the United States and in other jurisdictions worldwide.

All specifications are subject to change without notice.

Document information

Document title: Streamvault™ Appliance User Guide

Original document number: EN.803.003

Document number: EN.803.003

Document update date: November 3, 2023

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

Preface

Chapter 1: Introduction to your Streamvault appliance

Chapter 2: Getting started with SV Control Panel

Chapter 3: Getting started with Streamvault Maintenance plugin

Chapter 4: SV Control Panel reference

Chapter 5: Additional resources

Chapter 6: Troubleshooting

Chapter 7: Technical support

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, read the release notes to learn about the new features, known issues, and limitations.	In the *Streamvault Release Notes* for the image version installed on your appliance, see: • What's new • Known issues • Limitations
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 11.
Complete the setup wizards		
4	Complete the *Streamvault Control Panel setup* wizard. **NOTE:** Remote desktop is disabled by default. To enable remote desktop, turn off the **Block remote desktop** setting on the *Security* page of this wizard.	• Setting up your appliance in the SV Control Panel on page 14. • Allowing Remote Desktop connections to a Streamvault appliance on page 68.
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 is not connected to the internet, activate your license manually from Server Admin.	• Activating your Security Center license on an appliance on page 17. • Activating a license manually from Server Admin on page 19.
6	Activate the System Availability Monitor.	• Activating System Availability Monitor on page 21.
7	Configure the Genetec™ Update Service so that you can get the latest version of Security Center and SV Control Panel. If there are updates, install them.	• In the *Genetec™ Update Service User Guide*, see "Configuring Genetec Update Service".

Step	Task	Where to find more information
8	If SV Control Panel indicates that there are more updates available, install them now.	- About updating SV software on page 7.
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 33. - For SV-7000E and for All-in-one: Manually adding partitions and Archiver roles on page 35.
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 22. - Configuring unit enrollment settings on page 24.
11	Back up the Security Center configuration.	- Backing up your Directory database on page 31.

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 table lists the ports that must be opened for inbound traffic so that the Streamvault™ Maintenance plugin can communicate with the Streamvault hardware.

Module	Inbound port	Port usage
Streamvault hardware monitor	65115	Used for communicating between Security Center and the Streamvault hardware's iDRAC baseboard management controller through the network.

Streamvault Control Panel required ports

The following table lists the ports that must be opened for outbound traffic so that the Streamvault Control Panel components can 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 following table lists the ports that must be opened for outbound traffic so that the CylancePROTECT desktop agent can 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

Outbound port	Port usage	Destination URL
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
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

NOTE: If you do not wish 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).

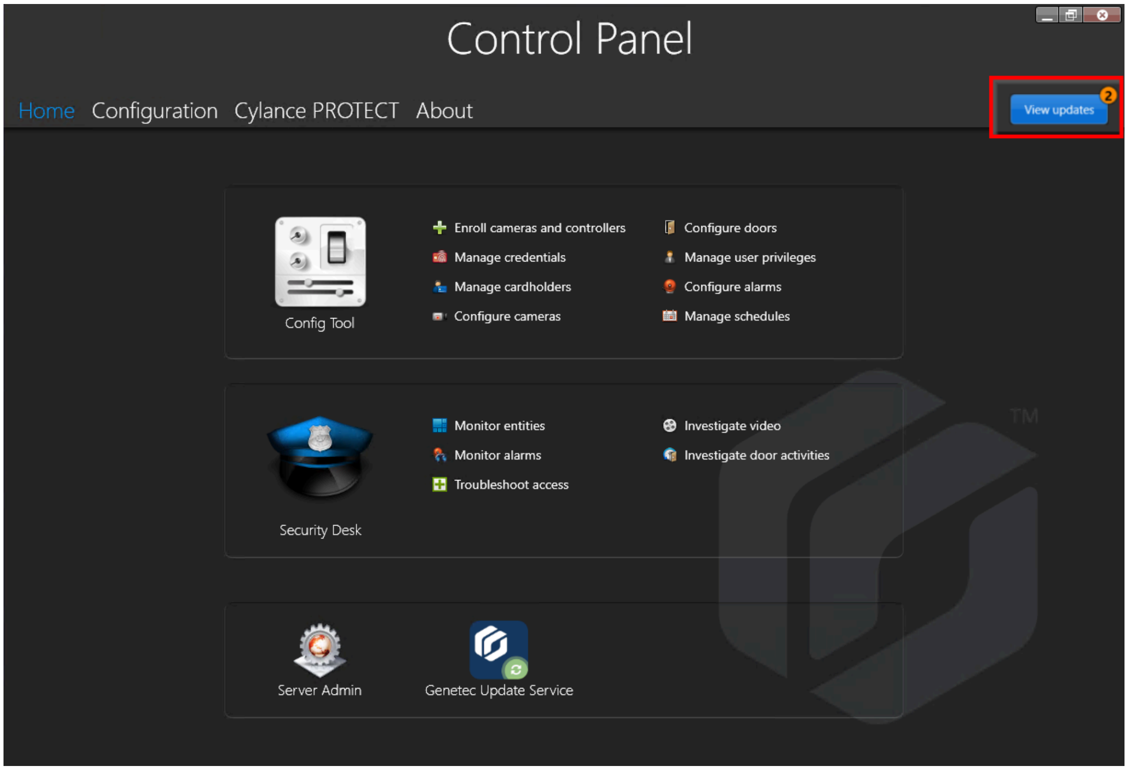
For more information about the modes in which the Streamvault appliance communicates with Genetec management services, see CylancePROTECT page of the SV Control Panel on page 58.

About updating SV software

The Genetec™ Update Service (GUS) is integrated into 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 is 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*.

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.

To connect the peripherals and power to the appliance:

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

   You must connect at least one monitor 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, and then connect the other end of the cable to the IP network RJ-45 jack.
6. For SV-100E appliances, insert the DC plug into the 19.5V input jack on the appliance and the other end to the power supply brick, and then 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

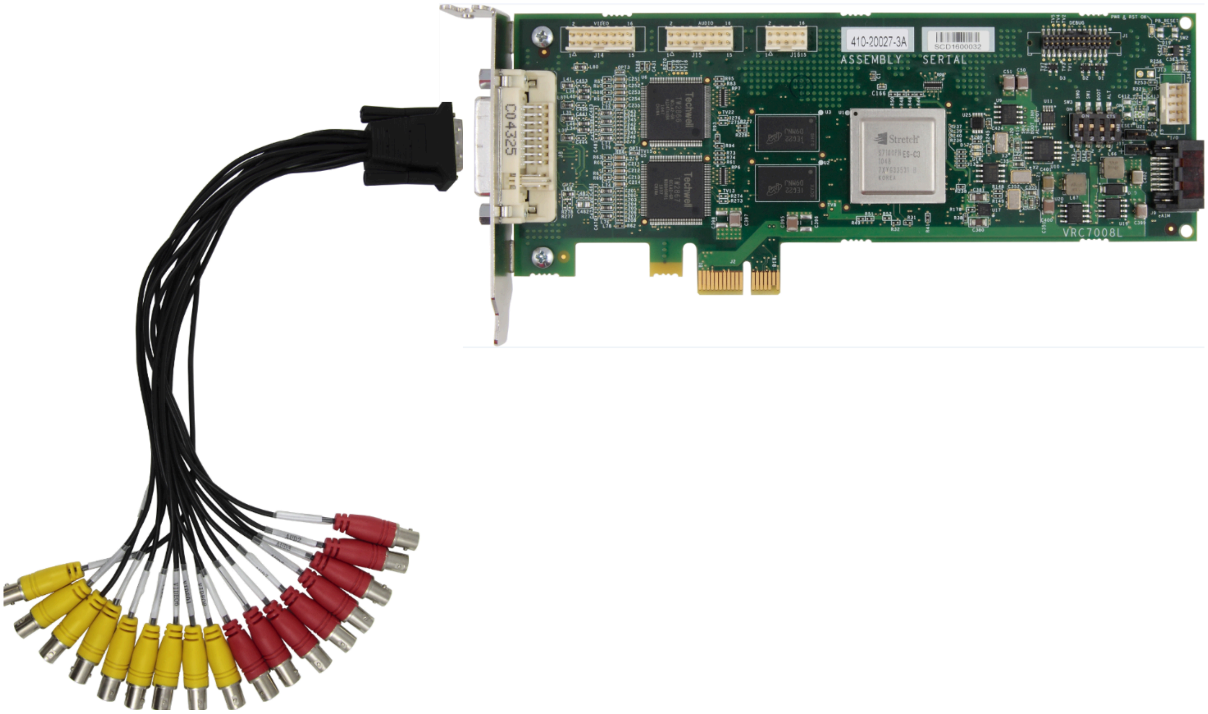
If you are using a Streamvault appliance to implement a video surveillance system with analog cameras, you must connect the cameras to the Genetec™ analog encoder card on the appliance.

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 is shipped with a breakout cable with BNC connectors 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 about the Unit enrollment tool, refer to the *Security Center Administrator Guide*.

Consider the following when adding analog cameras:

- You cannot add analog cameras in Security Center using the *Manual add* method. You must 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, all analog cameras are listed under the manufacturer *Genetec encoder card*.

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.

To disable camera inputs on encoder cards:

1. From the Config Tool home page, 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 greyed-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, and you are able to view playback from that camera.

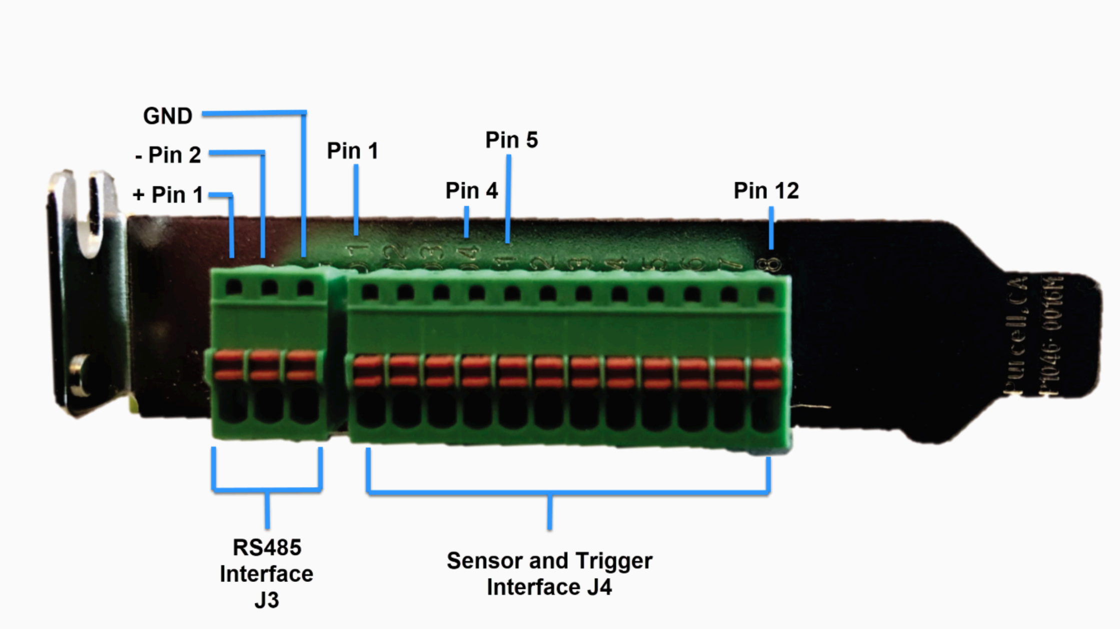
Alarm inputs and outputs of a Streamvault appliance

If you are 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

If you order a Streamvault appliance with the I/O card, you can connect the input and output wires from hardware devices directly to the I/O card on the back of the 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 appliance inputs and outputs, refer to the *Security Center Administrator Guide*.

Logging on to a Streamvault appliance

The first time you start your Streamvault™ appliance, you are prompted to change the default Admin password. You should 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

You must be logged on as an Admin user to configure your appliance in the SV Control Panel.

IMPORTANT: Passwords must meet the following requirements:

- Minimum of 10 characters
- At least three characters from the following four categories:
  - Uppercase letters
  - Lowercase letters
  - Base 10 digits (0-9)
  - Non-alphanumeric characters (such as $, %, !)

To log on to your Streamvault appliance for the first time:

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 are 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 are 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.

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
Operator	operator	• Recycle Bin • Libraries • My Computer • C: drive • SV Control Panel home page, 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	Not applicable until the SV Control Panel are completed. **NOTE:** This option is unavailable for Workstation appliances.

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

NOTE: The Operator account is not created with a template. If you create a new user account, they will not 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 from a remote machine, you must know the server's DNS name or IP address, the web server port, and the server password. When you enter the default password, you are 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.

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

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 made in the SV Control Panel 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 main 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.
- The option to enable and disable Genetec™ Mobile and Synergis™ Softwire from the *Features* section of the *Configuration* page, if they are installed on the appliance.
- Links to GTAP and product documentation.
- CylancePROTECT communication configuration page to choose the mode in which your Streamvault™ appliance communicates with the cloud Console.
- The ability to create additional Archiver roles and partitions for setups on expansion servers.

NOTE: Guide applicable to Streamvault Control Panel version 2.8 and earlier.

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 are not prompted to change any user passwords.

To set up your appliance:

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 SV Control Panel.
2. On the *Introduction* page, click **Next**.

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

   a) For an appliance with two network interface cards, select the card you want to configure from the **Network interface** list.

      The **Network interface** list is hidden when only one network interface card is connected.

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

   c) If you want to specify the IP settings, click **Use static configuration**, and enter a unique IP address for this appliance.

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

   e) 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, from the *Computer setup* page, click **Next**.

6 On the *Security* page, change the password the admin user enters to log on to Windows.

   By default, this password is also used to log on to all Genetec™ applications. You are not prompted to change any passwords on an appliance that is a Security Center expansion server.

7 In the **Security** section, configure passwords by clicking **Modify password** for the following applications:

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

8 Configure the following security settings, and then click **Next**:

   - **Automatic logout:** Turn on this option to configure Windows to log off a user after 15 minutes of inactivity.
   - **Password complexity:** Turn on this option to require a complex password of at least 10 characters for Windows users.
   - **Server management functions:** Turn on this option to allow functions such as adding roles and other tasks using applications such as *Windows Admin Center*, *Server Manager*, or *Windows PowerShell*.
   - **Removable storage access:** Turn on this option to enable access to a connected USB key or USB hard disk from Windows.

     NOTE: Users with administrative privileges automatically have removable storage access.
   - **Enable Smart Cards support:** Turn on this option to create or use a smart card reader with the Security Desk application. To prevent malicious software from affecting the device, this option has been turned off by default.
   - **Incoming remote connections:** Turn on this option to allow access to *Remote Desktop* connections and file sharing to the appliance from your computer network. To prevent malicious software from affecting the device, this option has been turned off by default.
   - **Remote Desktop:** Turn on this option to allow people in your network to log on to the appliance using a *Remote Desktop* application. The **Incoming remote connections** option must also be turned on to allow access for *Remote Desktop*. To prevent malicious software from affecting the device, this option has been turned off by default.
   - **File sharing:** Turn on this option to share files and folders that are on the appliance with people in your network. The **Incoming remote connections** option must also be turned on to allow file sharing. To prevent malicious software from affecting the device, this option has been turned off by default.

9 Read the information on the *About CylancePROTECT* page and click **Next**.

10 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.

IMPORTANT: When CylancePROTECT is turned off, you cannot change between **Disconnected** and **Online**. To change these settings, you must reset the software image on your appliance.

11 To access logs and advanced features for your system, select **Run CylancePROTECT in Advanced UI Mode**.

12 Click **Next**.

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

- **Do not collect data:** The System Availability Monitor Agent is installed but does not 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 cannot 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).

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

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

The **Start the activation wizard after setup** option is selected by default. If you clear it, you are reminded to activate the product at a later time.

NOTE: Your appliance must be activated before use.

After you finish

Activate your appliance.

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 appliances that are expansion servers or workstations.

To activate your Security Center license using a System ID:

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 not currently 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 at the moment, the update check might fail with 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 19
About page of the SV Control Panel on page 59
License information on page 59

Activating a license manually from Server Admin

If your Streamvault™ appliance does not have Internet access, you must activate your Security Center license manually from Server Admin.

To activate a license manually from Server Admin:

1 Save the validation key:

a) From your appliance, open the SV Control Panel.

b) From the *Home* page, click the **Server Admin** icon.

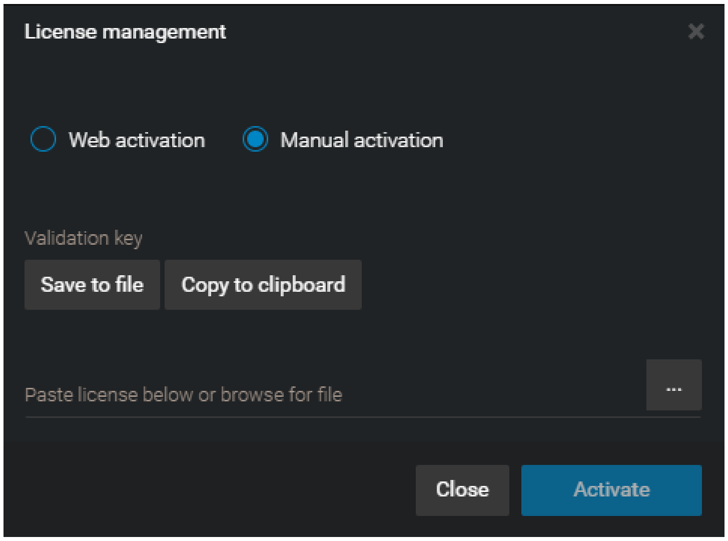
c) Log on to Server Admin.

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*.



○ Web activation ● Manual activation

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 on 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, in the *License information* section, click **Activate license**.

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 17

Activating System Availability Monitor

To monitor your system availability and health issues on GTAP, you can set the 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, as described in the *System Availability Monitor User Guide*.

To activate the System Availability Monitor Agent:

1. Open the SV Control Panel.
2. From the *Configuration* page, under the *System Availability Monitor* section, click **Configure**.
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 surveillance 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

To enable Security Center video and access control features:

1. Log on using 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 does not support a feature, it is unavailable in the list.

4. On the *Camera security* page, specify the default username and password that is 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 does not 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 cannot 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) using 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 cannot 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. In addition, 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 does not have access to other Security Center applications, for example, Config Tool, and Security Desk. The Patroller user cannot 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 the user profiles in the **Users** view of the *User Management* task. For more information, see the *Security Center Administrator Guide*.
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 at a later time by clicking the **Enroll cameras and controllers** shortcut on the *Home* page of the SV Control Panel.

After you finish

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

Related Topics

Configuring default camera settings on page 27

Creating custom recording schedules on page 29

Home page of the SV Control Panel on page 51

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*.

Related Topics

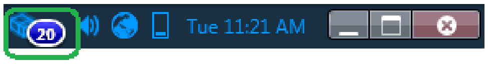
Config Tool shortcuts in the SV Control Panel on page 51

Opening the Unit enrollment tool

There are three ways to open the Unit enrollment tool.

To open the Unit enrollment tool:

- Do one of the following:
  - From the *Home* page of the SV Control Panel, click **Enroll cameras and controllers**.
  - From the *Home* page of the SV Control Panel, click the **Config Tool** icon, and then click **Tasks** > **Unit enrollment**.
  - From the *Home* page of the SV Control Panel, 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.

To configure your discovery settings:

1. From the home page, click **Tools** > **Unit enrollment**.
2. In the *Unit enrollment* dialog box, click **Settings and manufacturers** (⚙).
3. Configure the following options:
   - **Always run extensive search**. Turn this on if you want all units on the system to be discovered.

     NOTE: Units from other manufacturers may also be discovered because UPnP and *Zero config* are also used in the discovery process.
   - **Refuse basic authentication** (video units only). Use this switch to enable or disable basic authentication. 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 enroll a camera that only supports basic authentication. To turn basic authentication back on, you must switch the **Refuse basic authentication** option to **Off**.

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

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

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

5 Configure the individual settings for any manufacturers 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 26).

7 Click **Save**.

Adding units

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

To add a unit:

1 From the home page, 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 on 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.

To clear added units:

1 Add the desired discovered units to your system, see Adding units on page 25.

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.

To ignore a unit:

1 From the home page, 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 26.

Removing units from list of ignored units

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

To remove a unit from the list of ignored units:

1 From the home page, 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.

To configure the default camera settings:

1. From the Config Tool home page, 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 does not 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 cannot support a High resolution, it uses the highest resolution it can support from the Standard group.
4. Under **Recording**, click ➕ to add a schedule.

   The schedules that are available include schedules that were created using the **Schedules** view in the *System* task or the 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 recording to continue after a motion event. During this time, the recording cannot be stopped by the user.
- **Default manual recording length:** Set the number of minutes that you want to record when recording is started by a user. The user can stop the recording 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 22

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.

To set up a schedule:

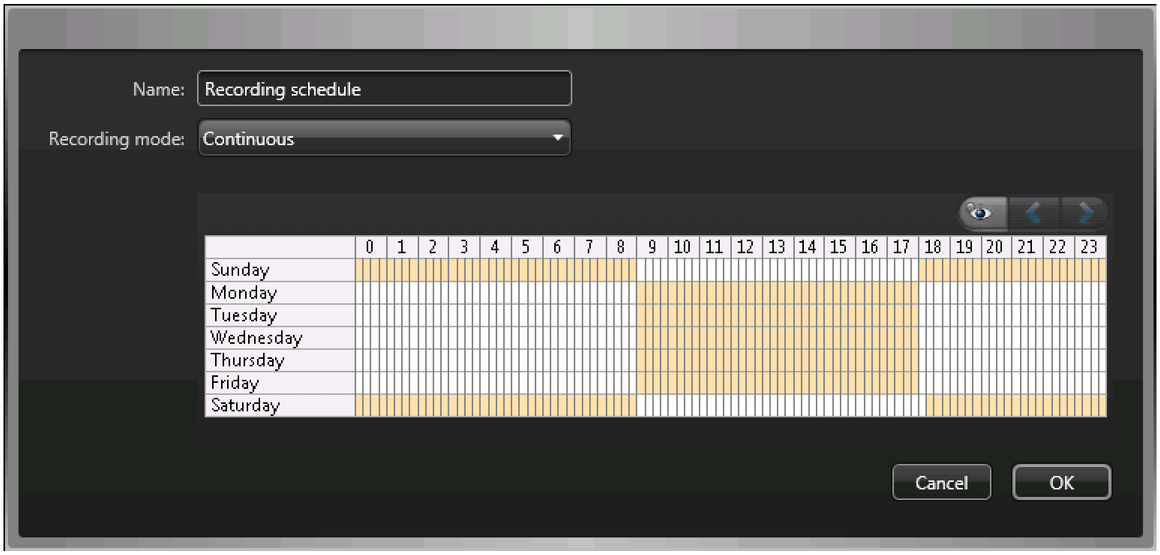
1. On the *Recording settings* page, click ➕ under **Recording schedule**.
2. Enter a name for the new schedule.
3. From the **Recording mode** list, select one of the following:
   - **Off:** Recording is off.
   - **Continuous:** Cameras record continuously. This is the default setting.
   - **On motion/Manual:** 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.



Name: Recording schedule

Recording mode: Continuous

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sunday	▨	▨	▨	▨	▨	▨	▨	▨	▨										▨	▨	▨	▨	▨	▨
Monday										▨	▨	▨	▨	▨	▨	▨	▨	▨						
Tuesday										▨	▨	▨	▨	▨	▨	▨	▨	▨						
Wednesday										▨	▨	▨	▨	▨	▨	▨	▨	▨						
Thursday										▨	▨	▨	▨	▨	▨	▨	▨	▨						
Friday										▨	▨	▨	▨	▨	▨	▨	▨	▨						
Saturday	▨	▨	▨	▨	▨	▨	▨	▨	▨										▨	▨	▨	▨	▨	▨

Related Topics

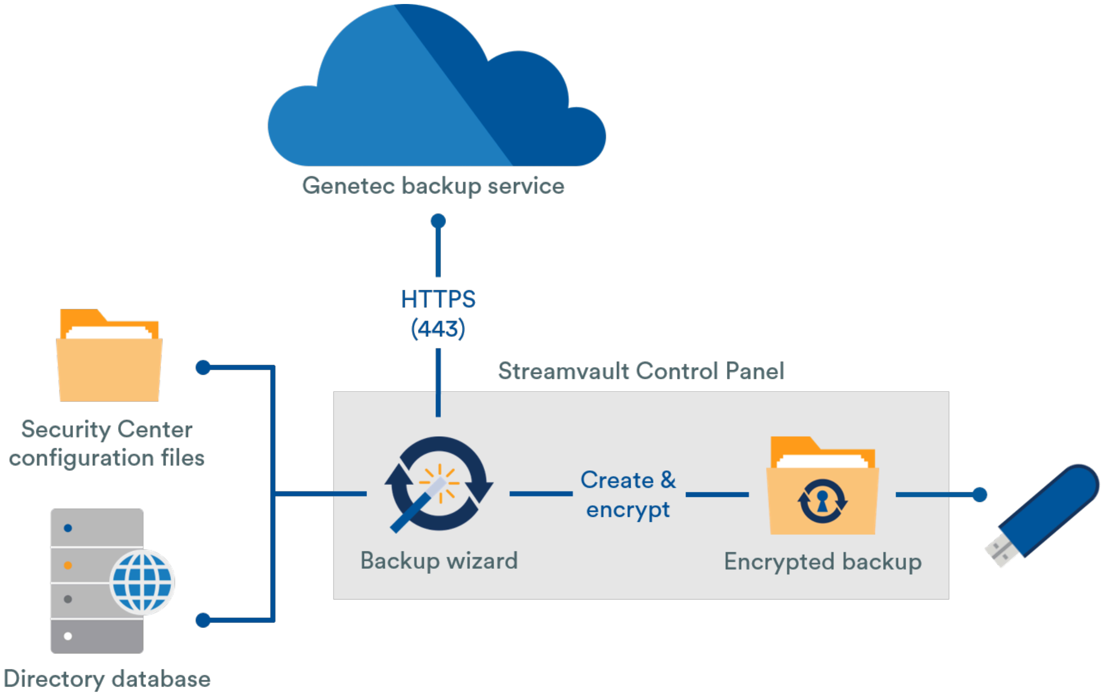
Enabling Security Center video and access control features on page 22

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 do not 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 cannot restore a backup on an earlier version of Security Center. For example, you cannot restore a backup from a Security Center 5.6 system to a Security Center 5.5 system.
- You cannot restore the configuration files if you are restoring across major versions of Security Center. For example, you cannot restore the configuration files from a Security Center 5.5 system backup to a Security Center 5.6 system.

Related Topics

Backing up your Directory database on page 31
Restoring your Directory database on page 32

Backing up your Directory database

To make configuring your system easier after a hardware upgrade, or to restore your configurations after a system failure, you can safely back up your Directory database and configuration files using backup and restore.

Before you begin

Make sure of the following:

- Security Center 5.5 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.

To back up your Directory database and configuration files:

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**.
   - **Cloud**. 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 have entered your credentials the first time, you will not be asked again for future backups.
     b. On the *Security* page, select one of the following two options:
        - **Let Genetec manage my security:** You do not need to provide a password. The backup cloud service from Genetec Inc. encrypts your data.
        - **Use my own password:** You must create and remember your own password to use later for the encryption of your backup files.
          IMPORTANT: If you lose or forget your password, it is not possible for Genetec Inc. to recover the lost password.
   - **Local**. 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 is not recommended.
4. Follow the rest of the steps in the wizard to complete your backup.

Related Topics

About backup and restore on page 30
Restoring your Directory database on page 32

Restoring your Directory database

If you have backed up your Directory database and configuration files using backup and restore in the SV Control Panel, you can easily restore your backup files to the same System ID in events such as a system failure or hardware upgrade.

Before you begin

Make sure of the following:

- Security Center 5.5 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 will need it to restore your files.

To restore your Directory database and configuration files:

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 31
About backup and restore on page 30

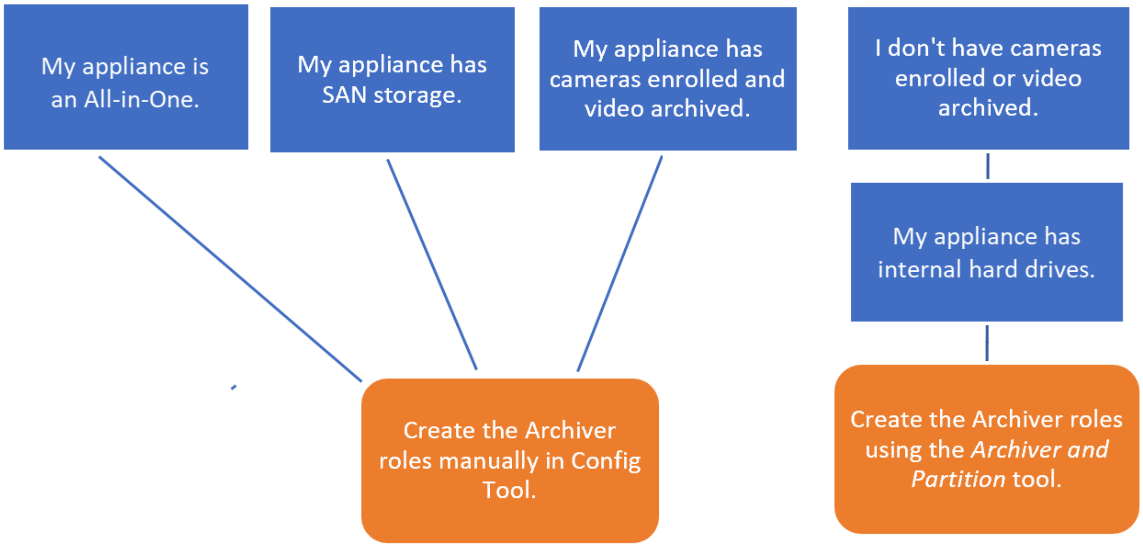
Choosing the method for creating Archiver roles and partitions

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:


My appliance is an All-in-One.
My appliance has SAN storage.
My appliance has cameras enrolled and video archived.
I don't have cameras enrolled or video archived.
My appliance has internal hard drives.
Create the Archiver roles manually in Config Tool.
Create the Archiver roles using the *Archiver and Partition* tool.

About the Archiver Roles and Partitions tool in the SV Control Panel

The Archiver Roles and Partitions tool calculates how many Archiver roles you need based on the number of cameras you plan to deploy and their expected bandwidth.

This tool is only available on Streamvault™ models that have an internal hard drive. If you are setting up an external storage device, such as SAN on a SV-7000E series appliance, follow the steps in Manually adding partitions and Archiver roles on page 35.

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

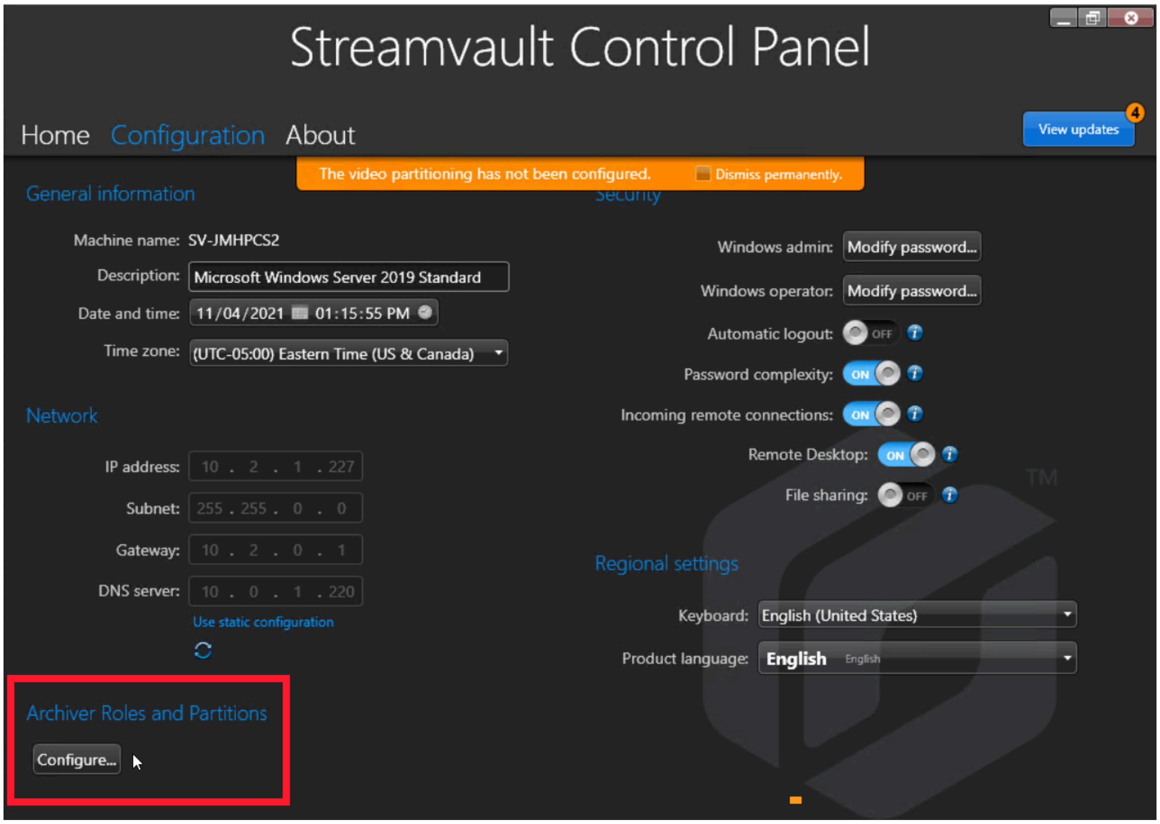
- Choose the appropriate method for creating Archiver roles and partitions.

- 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.

To create additional Archiver roles and drive partitions:

1. In the SV Control Panel, click the **Configuration** tab.
2. Under *Archiver Roles and Partitions*, click **Configure**.



The video partitioning has not been configured. □ Dismiss permanently.

General information

Machine name: SV-JMHPCS2

Description: Microsoft Windows Server 2019 Standard

Date and time: 11/04/2021 01:15:55 PM

Time zone: (UTC-05:00) Eastern Time (US & Canada)

Network

IP address: 10 . 2 . 1 . 227

Subnet: 255 . 255 . 0 . 0

Gateway: 10 . 2 . 0 . 1

DNS server: 10 . 0 . 1 . 220

Use static configuration

Archiver Roles and Partitions

Configure...

Security

Windows admin: Modify password...

Windows operator: Modify password...

Automatic logout: OFF

Password complexity: ON

Incoming remote connections: ON

Remote Desktop: ON

File sharing: OFF

Regional settings

Keyboard: English (United States)

Product language: English English

The *Archiver Roles and Partitions* dialog box opens.

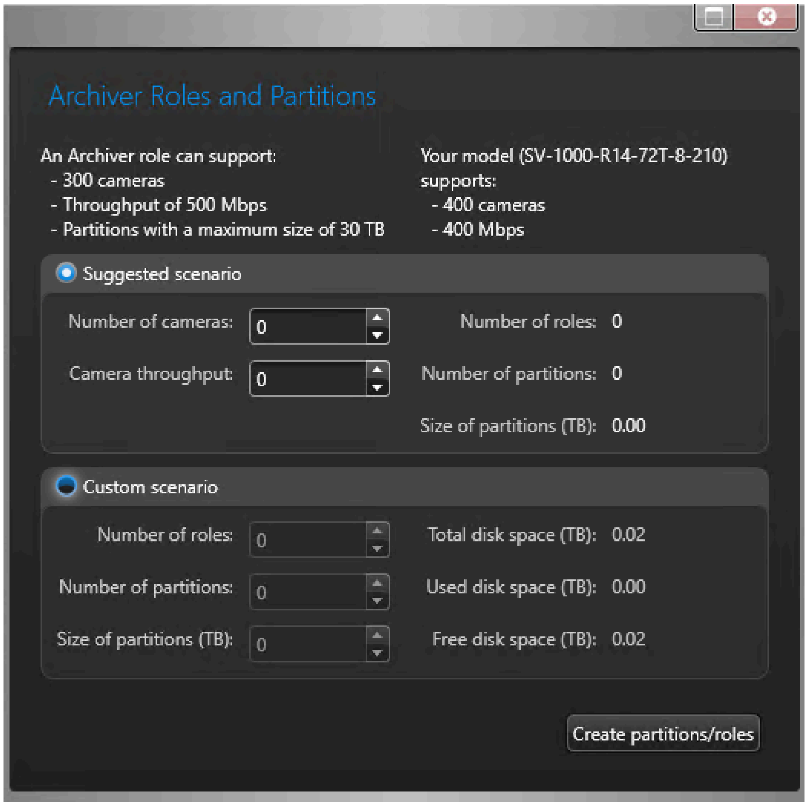
3. Select one of the following options to configure the number of Archiver roles and partitions:

   - 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 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**.



Archiver Roles and Partitions

An Archiver role can support:
- 300 cameras
- Throughput of 500 Mbps
- Partitions with a maximum size of 30 TB

Your model (SV-1000-R14-72T-8-210) supports:
- 400 cameras
- 400 Mbps

● Suggested scenario

Number of cameras: 0

Camera throughput: 0

Number of roles: 0

Number of partitions: 0

Size of partitions (TB): 0.00

○ Custom scenario

Number of roles: 0

Number of partitions: 0

Size of partitions (TB): 0

Total disk space (TB): 0.02

Used disk space (TB): 0.00

Free disk space (TB): 0.02

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.

Manually adding partitions and Archiver roles

To set up your SV-7000E 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.

To distribute cameras across multiple Archiver roles:

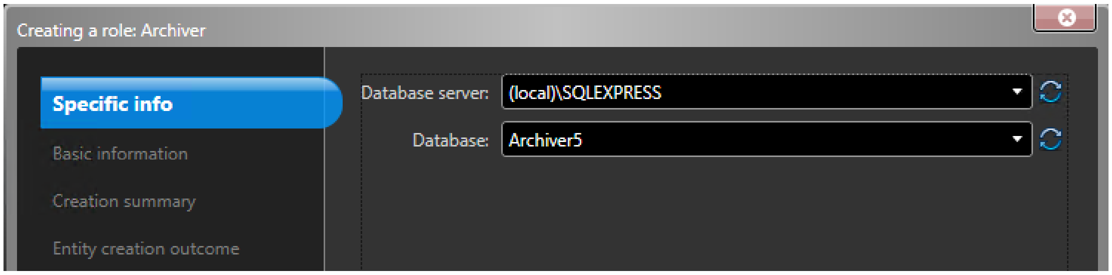
1 If the appliance already has cameras enrolled, video archived, or access control data, do the following:

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. See "Viewing camera settings" in the *Security Center User Guide*.

2 Create the volumes that you need for the Archiver roles you plan to create on the appliance.
   - On appliances that have SAN storage, such as SV-7000E 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.

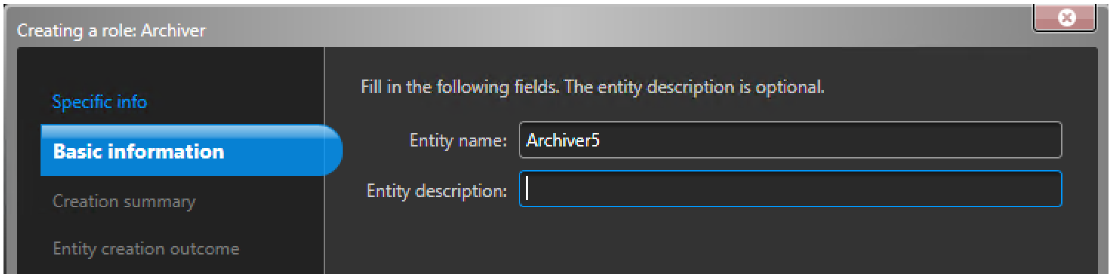


Creating a role: Archiver

Database server: (local)\SQLEXPRESS

Database: Archiver5

   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.



Creating a role: Archiver

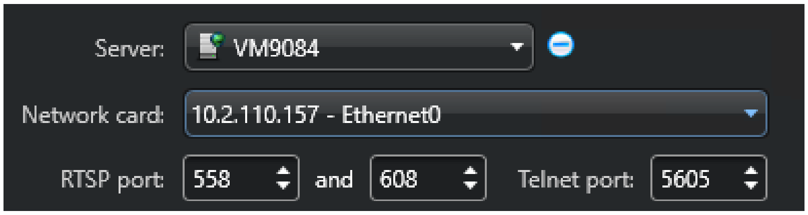
Fill in the following fields. The entity description is optional.

Entity name: Archiver5

Entity description:

   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 NIC from the **Network card** list.
      All Archiver roles must use the same NIC.



Server: VM9084

Network card: 10.2.110.157 - Ethernet0

RTSP port: 558 and 608 Telnet port: 5605

   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 there should never be two roles using 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.

The Streamvault Maintenance plugin includes the following components:

- Streamvault role: Plugin role used to run either the hardware monitor or manager entity. One role per Streamvault appliance you need to monitor is required.
- *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**, level of **Severity**, and types of **Notification** that affect alerts addressing the health status' 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.
- **iDRAC integration**: used to exercise more precise control over credential management. This feature can be found in the **Management** tab of the plugin.

  IMPORTANT:

  - iDRAC firmware must be at version 6.0 or later.
  - The Streamvault Maintenance plugin accesses health data using out-of-band communication with iDRAC. This means that there must be a network connection between the iDRAC dedicated port and at least one LAN port if port sharing is not 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.
  - Configuration using iDRAC is not relevant for most users. For more information, contact the Streamvault product team.
  - Guide applicable for Streamvault Maintenance plugin 1.0.

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 of the following:

- A compatible version of Security Center is installed.

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 using DHCP.
- **IMPORTANT:** Ensure the iDRAC module is updated to firmware 6.00 or later, and that the server BIOS is updated to the latest version before proceeding.
- The plugin is only supported 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.

To install the plugin:

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 do not 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*.

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™ hardware monitor entities. Only one Streamvault™ manager is allowed per system.
- **NOTE:** If the Directory servers are virtual machines or non-Streamvault servers, you must create a role for these servers only if you wish to use the Manager entity.

To create a plugin role:

1 From the Config Tool home page, 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 do not use expansion servers in your system, the **Server** option is not 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 do not use partitions in your system, the **Partition** option is not 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.

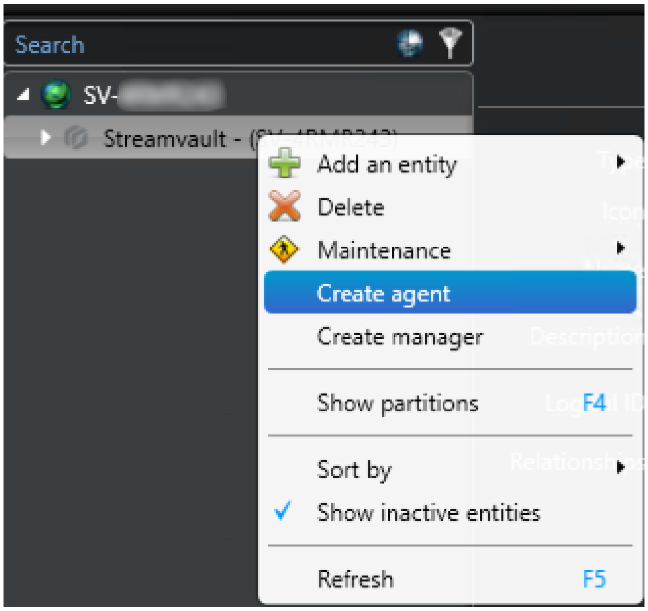
Before you begin

- Enroll your Streamvault appliances.
- Create the Streamvault Plugin role.
- **IMPORTANT:** An agent is automatically created on each Streamvault server that is hosting a Streamvault role. If the agent is not present in your system after you have created the role, you must create the agent manually.

To configure a Streamvault hardware monitor entity:

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

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

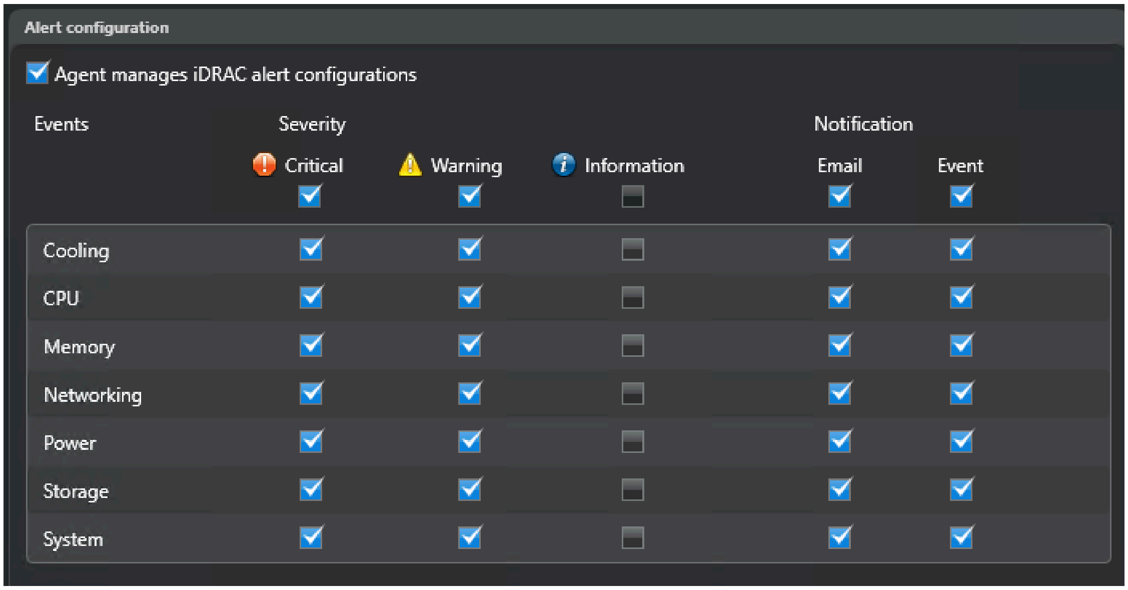


3 From the **Identity** tab, enter a name for the Streamvault hardware monitor in the **Name** field.

4 From the **General** tab, configure the following:

a) To manage alert configurations through the Streamvault hardware monitor role configurations, activate the **Agent manages iDRAC alert configurations** checkbox.

b) In the **Alert notification** section, activate the checkboxes that correlate with the types of **Events**, level of **Severity**, and types of **Notifications** that you want to include for this Streamvault hardware monitor.



Alert configuration

☑ Agent manages iDRAC alert configurations

Events	Severity			Notification	
	Critical	Warning	Information	Email	Event
	☑	☑	□	☑	☑
Cooling	☑	☑	□	☑	☑
CPU	☑	☑	□	☑	☑
Memory	☑	☑	□	☑	☑
Networking	☑	☑	□	☑	☑
Power	☑	☑	□	☑	☑
Storage	☑	☑	□	☑	☑
System	☑	☑	□	☑	☑

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

6 (Optional) In the **Remote management credentials** section, activate the **Agent manages iDRAC account** checkbox to manage credentials directly through the plugin.

7 (Optional) In the **Remote management credentials** section, deactivate the **Agent manages iDRAC account** checkbox to use iDRAC to control user and password creation.

8 (Optional) If you deactivated the **Agent manages iDRAC account** checkbox, navigate to the **Management** tab and configure credentials directly in iDRAC.

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

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 and set up notifications to be raised when problems occur. The Streamvault manager entity is only used for this and is optional.

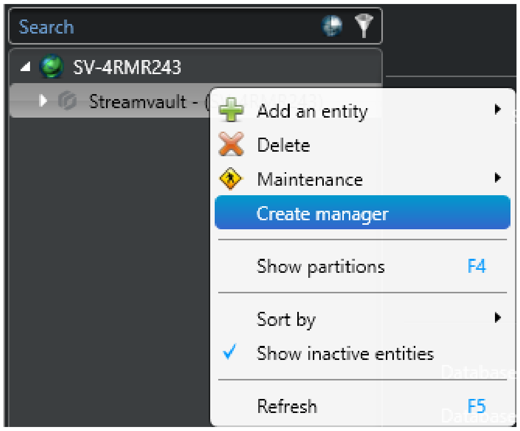
Before you begin

- Enroll your Streamvault devices.
- Create the Streamvault Plugin role.

To configure a Streamvault manager entity:

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

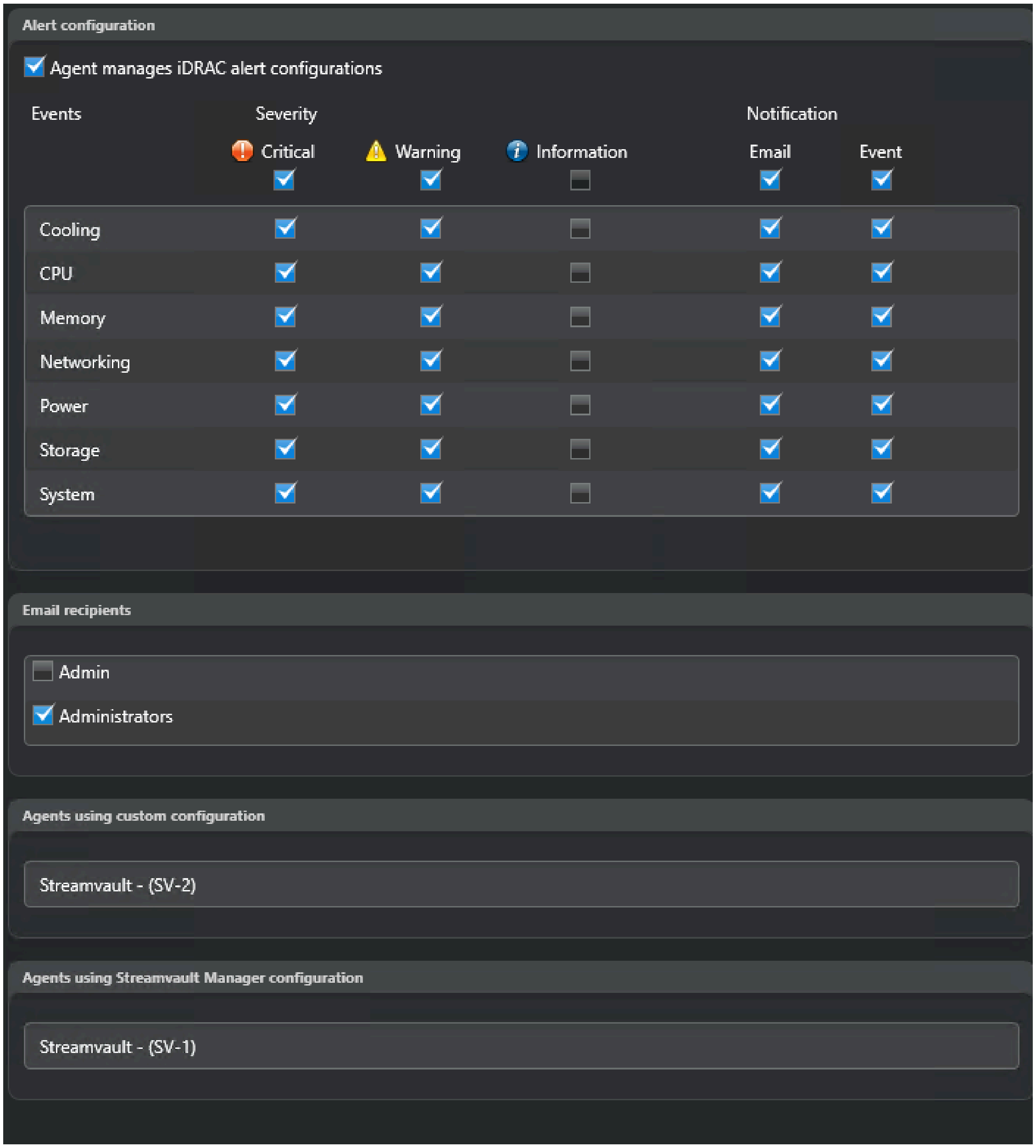
2 Right click on the Streamvault plugin role and click **Create manager**.



3 From the **General** tab, configure the following:

a) To manage alert configurations through the Streamvault manager configurations, activate the **Agent manages iDRAC alert configurations** checkbox.

b) In the **Alert notification** section, activate the checkboxes that correlate with the types of **Events**, level of **Severity**, and types of **Notifications** that you want to include for the Streamvault Maintenance plugin instances controlled by this Streamvault manager.



Alert configuration

☑ Agent manages iDRAC alert configurations

Events	Severity			Notification	
	Critical	Warning	Information	Email	Event
	☑	☑	□	☑	☑
Cooling	☑	☑	□	☑	☑
CPU	☑	☑	□	☑	☑
Memory	☑	☑	□	☑	☑
Networking	☑	☑	□	☑	☑
Power	☑	☑	□	☑	☑
Storage	☑	☑	□	☑	☑
System	☑	☑	□	☑	☑

Email recipients

□ Admin

☑ Administrators

Agents using custom configuration

Streamvault - (SV-2)

Agents using Streamvault Manager configuration

Streamvault - (SV-1)

NOTE: Streamvault instances that have their configurations set by the Streamvault manager are shown in the **Agents using Streamvault manager configuration** section.

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

5 (Optional) In the **Remote management credentials** section, activate the **Agent manages iDRAC account** checkbox to manage credentials directly through the plugin.

6 (Optional) In the **Remote management credentials** section, deactivate the **Agent manages iDRAC account** checkbox to use iDRAC to control user and password creation.

7 (Optional) If you deactivated the **Agent manages iDRAC account** checkbox, navigate to the **Management** tab and configure credentials directly in iDRAC.

Reviewing Streamvault appliance health

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

To view the health status of your Streamvault appliances:

1 From the home page, 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 the Reporting task workspace overview.

4

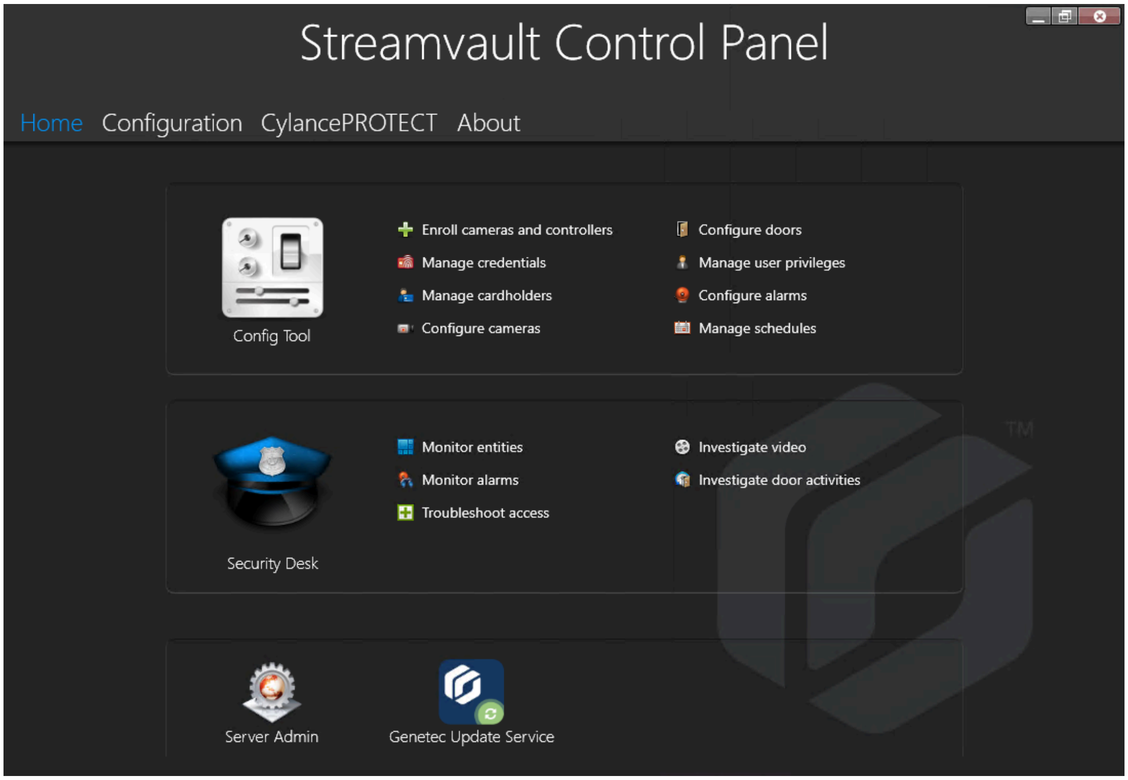
SV Control Panel reference

These reference pages help you understand the SV Control Panel.

This section includes the following topics:

Home page of the SV Control Panel

Use the *Home* page to access the basic tasks 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.

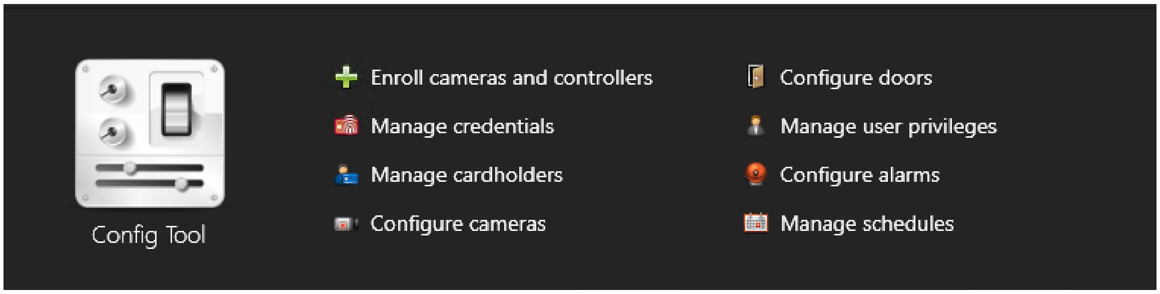
For systems running in Client mode, the Server Admin shortcut is unavailable. Likewise, the Config Tool and Security Desk shortcuts are limited.

NOTE: If your system is not activated, you are notified by a red banner. Click **The system is not activated. Click here to activate.** to open the *Streamvault Control Panel activation* wizard.

Config Tool shortcuts in the SV Control Panel

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.



- **Config Tool:** Click the icon to open Config Tool.

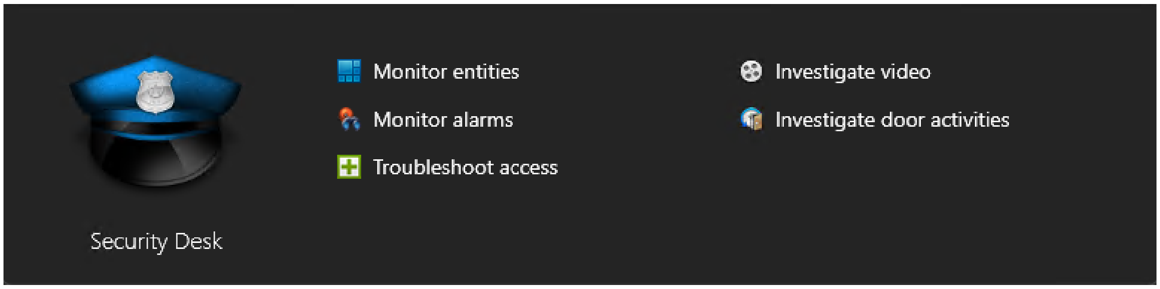
Related Topics

About the Unit enrollment tool on page 24

Security Desk shortcuts in the SV Control Panel

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.



- **Security Desk:** Click the icon to open Security Desk.
- **Monitor entities:** Click to open the *Monitoring* task to monitor system events in real-time.
- **Monitor alarms:** Click to open the *Alarm monitoring* task to monitor and respond to active alarms, and view past alarms.
- **Troubleshoot access:** Click to open the Access troubleshooter tool, to diagnose and access configuration problems.

  NOTE: This shortcut is unavailable for systems running in Client mode.
- **Investigate video:** Click to open the *Archives* task to search for video archives.

  NOTE: This shortcut is unavailable for systems running in Client mode.
- **Investigate door activities:** Click to open the *Door activities* task to investigate events at selected doors.

  NOTE: This shortcut is unavailable for systems running in Client mode.

Server Admin in the SV Control Panel

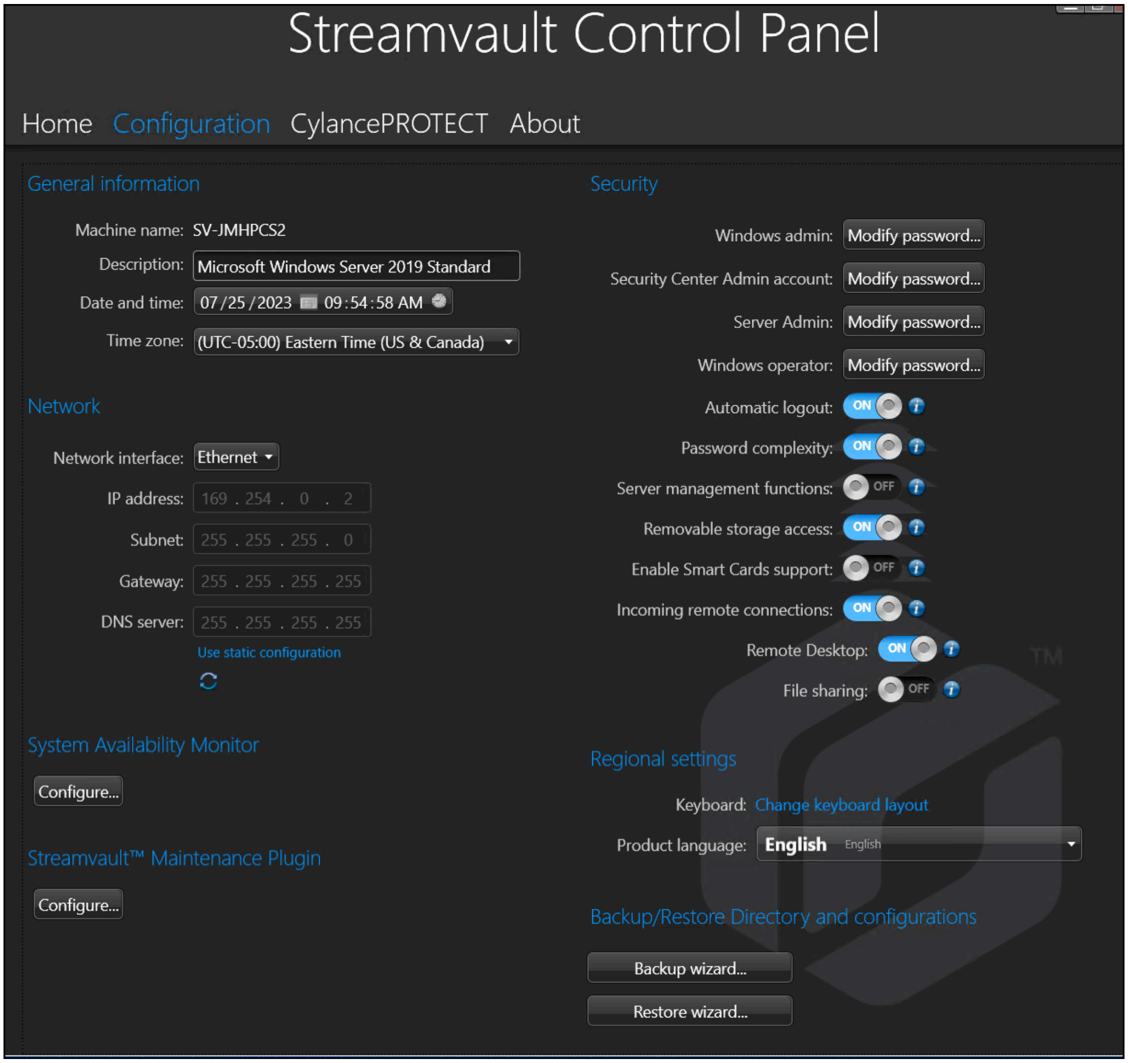
Use the Server Admin application to manually apply a license, or view and change the configuration of the server.

Genetec Update Service in the SV Control Panel

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

Configuration page of the SV Control Panel

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



General information

Machine name: SV-JMHPCS2

Description: Microsoft Windows Server 2019 Standard

Date and time: 07 /25 /2023 09 :54 :58 AM

Time zone: (UTC-05:00) Eastern Time (US & Canada)

Network

Network interface: Ethernet

IP address: 169 . 254 . 0 . 2

Subnet: 255 . 255 . 255 . 0

Gateway: 255 . 255 . 255 . 255

DNS server: 255 . 255 . 255 . 255

Use static configuration

System Availability Monitor

Configure...

Streamvault™ Maintenance Plugin

Configure...

Security

Windows admin: Modify password...

Security Center Admin account: Modify password...

Server Admin: Modify password...

Windows operator: Modify password...

Automatic logout: ON

Password complexity: ON

Server management functions: OFF

Removable storage access: ON

Enable Smart Cards support: OFF

Incoming remote connections: ON

Remote Desktop: ON

File sharing: OFF

Regional settings

Keyboard: Change keyboard layout

Product language: English English

Backup/Restore Directory and configurations

Backup wizard...

Restore wizard...

For systems running on an expansion server or in Client mode, the *System Availability Monitor*, *Features*, and *Backup/Restore Directory and configurations* sections are unavailable. Likewise, in the *Security* section, only the passwords for the **Windows admin** and **Windows operator** can be modified.

General information settings

Use the *General information* section of the *Configuration* page 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 list.

Network settings

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

- **Network interface:** Select the network card that you want to configure.

  NOTE: This option is not available when only one network card is connected.
- **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.
- **Use static configuration:** Click when you do not want the IP address assigned dynamically by your Dynamic Host Configuration Protocol (DHCP) server. By default, Dynamic Host Configuration Protocol (DHCP) is used to automatically assign the IP address, Subnet, Gateway, and DNS server.
- 🔄 **Refresh (DHCP only):** Click to refresh your DHCP settings and obtain a new IP address.

System Availability Monitor settings

Use the *System Availability Monitor* section of the *Configuration* page 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.

Feature information

Use the *Features* section of the *Configuration* page to display and activate the additional features you purchased.

The following features can be enabled:

- Security Center Mobile
- Synergis™ Softwire

NOTE: If Security Center Mobile or Synergis Softwire are not installed, the respective options are not displayed in the *Features* section. Security Center Mobile is only available for Security Center 5.7 and earlier. For systems running Security Center 5.8 GA and later, Security Center Mobile is activated in Config Tool.

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

Security

Use the *Security* section of the *Configuration* page to change some of the user account and system security settings for your Streamvault™ appliance.

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

Define a password for each product:

- **Windows admin:** The admin user's password for Windows.

- **Client applications:** 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.
- **Automatic logout:** Turn on this option to configure Windows to log off a user after 15 minutes of inactivity.
- **Password complexity:** Turn on this option to require a complex password of at least 10 characters for Windows users.
- **Server management functions:** Turn on this option to allow functions such as adding roles and other tasks using applications such as *Windows Admin Center*, *Server Manager*, or *Windows PowerShell*.
- **Removable storage access:** Turn on this option to enable access to a connected USB key or USB hard disk from Windows.

  NOTE: Users with administrative privileges automatically have removable storage access.
- **Enable Smart Cards support:** Turn on this option to create or use a smart card reader with the Security Desk application. To prevent malicious software from affecting the device, this option has been turned off by default.
- **Incoming remote connections:** Turn on this option to allow access to *Remote Desktop* connections and file sharing to the appliance from your computer network. To prevent malicious software from affecting the device, this option has been turned off by default.
- **Remote Desktop:** Turn on this option to allow people in your network to log on to the appliance using a *Remote Desktop* application. The **Incoming remote connections** option must also be turned on to allow access for *Remote Desktop*. To prevent malicious software from affecting the device, this option has been turned off by default.
- **File sharing:** Turn on this option to share files and folders that are on the appliance with people in your network. The **Incoming remote connections** option must also be turned on to allow file sharing. To prevent malicious software from affecting the device, this option has been turned off by default.

Regional settings

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

- **Change keyboard layout:** Click to open the *Windows Setting Panel* to change the layout of your keyboard.

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

NOTE: The SV Control Panel is only available in English.

Backup and restore

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

Backup and restore is an SV Control Panel feature that you can use to securely back up your Directory database and configuration files, and later restore them to the same System ID in the event of a system failure or hardware upgrade. This feature does not 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.

Related Topics

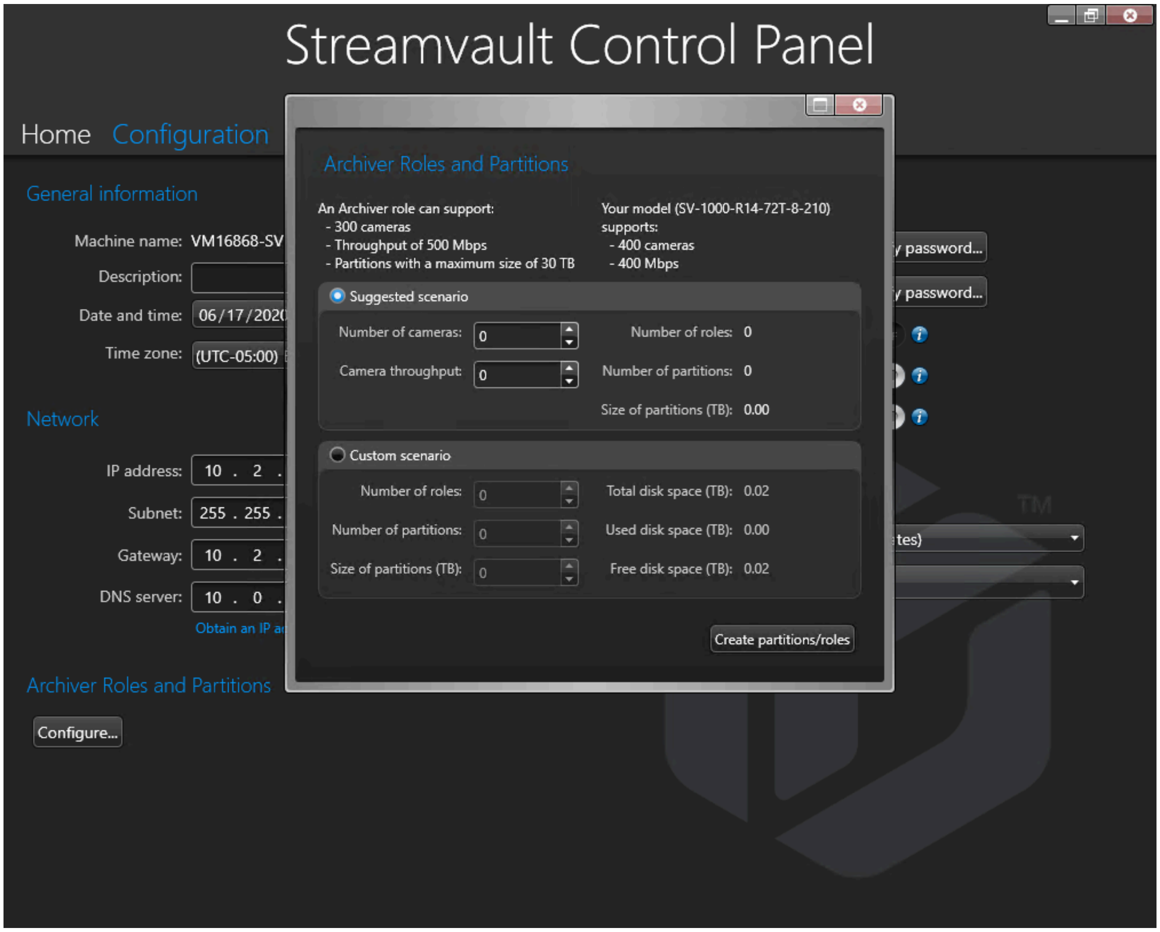
About backup and restore on page 30
Backing up your Directory database on page 31
Restoring your Directory database on page 32

Archiver Roles and Partitions

Use the *Archiver Roles and Partitions* section on the *Configuration* page to extend the maximum number of cameras supported in your system.

Archiver Roles and Partitions is an SV Control Panel feature you can use to configure systems that require more than the maximum amount of cameras and throughput supported by a single Archiver.

This section is only available for systems running on an expansion server with Security Center 5.8 and later.


Streamvault Control Panel
Home
Configuration
General information
Network
Archiver Roles and Partitions
Configure...
Archiver Roles and Partitions
Create partitions/roles

Machine name: VM16868-SV
Description:
Date and time: 06/17/2020
Time zone: (UTC-05:00)

IP address: 10 . 2 .
Subnet: 255 . 255 .
Gateway: 10 . 2 .
DNS server: 10 . 0 .
Obtain an IP a

An Archiver role can support:
- 300 cameras
- Throughput of 500 Mbps
- Partitions with a maximum size of 30 TB

Your model (SV-1000-R14-72T-8-210) supports:
- 400 cameras
- 400 Mbps

● Suggested scenario

Number of cameras: 0
Camera throughput: 0
Number of roles: 0
Number of partitions: 0
Size of partitions (TB): 0.00

○ Custom scenario

Number of roles: 0
Number of partitions: 0
Size of partitions (TB): 0
Total disk space (TB): 0.02
Used disk space (TB): 0.00
Free disk space (TB): 0.02

- **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 amount of roles, partitions, and partition size needed for your desired amount 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 33.

CylancePROTECT page of the SV Control Panel

Use the CylancePROTECT page to view information about Cylance and to choose the mode in which the Streamvault™ appliance communicates with the Cylance Console in the cloud.

You can choose between the following options:

- **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.

IMPORTANT: When CylancePROTECT is turned off, you cannot change between **Disconnected** and **Online**. To change these settings, you must reset the software image on your appliance.

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

To access logs and advanced features for your system, select **Run CylancePROTECT in Advanced UI Mode**.

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 license information, Software Maintenance Agreement (SMA) information, links to the Genetec™ Technical Assistance Portal (GTAP), and links to the product documentation.

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

License information

Use the *License* section of the *About* page to display 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 additional license information.

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

Related Topics

Activating your Security Center license on an appliance on page 17

Software Maintenance Agreement information

Use the *SMA* section of the *About* page to display information about Software Maintenance Agreement.

- **Expiration date:** Displays the expiration date of the Software Maintenance Agreement (SMA).
- **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.

System information

Use the *System* section of the *About* page to display information about the system.

- **Manufacturer:** Displays the manufacturer of the hardware.
- **Hardware model:** Displays the hardware model.
- **Software revision:** Displays the version or image of the software.
- **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 of the *About* page to access useful links to Genetec™ Technical Assistance Portal (GTAP) and product documentation.

- **GTAP:** Click the link to open GTAP and support forums.

  NOTE: You must have a valid username and password to log on to GTAP.
- **TechDoc Hub:** Click the link to open the Genetec TechDoc Hub.
- **Control Panel:** Click the link to open the *SV Control Panel User Guide*, which also contains the release notes for SV Control Panel.
- **Security Desk:** Click the link to open the *Security Center User Guide*.

5

Additional resources

This section includes the following topics:

Creating a factory reset USB key

To reset the image of a Streamvault™ SV-100E, SV-300E, SV-350E appliance, or a Streamvault server or workstation appliance, you must prepare a bootable USB key that contains the required Streamvault software image.

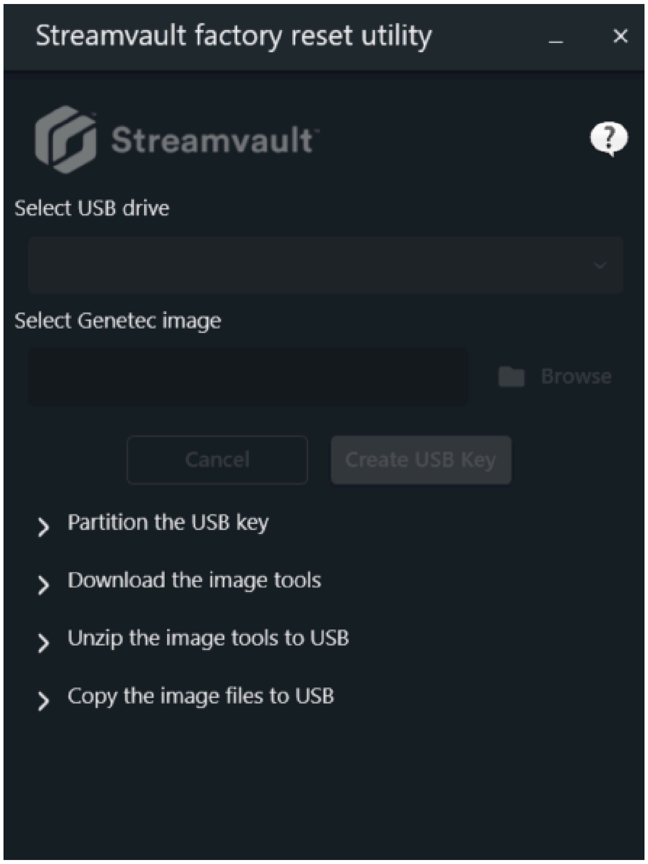
Before you begin

- Download the *Streamvault factory reset utility* from the Downloads section of the *Streamvault Appliance User Guide* on TechDoc Hub.
- Before opening the *Streamvault factory reset utility*, unzip the backup images into a Windows folder.
- Ensure that you have a USB key with a minimum of 32 GB storage.

Watch this video to learn how to create a factory reset USB key.

To create a bootable USB key with the required software image on the *Streamvault factory reset utility*:

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



2 In the *Select Genetec image* section, click **Browse** and select the required *.swm* file.

- For All-in-One appliances, select any one of the unzipped files from the *wim* folder.
- For workstations and servers, select the required image from the <*service tag number*> folder.

3 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, you will see a *Streamvault factory reset utility* message informing you that the USB key was created successfully.

After you finish

- For an SV-100E, SV-300E, or SV-350E appliance, reset the software on the appliance.
- For a workstation or server appliance, reset the image of the Streamvault appliance using the bootable USB key.

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.

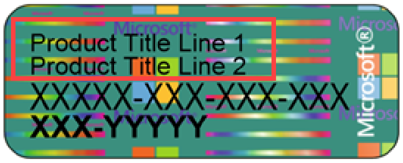
For a detailed description of the terms and conditions of the Genetec™ product warranty, refer to the Genetec™ Product Warranty Overview.

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 for products that contain embedded versions of Microsoft software.



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 software revision number of a Streamvault appliance

When contacting Genetec™ Technical Support, you need the System ID and the software revision number (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 software revision number, Genetec Technical Support might request the certification number and serial number. To find this information, look for a label on the Streamvault appliance.

To find the System ID and image version of your appliance:

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 **Software revision** number.

Related Topics

Performing a factory reset on an SV-100E, SV-300E, or SV-350E appliance on page 70

Performing a factory reset on a Streamvault workstation or server appliance on page 73

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 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.

To enables file sharing on your appliance:

1. On the *Configuration* page of SV Control Panel:
   - Turn on the **Incoming remote connections** option.
   - Turn on the **File sharing** 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.

To allow Remote Desktop connections to your Streamvault™ appliance:

1. On the *Configuration* page of SV Control Panel:
   - Turn on the **Incoming remote connections** option.
   - Turn on the **Remote Desktop** option.
2. Click **Apply**.

Related Topics

Remote Desktop cannot connect to a Streamvault appliance on page 78

6

Troubleshooting

This section includes the following topics:

Performing a factory reset on an SV-100E, SV-300E, or SV-350E appliance

If the software on an SV-100E, SV-300E, or SV-350E appliance 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 31.
- 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.
- (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

- For appliances with model numbers other than SV-100E, SV-300E, and SV-350E, see Performing a factory reset on a Streamvault workstation or server appliance on page 73.
- A factory reset deletes and overwrites all data currently on the Windows drive (C:), including databases and logs.

To perform a factory reset on an SV-100E, SV-300E, or SV-350E series appliance:

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

Set up your appliance.

Related Topics

Finding the system ID and software revision number of a Streamvault appliance on page 66

Resetting the software image on an SV-100E, SV-300E, or SV-350E appliance using a bootable USB

You can reset the software image using a USB recovery drive.

Before you begin

- Have the USB key that contains the recovery software image for your appliance.
- 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

- A factory reset deletes and overwrites all data currently on the Windows drive (C:), including databases and logs.

  CAUTION: Only the files on C: are deleted, but we advise you to back up the video files on all your drives.
- Resetting takes approximately 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.

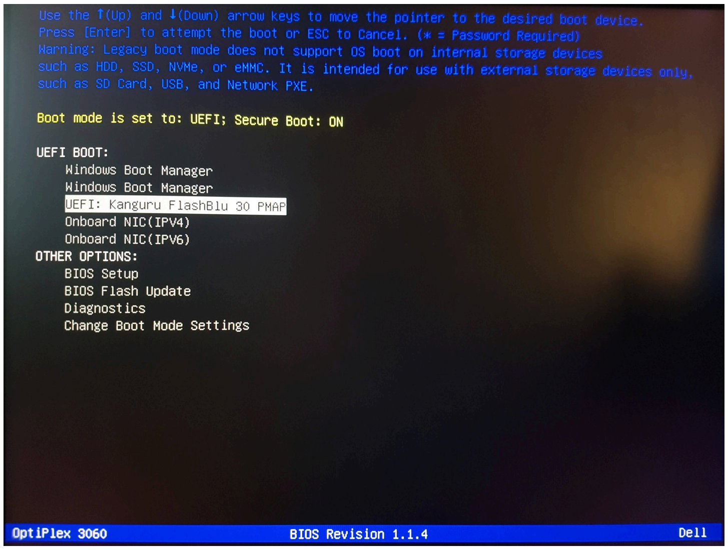
Watch this video to learn how to reset the software image on an SV-100E, SV-300E, or SV-350E appliance using a bootable USB.

To reset the SV-100E, SV-300E, or SV-350E series appliance image:

1 Shut down the appliance.

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

3 Select the USB drive and press Enter.



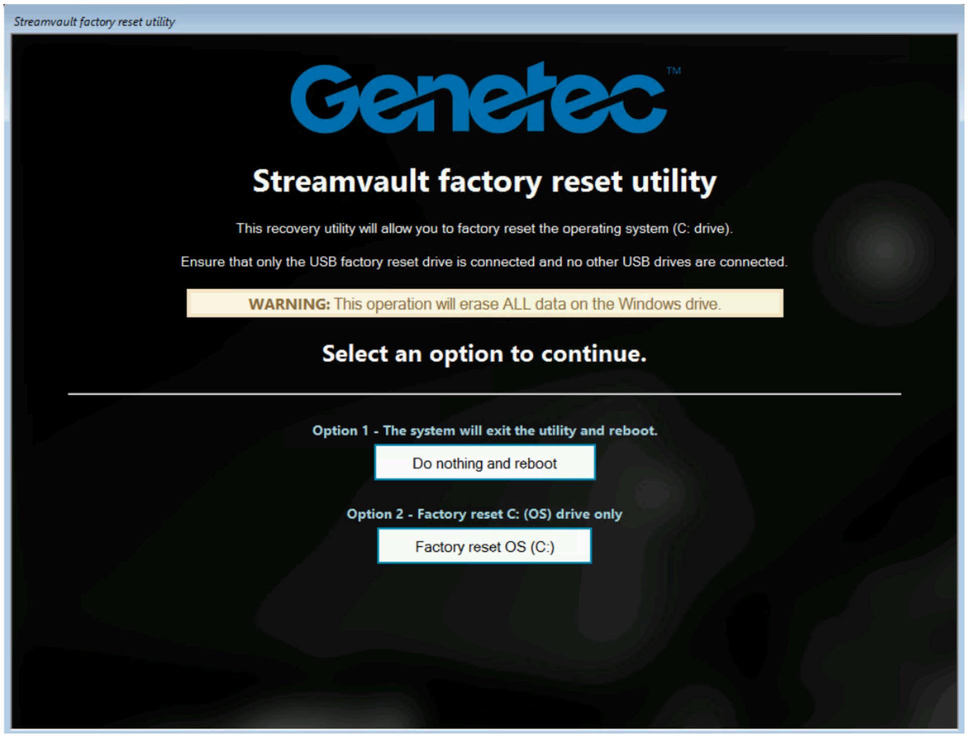
```
Use the ↑(Up) and ↓(Down) arrow keys to move the pointer to the desired boot device.
Press [Enter] to attempt the boot or ESC to Cancel. (* = Password Required)
Warning: Legacy boot mode does not support OS boot on internal storage devices
such as HDD, SSD, NVMe, or eMMC. It is intended for use with external storage devices only,
such as SD Card, USB, and Network PXE.

Boot mode is set to: UEFI; Secure Boot: ON

UEFI BOOT:
    Windows Boot Manager
    Windows Boot Manager
    UEFI: Kanguru FlashBlu 30 PMAP
    Onboard NIC(IPV4)
    Onboard NIC(IPV6)
OTHER OPTIONS:
    BIOS Setup
    BIOS Flash Update
    Diagnostics
    Change Boot Mode Settings

OptiPlex 3060                 BIOS Revision 1.1.4                    Dell
```

4. When the USB boots in recovery mode, select one of the following options:
   - **Do nothing and reboot:** Choose this option to exit the recovery program and restart the appliance.
   - **Factory reset OS (C:):** Choose this option to format and reinstall the appliance system drive and preserve video files on the other video drives. All files on the C: drive will be lost: database logs, and so on.



Streamvault factory reset utility

This recovery utility will allow you to factory reset the operating system (C: drive).

Ensure that only the USB factory reset drive is connected and no other USB drives are connected.

WARNING: This operation will erase ALL data on the Windows drive.

Select an option to continue.

Option 1 - The system will exit the utility and reboot.

Option 2 - Factory reset C: (OS) drive only

5. When prompted, type `Yes` and press Enter to proceed with the factory reset, and wait for the process to complete.
6. When the factory reset is complete, remove the USB key from the appliance, and press Enter to reboot.
7. 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 is no label, you can enter any text to continue.

   The **Start** button appears.
8. Click **Start**.

   One of the following status messages is displayed:
   - **PASS:** The process was validated as successful. Proceed to the next step.
   - **PASS - No Transmission:** The process was validated as successful; however, an internet connection was not available at the time. Proceed to the next step.
   - **FAIL:** The process was validated as unsuccessful. Contact Genetec Technical Assistance.
9. If you receive a PASS or PASS - No transmission message, close the *Genetec™ Product Validator* window.
10. Wait for the background script to close, and then restart the 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 license.
- If you backed up Security Center configuration before the factory reset, restore the configuration using the SV Control Panel.

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 31.
- 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 an SV-100E, SV-300E, or SV-350E appliance on page 70.
- A factory reset deletes all the data currently on the System (OS) drive, but does not affect the factory default RAID drive settings.
- The reset might fail when the hard drives, RAID drives, or partitions on the appliance were changed from the factory default settings. If this is the case, contact Genetec™ Technical Assistance Center (GTAC).

To perform a factory reset on Streamvault workstation or server appliances:

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 software revision number of a Streamvault appliance on page 66

Resetting the software image on a Streamvault workstation or server appliance

You can reset the software image of your Streamvault appliance to its default state using a USB recovery drive.

Before you begin

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

What you should know

- Resetting deletes all the data currently on the System (OS) drive.

- Resetting does not 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. If this is the case, contact the Genetec™ Technical Assistance Center (GTAC).

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

To reset the image on the Streamvault appliance:

1 Shut down the appliance.

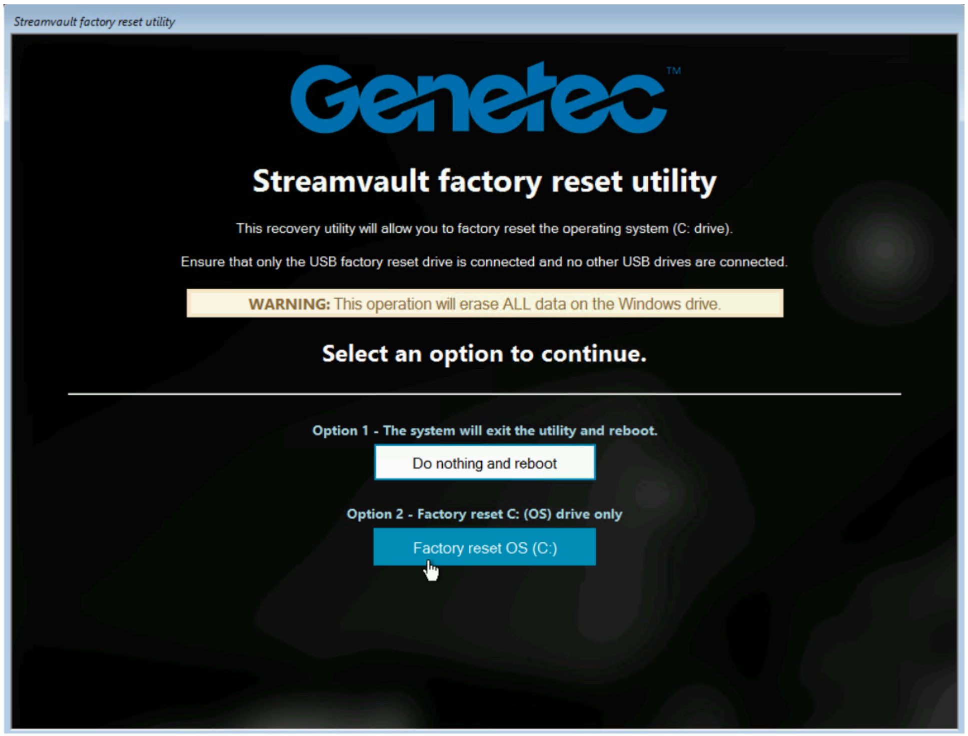
2 Insert the bootable USB key that you created into a USB port.

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:)**.



Streamvault factory reset utility

Streamvault factory reset utility

This recovery utility will allow you to factory reset the operating system (C: drive).

Ensure that only the USB factory reset drive is connected and no other USB drives are connected.

WARNING: This operation will erase ALL data on the Windows drive.

Select an option to continue.

Option 1 - The system will exit the utility and reboot.

Option 2 - Factory reset C: (OS) drive only

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, when prompted to reboot the workstation, press Enter.

9 Remove the USB key from the USB port.

The workstation is now reset to its default state.

After you finish

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

Mercury EP controllers remain offline when TLS 1.1 is disabled

After enrolling a Mercury EP controller in Security Center, the unit does not come online.

You do not receive any errors or warnings about this issue.

Applies to:

- SV-100E 16.3 and later
- SV-300E 16.3 and later
- 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 in Windows Registry Editor.

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.
- Only enable the version of TLS that is required by your device.
- You must enable TLS on the server (incoming) and client (outgoing) nodes.
- For security reasons, the Internet Properties options are disabled on appliances. For this reason, you can only enable TLS from the Windows Registry Editor.

To enable TLS on an appliance:

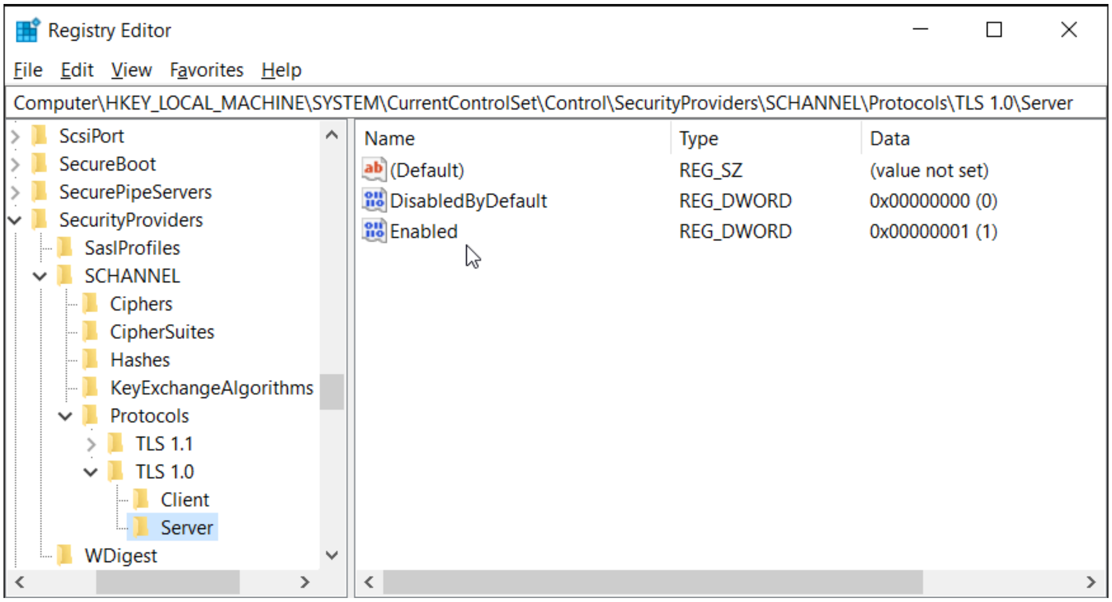
1 Open Windows Registry Editor.

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.



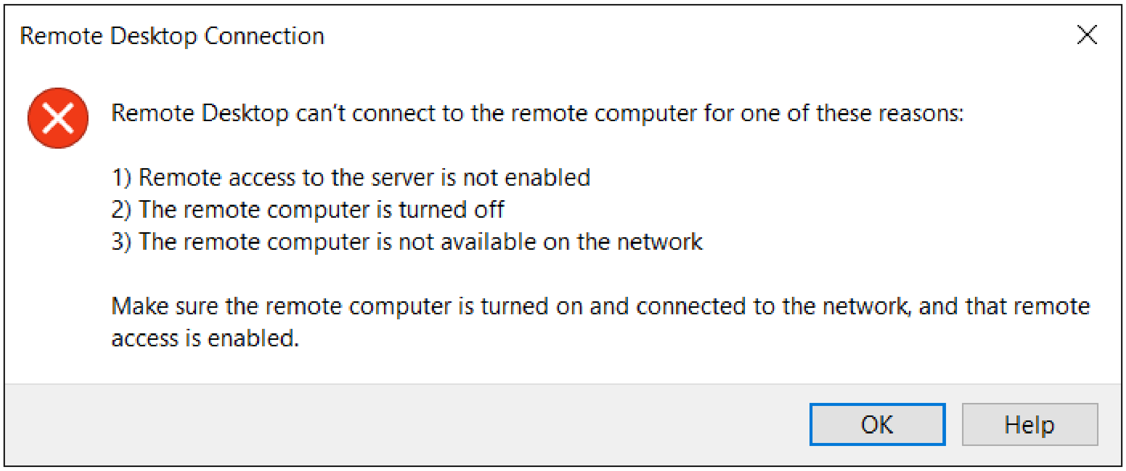
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000000 (0)
Enabled	REG_DWORD	0x00000001 (1)

3 Restart Windows.

Remote Desktop cannot connect to a Streamvault appliance

When you try to access an SV appliance using Remote Desktop, you receive a message that Remote Desktop cannot connect to the remote computer.



Remote Desktop can't connect to the remote computer for one of these reasons:

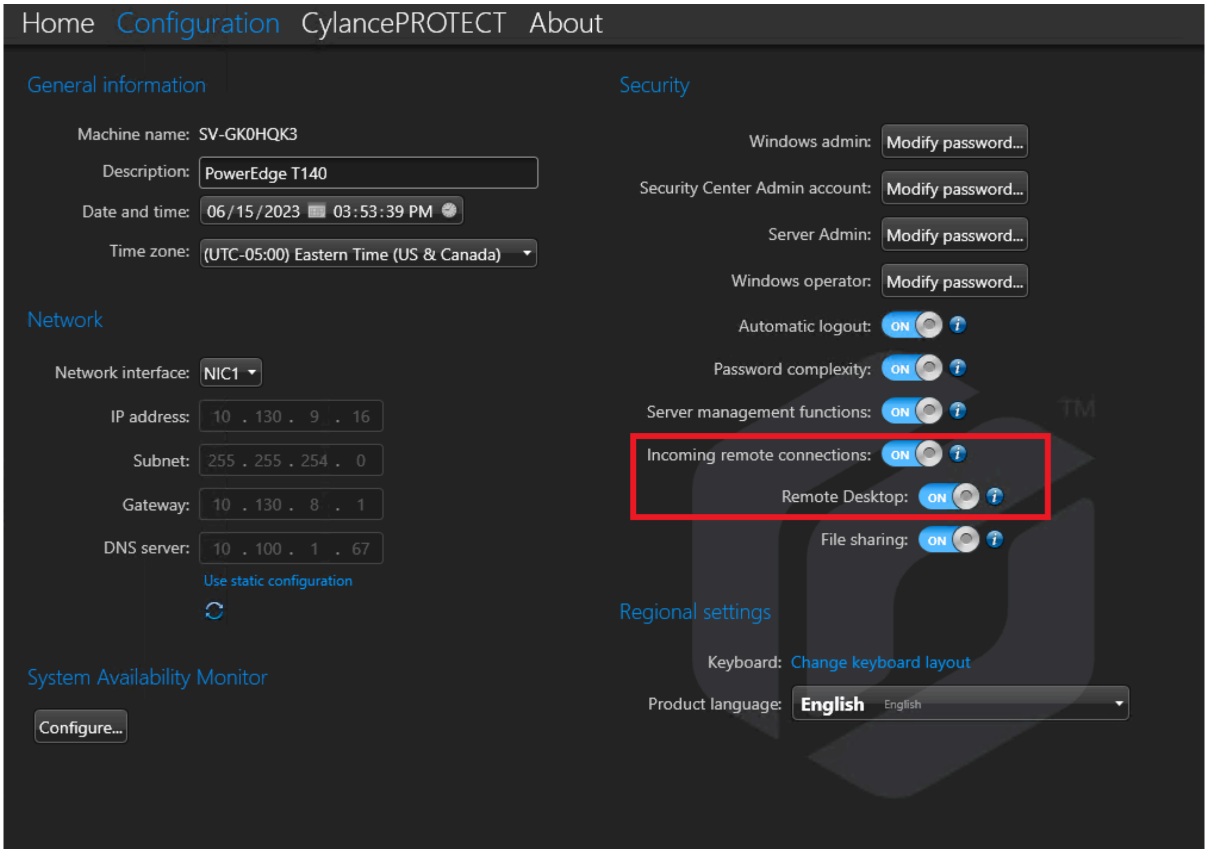
1) Remote access to the server is not enabled
2) The remote computer is turned off
3) The remote computer is not available on the network

Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.

Remote connections and Remote Desktop are disabled in SV Control Panel

Description: By default, remote access is disabled on an appliance to ensure maximum security.

Solution: Enable remote access on the appliance. On the *Configuration* page of SV Control Panel, enable **Incoming remote connections** and **Remote Desktop**.



General information

Machine name: SV-GK0HQK3

Description: PowerEdge T140

Date and time: 06/15/2023 03:53:39 PM

Time zone: (UTC-05:00) Eastern Time (US & Canada)

Network

Network interface: NIC1

IP address: 10 . 130 . 9 . 16

Subnet: 255 . 255 . 254 . 0

Gateway: 10 . 130 . 8 . 1

DNS server: 10 . 100 . 1 . 67

Use static configuration

System Availability Monitor

Configure...

Security

Windows admin: Modify password...

Security Center Admin account: Modify password...

Server Admin: Modify password...

Windows operator: Modify password...

Automatic logout: ON

Password complexity: ON

Server management functions: ON

Incoming remote connections: ON

Remote Desktop: ON

File sharing: ON

Regional settings

Keyboard: Change keyboard layout

Product language: English English

Remote connections or Remote Desktop are not allowed in Windows

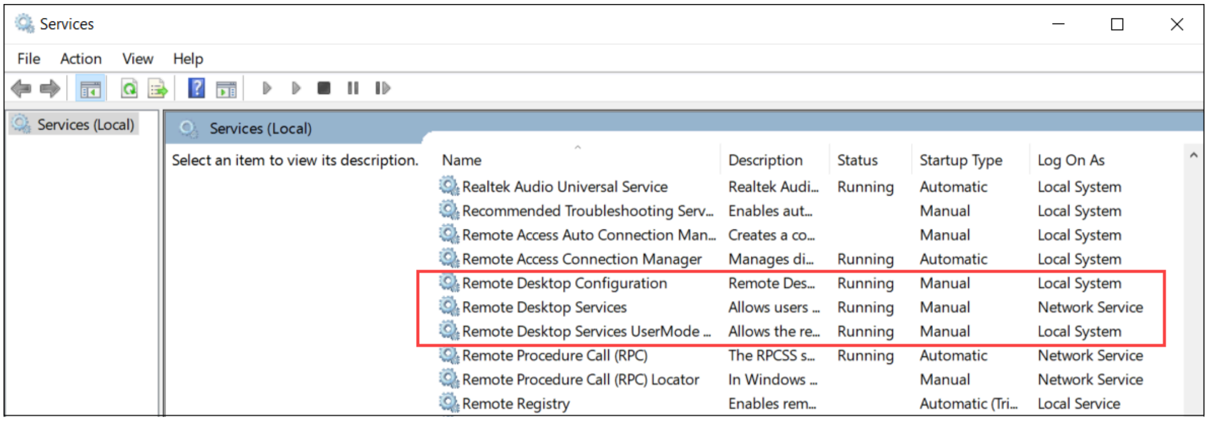
Description: Although both **Incoming remote connections** and **Remote Desktop** are enabled in SV Control Panel, these settings are currently not allowed in Windows.

Solution: Overwrite the Windows settings by disabling and re-enabling the **Incoming remote connections** and **Remote Desktop** options in SV Control Panel.

Remote Desktop Services are not 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.



Select an item to view its description.

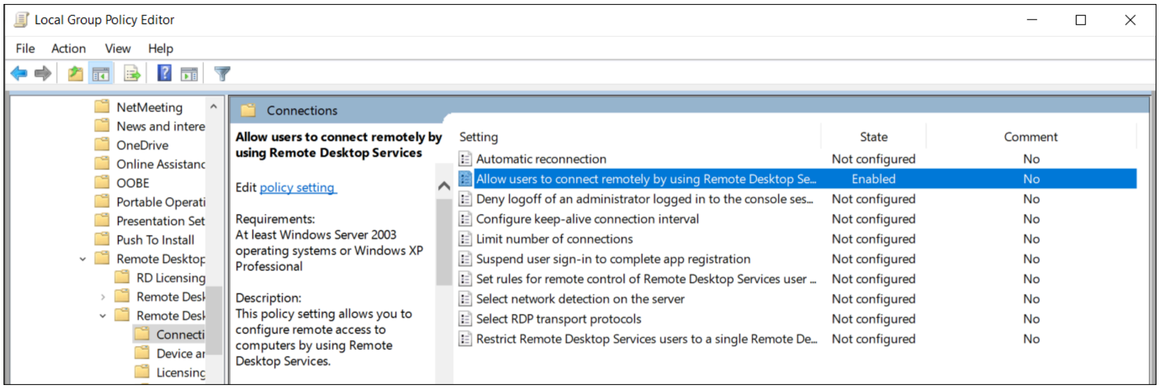
Name	Description	Status	Startup Type	Log On As
Realtek Audio Universal Service	Realtek Audi...	Running	Automatic	Local System
Recommended Troubleshooting Serv...	Enables aut...		Manual	Local System
Remote Access Auto Connection Man...	Creates a co...		Manual	Local System
Remote Access Connection Manager	Manages di...	Running	Automatic	Local System
Remote Desktop Configuration	Remote Des...	Running	Manual	Local System
Remote Desktop Services	Allows users ...	Running	Manual	Network Service
Remote Desktop Services UserMode ...	Allows the re...	Running	Manual	Local System
Remote Procedure Call (RPC)	The RPCSS s...	Running	Automatic	Network Service
Remote Procedure Call (RPC) Locator	In Windows ...		Manual	Network Service
Remote Registry	Enables rem...		Automatic (Tri...	Local Service

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**.



Allow users to connect remotely by using Remote Desktop Services

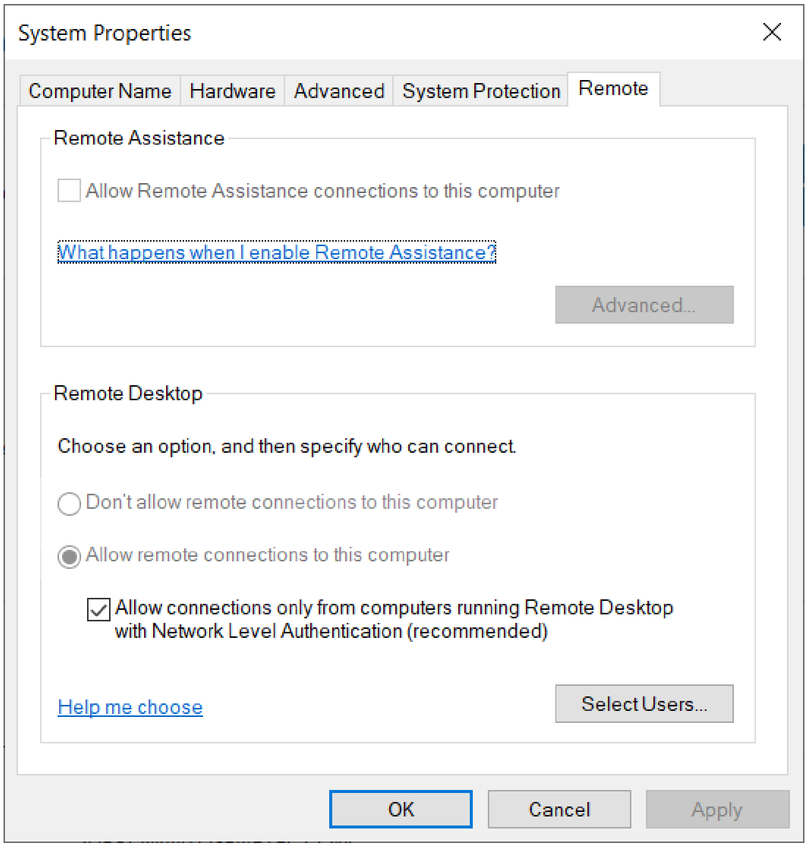
Edit policy setting

Requirements:
At least Windows Server 2003 operating systems or Windows XP Professional

Description:
This policy setting allows you to configure remote access to computers by using Remote Desktop Services.

Setting	State	Comment
Automatic reconnection	Not configured	No
Allow users to connect remotely by using Remote Desktop Se...	Enabled	No
Deny logoff of an administrator logged in to the console ses...	Not configured	No
Configure keep-alive connection interval	Not configured	No
Limit number of connections	Not configured	No
Suspend user sign-in to complete app registration	Not configured	No
Set rules for remote control of Remote Desktop Services user ...	Not configured	No
Select network detection on the server	Not configured	No
Select RDP transport protocols	Not configured	No
Restrict Remote Desktop Services users to a single Remote De...	Not configured	No

4. In Command Prompt, run `gpupdate /force`.
5. From the Windows Control Panel, go to **System** > **Remote settings**. The *System Properties* window opens.
6. On the *Remote* tab, in the *Remote Desktop* section, ensure that **Allow remote connections to this computer** is selected.



Remote Assistance

☐ Allow Remote Assistance connections to this computer

Remote Desktop

Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

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 do not 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 Technical Support.

Related Topics

Allowing Remote Desktop connections to a Streamvault appliance on page 68

Cannot uninstall CylancePROTECT from SV Control Panel for some Streamvault appliances

You turned off the **CylancePROTECT** option from SV Control Panel, but CylancePROTECT does not uninstall from your Streamvault™ appliance.

Affected versions

The following Streamvault image versions are affected by this issue:

- 0011.2.X.27.G (released January 18, 2021) and later
- 16.8.0 (released March 10, 2021) and later
- 2019.1.C.14.G (released January 14, 2021) and later
- 2016.1.C.19.G (released February 8, 2021) and later

Cause

A coding issue.

Workaround

1. Open the Windows *Services* console.
2. Right-click the **Server** service and click **Properties**.
3. Change the **Startup type** option to **Manual**, and then start the service.
4. Open SV Control Panel, click the **CylancePROTECT** tab, and select the **Turn off** option.

   Wait 2 minutes for the process to complete.
5. In the Windows *Services* console, change the **Startup type** of the **Server** service to **Disabled**.
6. Restart the Streamvault appliance.

7

Technical support

This section includes the following topics:

Contacting Genetec support

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 lost administrative access to the system and need a factory image.

- Your diagnostics TSR log file (if applicable).

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

1. Refer to the Genetec Technical Assistance Center *Contact us* page to find the GTAC phone number and business hours in your region.
2. Call the Genetec Technical Assistance Center 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) via live chat and support cases. Operating hours are from Monday to Friday 8 am - 8 pm (local time).

To contact us using 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).

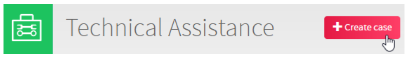
Contacting Genetec support through GTAP

All customers have support available during the business hours of their region through online support cases on the Genetec™ Technical Assistance Portal (GTAP).

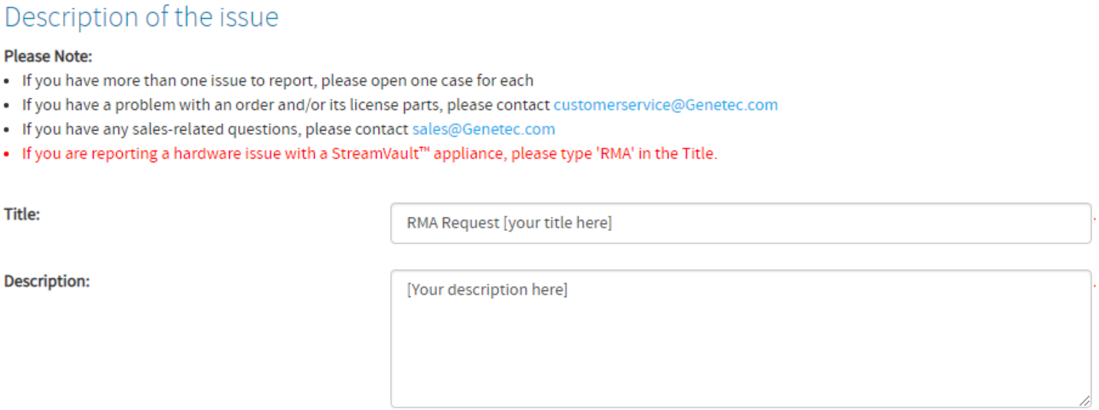
For customers without Advantage coverage, a case needs to be opened through Genetec Technical Assistance Portal (GTAP). For more information on Genetec Advantage, contact advantage@genetec.com.

To 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.



Description of the issue

Please Note:

- If you have more than one issue to report, please open one case for each
- If you have a problem with an order and/or its license parts, please contact customerservice@Genetec.com
- If you have any sales-related questions, please contact sales@Genetec.com
- If you are reporting a hardware issue with a StreamVault™ appliance, please type 'RMA' in the Title.

Title: RMA Request [your title here]

Description: [Your description here]

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

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

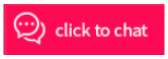
Contacting Genetec support through live chat

Customers with Genetec Advantage coverage have live support is available during the business hours of your region through live chat on the Genetec Technical Assistance Portal (GTAP).

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

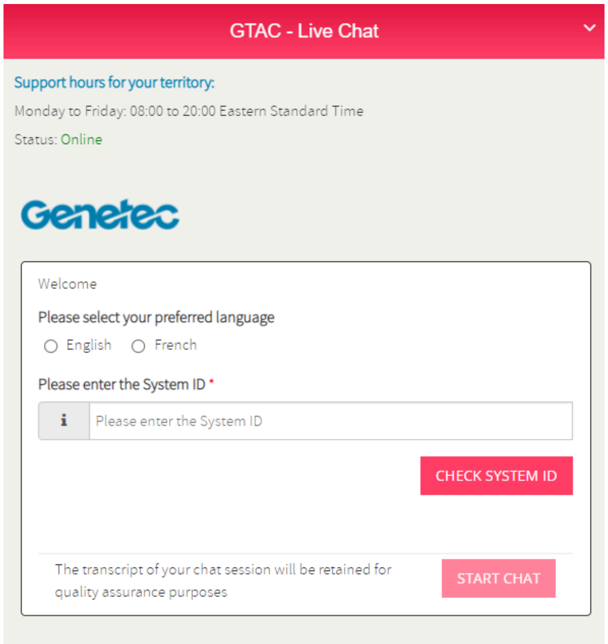
To start a Live Chat:

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 are chatting about a new or existing case.

7. Select the product.
8. Click **Start chat**.



Support hours for your territory:

Monday to Friday: 08:00 to 20:00 Eastern Standard Time

Status: Online

Welcome

Please select your preferred language

○ English ○ French

Please enter the System ID *

Please enter the System ID

The transcript of your chat session will be retained for quality assurance purposes

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 are 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 reimaging 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 Genetec Lifecycle Management (GLM) documents: Genetec Advantage Description and Genetec Assurance 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 DellProSupport.

Product family	Warranty length[1]		Advanced replacement or on-site repair	In warranty return and repair[2]
	Standard	Extended		
SV-100E SV-300E SV-350E	3 years	2 years	1 year of Advanced Replacement	Included
SVW-300 SVW-500 SV-1000	3 years	Not applicable	HP on-site repair warranty[3]	Included
SV-2000E SV-4000E SV-7000E	5 years	2 years	Dell ProSupport next business day[4] on-site repair warranty with keep your hard drive[3]	Included
SVW-300E SVW-500E SV-1000E	5 years	Not applicable	Dell ProSupport next business day[4] on-site repair warranty with keep your hard drive[3]	Included
SV-2000 SV-4000 SV-7000	5 years	2 years	HP on-site repair warranty[3]	Included
Storage Area Network (SAN)	5 years	Extension possible upon request on a case-by-case basis	Dell ProSupport next business day[4] on-site repair warranty with keep your hard drive[3]	Included

[1] You can purchase an additional 2 year warranty extension (for a total of 7 years warranty). It must be purchased before 5 years are up.

[2] You can choose to return the unit for repair or receive on-site services.

[3] For more information about the terms defined by these suppliers please consult Dell ProSupport and HP support documentation.

[4] The next business day on-site repair warranty starts when the troubleshooting is completed, the hardware issue has been identified, the case has been raised with Dell, and Dell has deemed the issue to be a hardware failure. The next business day does not apply as soon as the support case is opened with Genetec Inc.

Specifications for Streamvault™

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

Technical, mechanical, and environmental specifications

All-in-one appliances:

- SV-100E datasheet
- SV-300E datasheet
- SV-350E datasheet

Rackmount appliances:

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

High-availability centralized storage:

- SV-7000EX series datasheet
- SVS-7000E NAS series datasheet
- SVS-7000E SAN series datasheet

Workstations:

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

Analytics-ready appliances:

- SVA-100E series datasheet
- SVA-1000E 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 following terms and conditions relating to repairs, replacements, remedies, or exclusions to the warranty.

Terms and conditions

Warranty on repairs and replacement parts

All Genetec products serviced by Genetec Inc. for repair and replacement parts are warranted against defects in workmanship and materials for 90 days or the remainder of the original warranty, whichever is longer. Additional charges may be applied if damage is a result of using the product in a way that it is not typically intended to be used.

For Streamvault™, all replaced equipment (or portions thereof) shall become the property of Genetec Inc. upon Customer receipt of the corresponding replacement, and the customer shall promptly return such replaced equipment (or portions thereof) upon Genetec Inc.'s request. If such replaced equipment is not returned within 30 days after receiving of the new parts, the customer will be obliged to pay to Genetec Inc. the value of the replacement part. This does not apply to the **Keep Your Hard Drive** service.

Exclusive warranty remedy

During the applicable warranty period and in the event that a product is determined by Genetec Inc. to be defective in materials or assembly, Genetec Inc. will, at its sole discretion, do one of the following:

- Credit the customer the price paid for the defective product.
- Repair the defective product.
- Replace the defective product with a new or refurbished product.
- Replace the defective product with a different product that has identical or better specifications.

Warranty exclusions

The following items are not covered by the Genetec Standard Hardware Warranty:

- Equipment not purchased from Genetec Inc.
- Products used with unsupported ancillary equipment or software.
- Defects or damages from misuse (including, but not limited to, use that is not in accordance with accompanying documentation and manuals), improper modifications, accident, or neglect.
- Defects or damages from drilling holes, adding decals or adhesives, or painting the product.
- Defects or damages due to water damage, lightning, explosions, or other electrical discharges.
- Products that are disassembled or repaired in a manner that adversely affects performance or prevents adequate inspection and testing to verify any warranty claim.
- Modification, abuse, or tampering with the product.
- Acts of God (flash floods, earthquakes, lightning, fire, gas leaks, and so on).
- Normal wear and tear.

Genetec return merchandise authorization terms and conditions

Return merchandise authorization

Before returning an item, the customer must obtain a return merchandise authorization (RMA) form from Genetec Inc. The RMA number must be clearly marked on the outside of each returned package and on the RMA form included with the package. The customer must ensure the return of the exact material, in the correct quantity, and with the exact serial numbers (if applicable) approved by Genetec Inc. and registered in the RMA form provided. Any unapproved, mislabeled, or excess inventory that is shipped to Genetec Inc. will be refused and returned to the shipper.

Packaging

The customer is responsible for adequate packaging of the goods returned. Any damage incurred during transport due to bad packaging will not be covered under the Genetec Hardware Warranty policy. The customer is responsible for any damage during transit. Failure to comply results in Genetec Inc. voiding the RMA and repair fees or the full replacement cost may be billed.

Freight

The customer is responsible for all costs incurred to return the unit. Unless the RMA is voided, Genetec Inc. is responsible for all costs incurred to return the repaired goods or replacement units back to the customer.

If Genetec Inc. mistakenly shipped non-purchased products or products in excess to the customer, Genetec Inc. covers the costs to return the products by providing the customer with shipping labels and export documents, if required. Failing to do so results in an invoice sent to the customer for the goods.

Under some conditions, Genetec Inc. accepts the return of non-damaged items and issues a credit. To be eligible for a return for credit, the item must be unused and in the same condition as when it was received. It must also be in the original packaging. The item must be returned within 30 days of the date when the item was shipped to the customer or within the period allowed by the Genetec Inc. vendor, whichever is shortest.

For all returns for credit, Genetec Inc. issues a credit when the products have been received, inspected, and found in their original condition. The credit is issued for the original selling price minus the applicable restocking fee as per Schedule A. Genetec Inc. reserves the right to refuse any return for credit. Furthermore, Genetec Inc. reserves the right to modify the restocking fee under unusual circumstances, at the sole discretion of Genetec Inc.

Customized items sold under a non-cancellable, non-refundable (NCNR) policy are not eligible for a return for credit.

Damaged in shipment

The products must be inspected upon receipt. Any damage from shipping must be reported to Genetec Inc. within 14 days of receipt of the product. In case of failure to report damages within the 14 days after receipt, Genetec Inc. reserves the right to refuse a return for credit or replacement of the damaged products. For products damaged during shipment, email customerservice@genetec.com immediately. A description of the damages is required, with pictures if possible.

Responsibilities and expectations

- An RMA is valid for 30 days. The items must be returned within this period and be identified with the corresponding RMA number.
- For returns where the customer chooses to bypass the Genetec Technical Assistance Center (GTAC), the customer is obliged to pay an inspection charge if no defect is found with the returned units according to Schedule A.
- The units shipped to the customer as part of the “advanced replacement” warranty is invoiced to the customer immediately and is credited if the damaged unit is returned within 30 days of the RMA creation date.
- The customer is responsible for returning the units in proper condition and according to the instructions provided in this document. Failure by the customer to do so might result in additional fees charged to the customer or Genetec Inc. voiding the RMA Request.
- If an advanced replacement unit is deemed to have been mishandled, abused, or used for purposes other than intended, the customer might be charged the full price of the advanced replacement unit under the “advanced replacement” warranty.
- Out-of-warranty returns and repairs are charged according to Schedule A.

Return instructions

1. Gather the following details before contacting Genetec Inc. for an RMA:
   - Name of the company (integrator) that placed the order.
   - Customer’s order number (purchase order number) for the unit requiring an RMA.
   - Valid contact information (name, email address, phone number) for future correspondence.
   - The part number of the unit requiring repair, replacement, or credit.
   - The serial number of the unit requiring an RMA, if applicable.
   - The system ID, if available.
   - Reason for return.
   - As many details on the hardware issue as possible, if applicable.
2. Contact Genetec Inc. to request an RMA.

Return and repair RMAs

1. Contact the Genetec Technical Assistance Center (GTAC) to advise us of the issue and request an RMA.

   For customers with Genetec Advantage coverage, live support is available during business hours over the phone and through our online chat services on the Genetec Technical Assistance Portal (GTAP). For customers without Advantage coverage, a case needs to be opened through GTAP. When creating the case, include **RMA Request** in the title so our team can easily identify these requests. To find the GTAC phone number and business hours in your region, refer to the Genetec Technical Assistance Center *Contact us* page.
2. Genetec Customer Service provides the customer with an RMA form.

   This form is required to send back the unit. The customer receives the form by email within 24 hours following GTAC contact and processing by Customer Service. This RMA form provides the customer with the complete return address for Genetec Inc. or the vendor, and the RMA number of Genetec Inc. or the vendor.

Return for credit RMAs

1. Contact Genetec Customer Service to advise us of the reason of the return. The request can be submitted by sending an email to customerservice@genetec.com, or by phone. To find the Customer Service phone number and business hours in your region, see the *Contact Us* page on the Genetec Inc. website.
2. Genetec Customer Service provides the customer with an RMA form.

   This form is required to send back the unit. The customer receives the form by email within 24 hours after the contact to Genetec Customer Service. This RMA form provides the customer with the complete return address and the RMA number of Genetec Inc. or the vendor.
3. Customer returns the unit to Genetec Inc. or to the vendor.
   a. The customer is responsible for all shipping charges involved in returning the product to Genetec Inc. or to the applicable vendor.
   b. The customer must print the RMA form (emailed by Genetec Inc. to the customer) and include it with the package, along with the unit, for Genetec Inc. or its vendors to identify the package.
   c. The RMA number must be visible on the exterior of the package. Genetec Inc. provides this number to the customer on the RMA form.
   d. The customer must ship only the products the RMA was requested for. Ship to the complete address that is provided on the RMA form.
   e. Genetec Inc. or the vendor must receive the returned unit within 30 days of issuing the RMA. After this 30-day period, any RMA for “Return for credit” or “Return and repair” services will be voided.
   f. For “advanced replacement” services, Genetec Inc. sends the replacement unit when the RMA is created, or when the part becomes available.

      NOTE: If the damaged unit is returned within 30 days of the RMA creation date, the units shipped to the customer as part of the “advanced replacement” warranty is invoiced to the customer immediately and is credited.
   g. Genetec Inc. requires a tracking number from the customer to be emailed to Customer Service.

4. Genetec Inc. receives and inspects returned items.
   a. The part number and serial number (if applicable) of the returned unit must correspond to the information the customer provided to Genetec Inc. upon creation of the RMA. If there are discrepancies, Genetec Customer Service contacts the customer. The RMA will not be processed until the customer has been contacted, as the warranty may vary based on the serial number and part number.
   b. **Return for credit**: If undamaged, the unit is processed as a “return for credit.” A credit is only applied when the unit has been received and inspected. If the packaging is damaged or modified in any way, Genetec Inc. has the right to refuse the credit. A restocking fee is charged for a “return for credit” according to Schedule A.
   c. **Return for repair**: If under warranty and the damage to the unit is not deemed to be the result of abuse or mishandling by the customer, Genetec Inc. or the vendor proceeds with the repair. The repaired unit is then sent back to the customer. In cases where repair is not possible, the product might be replaced with a fully functional product, either refurbished or new depending on availability. Repair times vary by product line, product type, quantity, and manufacturer. If not under warranty or if the RMA is voided, Genetec Inc. determines if the item is reparable. In such cases, the repair costs are applied according to Schedule A.
   d. Advanced replacement: If the returned unit is covered by an “advanced replacement” clause, and the damage to the unit is not deemed to be a result of abuse or mishandling by the customer, no fee is charged to the customer for the replacement unit provided by Genetec Inc.
5. Genetec Inc. processes the RMA and returns the unit if applicable.

   Genetec Inc. is responsible for all shipping charges and custom clearance (if applicable) to return the unit to the customer.

   The tracking number is communicated to the customer by email when the item is shipped.

Schedule A

Product family	Restocking fees	Repair fees[3]	Inspection fees
Streamvault	Fees are evaluated on a case-by-case basis and are communicated to the customer.	Fees are evaluated on a case-by-case basis and are communicated to the customer.	Not applicable

[3] If the unit is not repairable, the customer is advised to determine if they want to pursue with a replacement of the unit instead.

Glossary

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