Genetec™ Security Center.

Security Center Release Notes 5.8.1.0

Click here for the most recent version of this document.

Document last updated: August 15, 2019

Genetec™

Legal notices

Document information

Document title: Security Center Release Notes 5.8.1.0

Original document number: EN.500.001-V5.8.1.0(1)

Document number: EN.500.001-V5.8.1.0(1)

Document update date: August 15, 2019

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

Contents

1

Release notes

Security Center is a truly unified platform that blends IP video surveillance, access control, license plate recognition, intrusion detection, and communications within one intuitive and modular solution. By taking advantage of a unified approach to security, your organization becomes more efficient, makes better decisions, and responds to situations and threats with greater confidence. Security Center 5.8.1.0 is a minor release that improves reliability and performance.This document describes the release in detail, and provides late-breaking or other information that supplements the Genetec™ Security Center documentation.

This section includes the following topics:

What's new in Security Center 5.8.1.0

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

Platform enhancements

Security Center 5.8.1.0 includes the following platform enhancements:

New version numbering

Security Center releases are now categorized by the following version types:

- Architecture version
- Major version
- Minor version
- Patch version

For more information, visit the Product Lifecycle page on GTAP.

Genetec Mission Control™ compatibility

Genetec Mission Control™ versions 2.12.0.0 and later are compatible with Security Center 5.8.

General enhancements

- **Dashboards: Health monitoring widgets:** The *Dashboards* task has been enhanced with additional health monitoring widgets. Hardware status and Role status widgets are now available to monitor the health of selected devices or roles.

  For more information, see "Standard dashboard widgets" in the *Security Center User Guide*.
- **Dashboards: Health dashboard:** You can now track your system health and identify potential issues in near real time with the *Health dashboard*. The Health dashboard is a system task that presents the following health monitoring dashboard widgets:
  - Archivers
  - Availability
  - Connections
  - Hardware status
  - Health events
  - Role status
  - Security score

  For more information, see "About dashboards" in the *Security Center User Guide*.
- **Enhanced audit trails:** Macro executions are now logged by the system. The execution history is available in the *Audit trails* task.

Genetec™ Update Service enhancements

- **Firmware Vault:** Firmware packages for some video units are now available directly from *Genetec™ Update Service (GUS)*. The firmware recommendations in Config Tool have been enhanced to allow the direct download and installation of recommended firmware.

For more information, see "Upgrading video unit firmware" in the *Security Center Administrator Guide*.

Video enhancements

Security Center 5.8.1.0 includes the following video enhancements:

Hanwha Techwin enhancements

- **Support for SPE-110:** Security Center now supports SPE-110 video encoders. These units can be added with the **SPE series** product type.

March Networks enhancements

- **Support for C0801A PTZ:** C0801A PTZ units can now be added to Security Center. Internal timeouts must be configured in Advanced settings before adding the unit to Security Center using ONVIF.

  For more information, see "Configuring timeouts for March Networks units" in the *Security Center Video Unit Configuration Guide*.

Pelco enhancements

- **Support for GFC Pro Multi:** A new **GFC Pro Multi** product type is available in Config Tool for GFC Pro multi-sensor units. A multi-sensor unit only requires one camera license.

About the documentation in Security Center 5.8.1.0

The documentation provided with a product is subject to change. With each product release, new documents might be added, current ones updated, and older ones replaced. For the latest version of the documentation, see the Genetec™ TechDoc Hub.

Documentation updates

The search feature is now available in the French Help files accessed from Security Desk and Config Tool.

IMPORTANT: Translation of documentation is ongoing and documentation in languages other than English might not be complete at the time of release.

Document title	Status	Languages
Getting Started with Security Desk • Glossary cleanup	Updated	• English • French • German • Italian • Korean • Portuguese • Spanish

Document title	Status	Languages
Security Center Administrator Guide • Firmware Vault: Upgrading video unit firmware • Genetec™ Mobile 5.1: Configuring Mobile Server roles • Media Gateway: About, Creating, and Configuring the Media Gateway role	Updated	• English • French • German • Spanish
Security Center Installation and Upgrade Guide • New four-digit versioning scheme • Ports in Security Center	Updated	• English • French • German • Spanish
Security Center Release Notes • See What's new in Security Center 5.8.1.0	Updated	• English • French • German • Spanish
Security Center SDK Release Notes	Updated	• English
Security Center System Requirements	Updated	• English • French • German • Spanish
Security Center Video Unit Configuration Guide • See Video enhancements	Updated	• English
Security Center User Guide • Health dashboard • New health monitoring widgets **NOTE:** This guide was formerly titled *Security Desk User Guide*.	Updated	• English • French • German • Spanish

Supported languages in Security Center 5.8.1.0

The supported languages are the languages in which the software is available.

Security Center 5.8.1.0 software is available in the following languages:

- Arabic
- Chinese (Simplified and Traditional)
- Czech
- Dutch
- English
- French

- German
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Persian
- Polish
- Portuguese–Brazil
- Russian
- Slovenian
- Spanish
- Swedish
- Thai
- Turkish
- Vietnamese

Resolved issues in Security Center 5.8.1.0

Resolved issues are software issues from previous releases that have been fixed in the current release.

The following software issues were resolved in Security Center 5.8.1.0:

Solution/Unit	Issue	Description
Access	2244125	Non-admin users that are granted all privileges cannot modify the security clearance property of a cardholder or cardholder group.
Access	2232683	After both the Directory and Access Manager roles restart, a cardholder's last known location is not reflected in the *People counting* task if the cardholder's last access request was on a captive door.
Access	2231643	In the *Monitoring* task, when a door is in a tile, and the tile is selected, right-clicking **Door** > **Unlock** for a different door from the area view unlocks the door in the selected tile.
Access	2223980	After an Access Manager failover, I/O zones cannot be armed or disarmed.
Access	2195418	You cannot create license plate credentials for cardholders from Active Directory.
Adcor Magnet	2159313	Ubik 360: Adding the unit and changing the video resolution from the maximum resolution to a lower resolution triggers the unit to reboot cyclically.
All	2247377	In Security Desk, when video sequences from PTZ cameras are paused, the *PTZ* widget is missing.
All	2229720	Security Desk freezes when a high number of alarms is received in the *Alarm monitoring* task.

Solution/Unit	Issue	Description
All	2212398	When federated cameras are in maintenance mode on the remote site, maintenance mode is not reflected on the Federation™ host.
All	2209979	Users who lack the *Modify user properties* privilege for a partition can still grant other users access to that partition.
All	2195211	On large systems, health issues might not load in the *System messages* window or in *Health history* reports that are filtered on **Show current health events**.
All	2189084	When dragging and dropping from a *Maps* task on screen A to a tile in a *Monitoring* task on screen B, the monitor focus stays on screen A.
All	2155312	Dashboards: In the *Archivers* widget, no statistics are listed when you click the **Statistics** icon in the **Total number of cameras** column for the Auxiliary Archiver role.
All	2118452	The *Packet loss normal* health event for Security Desk is not always triggered after a *Packet loss high* event is triggered.
All	2250684	When the Access Manager or LPR Manager roles are deactivated, the Health Monitor role does not generate the *Connection to unit stopped by user* event.
All	2227161	There is no activity trail for when macros are started or stopped.
All	2200510	Dashboards: In *Health* widgets, changes to the width and position of table columns are not persisted to Security Desk clients of different languages.
Avigilon	2145310	For some units, RTSP over HTTP streaming does not work.
Axis	2244513	On the **Video** page of Axis units, when **Constant bit rate** is enabled for the MPEG-4 stream, the **Bit rate** slider is not displayed.
Axis	2201025	When motion is detected from cameras with Axis Video Motion Detection (VMD), corresponding motion events are not triggered in Security Center.
Bosch	2238242	Bosch VIP-X16XF-E and VJM-4016 units using firmware 5.80 and later: On the *Video* page of the unit, the **Resolution** setting is missing.
Bosch	2142479	Video tracks from Bosch VRM cannot be played in the Security Desk*Archive storage details* task. The message *No recorded video at this time* is displayed.
Documentation	930259	Config Tool and Security Desk: Help file Search feature is not available in French.
Hanwha	2155760	Audio input does not work on PNM-9030V because of an external issue in FW 1.02_190129.
Interlogix	2219694	SymNet units: Playback video might be pixelated or skip frames.
Intrusion	2158868	You cannot arm an intrusion detection area from a tile widget on a dashboard.
LPR	2234092	When the SharpV is connected to the LPR Manager using the LPM protocol, the SharpOS version displayed in Config Tool might not be correct.

Solution/Unit	Issue	Description
LPR	594453	After performing an update using the *Updates* page in the Config Tool*LPR* task, the status of an update may sometimes change from *Installed* to *Waiting for status*.
LPR	2237492	The Sharp Updater Service is not completely disabled and might cause the Sharp version to be overridden by an older version.
Mercury	2202787	Mercury EP and LP units: Cardholder information is unavailable for offline access reads.
Synergis™ IX	2165159	Devices with names containing over 100 characters are not handled correctly in Security Center.
Verint	2238735	Verint S1500 series: After upgrading to Security Center 5.7 SR6 or later, units remain offline, even if they are rebooted or reconnected.
Video	2243371	The Media Router algorithm for the connection wait list of federated remote site does not work properly, leading to unreachable federated cameras and unrecoverable sites.
Video	2241873	Serial PTZ stops working after the Archiver role restarts.
Video	2236716	After exporting video with a 48 kHz sample rate to MP4, there are intermittent drops in the audio output.
Video	2235526	The MediaGateway cache cleaning algorithm does not delete files over the configured cache size limit for camera in playback, leading to low disk space on the server.
Video	2221522	The Media Gateway role increasingly takes up server resources until it crashes.
Video	2207507	When an exported G64 file contains hidden frames, watermark validation fails.
Video	2196892	Archive transfers configured to retrieve from edge on some cameras remain ongoing and never complete because of an incorrect edge transfer retry mechanism.
Video	2189027	When you generate a report from the *Archiver statistics* task, cameras might be missing in the results.
Video	2180594	Some video walls communicating with the Media Gateway role over RTSP disconnect every minute.
Video	2179988	Event-to-actions using *Go to preset* successfully move cameras with **PTZ** disabled.
Video	2177542	If the Video Unit Control process stops unexpectedly, it automatically restarts, but the Archiver role can no longer record.
Video	2171231	Archive transfers fail when creating a file with a single frame, preventing the transfer from proceeding.
Video	2152154	The cleanup of expired files from the Auxiliary Archiver database might fail because too many files must be deleted at the same time from the database.

Solution/Unit	Issue	Description
Video	2222249	On rare occasions, when using cameras configured for H.264, Archiver roles configured with software motion detection might crash.
Video	2243241	ONVIF cameras: After the Archiver role goes offline and then comes back online, the configured resolution of H.264 streams might change automatically.

What's new in Security Center 5.8 GA

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

Platform enhancements

Security Center 5.8 GA includes the following platform enhancements:

Genetec Mission Control™ compatibility notice

Genetec Mission Control™ is currently not compatible with Security Center 5.8. Genetec Mission Control™ users should continue using Security Center 5.7.

General enhancements

- **Dashboards:** Dashboards are now available in Security Desk. A dashboard is a customizable task that tracks the key indicators and other information that you need to achieve a comprehensive view of what matters to you. To build a view tailored to your day-to-day, you can pin Security Center tiles, reports, and charts to a blank canvas.

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages. If using Internet Explorer, the video might not display. To fix this, open the **Compatibility View Settings** and clear **Display intranet sites in Compatibility View**.

For more information, see "About dashboards" in the *Security Center User Guide*.

- **Privilege troubleshooter:** A new Privilege troubleshooter is available in Config Tool. Strengthen your security protocols with increased visibility into your users' privileges. The Privilege Troubleshooter lets you audit user rights on each entity in just a few clicks, so you can ensure only the right individuals can access, operate, or modify its settings.

With this tool, you can discover:

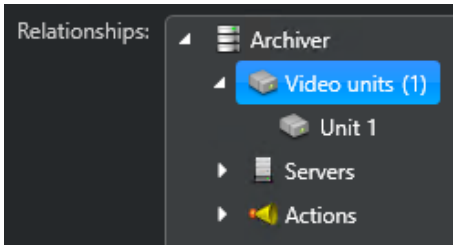
- Who has permission to work with a selected entity
- What privileges are granted to selected users or groups
- Who has been granted a privilege, has access to a specific entity, or both

For more information, see "About the Privilege troubleshooter" in the *Security Center Administrator Guide*.

- **Separate privileges for modifying and deleting incident reports:** From now on, users with the *Modify reported incidents* privilege can no longer delete incidents. To delete incidents, the user must have the *Delete reported incidents* privilege.

  NOTE: If you are upgrading from a previous version, the new privilege *Delete reported incidents* is not automatically granted to users who had the *Modify reported incidents* privilege.
- **Privilege required for Spy mode:** Users now require the *Spy mode* privilege to connect to remote Security Desk workstations in Spy mode.

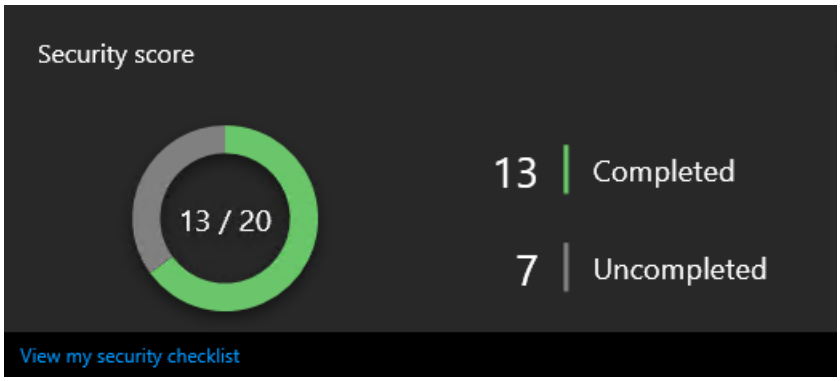
  For more information, see "Connecting to remote Security Desk applications" in the *Security Center User Guide*.
- **Enhanced audit trails:** Additional configuration and property changes are now logged by the system. The *Audit trails* task now logs the following:
  - Configuration changes to role databases
  - Property changes to the Intrusion Manager role and to video-related roles
- **New task commands:** You can now open a task in the background by pressing Ctrl and clicking the task, or duplicate an opened task by right-clicking the task from the taskbar, and then clicking **Duplicate task** in the contextual menu.
- **Entity count in the Relationships tree:** On the *Identity* page of an entity, the number of each associated entity is now displayed in the *Relationships* tree when you expand the entity.



- **Role state displayed in area view:** Deactivated roles are now displayed in grey instead of red in the area view.

Security enhancements

- **Security Score widget:** You can now track your system security and identify potential vulnerabilities in near real time with the Security Score dashboard widget. The Security Score measures compliance to Security Center hardening best practices, such as password strength, use of certificates and encryption, and more.



The Security Score widget is available with Security Desk dashboards. For more information, see "About dashboards" in the *Security Center User Guide*.

- **Database security:** The communication between roles and their database servers is now secured by default. Two options are available:
  - **Encrypt connections:** (Default) Uses Transport Layer Security (TLS) protocol for all transactions between the role and the database server. This option prevents eavesdropping and requires no setup on your part.
  - **Validate certificate:** Authenticates the database server before opening a connection. This is the most secure communication method and prevents *man-in-the-middle* attacks. The *Encrypt connections* option must first be enabled.
    NOTE: You must deploy a *valid* identity certificate on the database server. A valid certificate is one that is signed by a certificate authority (CA) that is trusted by all servers hosting the role and that is not expired.
- **Encryption of video in transit by default:** You now have the option to encrypt your video only when it is streamed from the Archiver. The video archive is not encrypted. This option does not require any certificate to be installed, and is the default setting for all Archiver roles created in 5.8 GA and later. All users who have the right to access the camera can view the encrypted video.

  Limitation: Multicast from the unit is not supported. This option is incompatible with Security Center 5.7 and earlier.

  For more information, see "Configuring default camera settings" in the *Security Center Administrator Guide*.

Federation™ enhancements

IMPORTANT: The following enhancements are supported only if both the Federation™ host and the remote systems are running Security Center 5.8 GA or later.

- **Remote configuration task:** You can now configure federated Security Center entities from the Config Tool connected to the Federation™ host, using the *Remote configuration* task.

  NOTE: Multi-level federations are not supported in this release.

  For more information, see "Configuring federated entities" in the *Security Center Administrator Guide*.

  When federated entities are modified from the Federation™ host, users at the federated site can see who made the changes by running the *Audit trails* report. This ensures the total transparency of the configuration process and improves your system security.
- **Monitoring enterprise data from a central system:** Previously, you could only view federated camera settings through the *Camera configuration* report. Now, provided that the Federation™ users have all required privileges, you can view all federated unit settings through the *Hardware inventory* report.

  For more information, see "Viewing unit properties" in the *Security Center Administrator Guide*.

  Limitation: The *Password* and the *Proposed firmware version* report columns are not available for federated units, nor are the action commands, such as **Reboot** ( ) and **Upgrade firmware** ( ). To see those settings and use those commands, you must run the *Hardware inventory* task from within the *Remote configuration* task.
- **Monitoring enterprise activities from a central system:** The **Forward Directory reports** option has been added to the Security Center Federation™ role. When this option is turned on (default=OFF), user activities (viewing cameras, activating the PTZ, and so on) and configuration changes performed at the remote site can be viewed from the Federation™ host through the *Activity trails* and *Audit trails* reports, as long as the Federation™ user has the privileges and access rights to view them.
- **Yellow arrow removed from federated entities:** In Security Desk, federated entities no longer have a yellow arrow superimposed on their entity icons by default. For example, a federated alarm in Config Tool is indicated by a yellow arrow ( ), but the same entity in Security Desk does not have the arrow ( ).

  To display the arrows on federated entity icons in Security Desk, you must modify the *App.SecurityDesk.config* file found in *C:\Program Files (x86)\Genetec Security Center*

*5.8**ConfigurationFiles*. In the *Presentation* section, change the value of DisplayFederationArrow to "true" (*DisplayFederationArrow="true"*).

Map enhancements

- **End of support for legacy Plan Manager 10.x plugin:** Starting with Security Center 5.8 GA, the legacy Plan Manager 10.x plugin is no longer tested nor supported. Only the native Plan Manager is supported in Security Center 5.8.

  If you want to use the legacy Plan Manager 10.x plugin with Security Center 5.8, your Security Center license must include the GSC-PM-Legacy part.

- **Configurable zoom level on custom Tile Map Service maps:** You can now specify a maximum zoom level between 1 - 25 (default = 17) for custom Tile Map Service (TMS) map providers.

  For more information, see "Connecting Map Manager to a TMS map provider" in the *Security Center Administrator Guide*.

- **AutoCAD format support:** You can now create maps from DXF and DWG image files. CAD layers are imported as flat images.

- **Web Map Service protocol support:** You can now use Web Map Service (WMS) servers as online map providers. When connecting the Map Manager to a WMS server, you can enable or disable layers to control what is shown on the map.

  Map Manager supports the WMS protocol version 1.3.0 and 1.1.1.

  For more information, see "Connecting Map Manager to a WMS map provider" in the *Security Center Administrator Guide*.

- **Configurable FOV colors:** You can now specify the color of camera FOV indicators from the *Field of view* widget in the *Map designer* task.

- **Customizing door state display :** You can now set different icons for *Door open* and *Door closed* events from the *Identity* widget in the *Map designer* task.

- **Show mobile users on maps :** With the new Mobile Server role and the new Genetec™ Mobile app, you can now show the location of mobile users on georeferenced maps in Security Desk. Mobile users are displayed as bubbles. Clicking on a user shows basic information such as the Security Center username, photo, location, and last update time. From the map, you can send messages to mobile users and share entities.

  For more information, see "Showing mobile users on maps" in the *Security Center Administrator Guide*.

  Limitation:

  - The street address of the mobile user is only available if the Map Manager role has a valid Google license key.
  - Some shareable entities cannot be displayed in Genetec™ Mobile.

- **Customizing map behavior in Security Desk:** You can now customize the following map behaviors from the *Options* dialog box in Security Desk:

  - Panel position of alarms, events, and map layers
  - Map item behavior on single-click, double-click, and lasso
  - Display of alarms from linked maps

  For more information, see "Customizing map behavior in Security Desk" in the *Security Center User Guide*.

- **Displaying alarms on linked maps:** You can now see the number of active alarms on linked maps on the *Maps* task toolbar, floor controls, and map links, by enabling the **Display alarms from linked maps** option in Security Desk.

- **Dynamic Keyhole Markup Language (KML) support:** Dynamic KML objects are now supported on maps in Security Center. These objects represent fluid information, such as weather conditions and traffic flow, that is refreshed automatically at the interval specified in the KML.

- **Floor management:** You can now designate two or more maps as floors of the same building. Each floor is automatically linked to all other connected floors. You can quickly navigate between floor maps from the floor controls, by pressing the button for the floor you want to see.

  Floor controls

  If an area is included in multiple buildings, like a shared parking lot, then the floor controls can be used to navigate between buildings.

  For more information, see "Configuring maps as floors of a building" in the *Security Center Administrator Guide*.

- **Lock map display:** You can now lock maps to their default home position from the *Map designer* task in Config Tool. Locking a map prevents users from changing the map position by panning, zooming or using presets.
- **New privilege for Switch to map mode:** The ability to switch between tile mode and map mode is now controlled by the *Switch to map mode* privilege.

  Map mode is a Security Desk canvas operating mode that replaces tiles and controls with a geographical map showing all active, georeferenced events in your system. Switching to Map mode is a feature of AutoVu™ and Genetec Mission Control™, and requires a license for one of these products.

New Mobile Server and Genetec™ Mobile app

Security Center 5.8 GA offers an entirely new mobile experience that is more secure, more versatile, and fully integrated into the Security Center platform.

For more information, see "About Genetec™ Mobile" in the *Security Center Administrator Guide*.

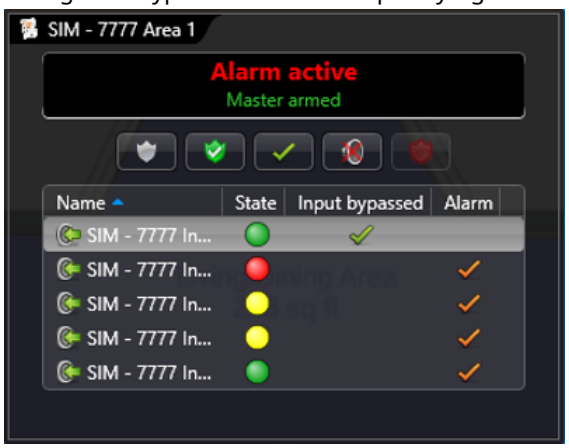
- **New Mobile Server role:** Mobile Server now runs as a role. It is automatically created after installation if your license supports *Mobile*. The Mobile Server role supports secure communications and can be expanded with new features without upgrading your system.
- **End of support for legacy Mobile Server 4.x:** The legacy Mobile Server 4.x is installed as a separate application. Legacy Mobile Server 4.x is no longer supported with Security Center 5.8 GA, but it is still supported with older versions of Security Center.
- **Enhanced collaboration between your HQ personnel and your agents in the field:** You can now show the location of your Genetec™ Mobile users on georeferenced maps in Security Desk. Your operators can also exchange text messages and send and receive video from Genetec™ Mobile users in the field.
- **New Genetec™ Mobile app:** The new Genetec™ Mobile app has a map-based interface with one-tap access to any of your security devices, such as cameras, doors. The Genetec™ Mobile app replaces the following mobile apps:
  - Genetec™ Security Center
  - Security Center Legacy
  - Genetec™ Threat Level

  For more information, visit our website.

Intrusion detection enhancements

- **Honeywell intrusion panel extension:** A new Honeywell intrusion panel extension is available as of Security Center 5.7 SR2. By Security Center 5.9, the legacy Honeywell Galaxy Dimension control panel integration will reach end-of-life and no longer be supported. Customers using this integration should migrate to the new Honeywell intrusion panel extension before upgrading to Security Center 5.9.

- **Changing bypass states of inputs:** When inputs associated to an intrusion detection area are bypassed or in an alarm state, you can now view them from a widget on a map or in a monitoring tile. You can change the bypass state of the input by right-clicking the input from the list.



- **New input type definitions:** You can now specify the intrusion input type from the *Peripherals* page of the intrusion detection unit. The types of inputs are listed on the *Input definitions* page of the Intrusion Manager role.

  For more information, see "Intrusion Manager configuration tabs" in the *Security Center Administrator Guide*.

- **New report pane column in the Intrusion detection area activities task:** In the *Intrusion detection area activities* report, you can now display the picture of the cardholder that triggered an event, and filter the results by input type.

Health monitoring enhancements

- **New health monitoring events:** The following health events are now available in the *Health history* report:
  - Unit time in sync with time server
  - Unit time out of sync with time server
  - Transmission lost
  - Transmission recovered

  You can configure whether or not to monitor them on the *Properties* page of the Health Monitor role.

- **Health event monitoring:** You can now trigger actions with health events, using event-to-actions.

Genetec™ Update Service enhancements

- **Updated notifications:** Genetec™ Update Service notifications in the Config Tool notification tray are now more detailed, and you can view the update details and configure Genetec™ Update Service from the *System* task by clicking **General settings** > **Updates**.

Video enhancements

Security Center 5.8 GA includes the following video enhancements:

General enhancements

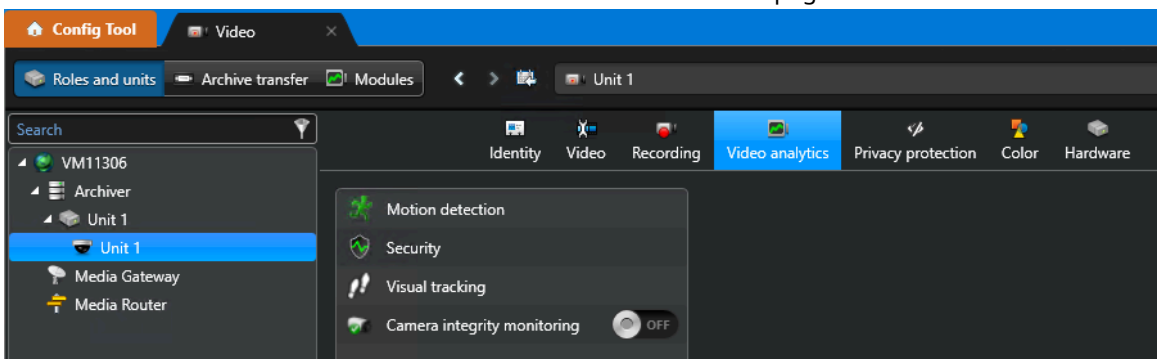
- **Archiver statistics report:** You can now monitor the operation statistics of all your Archiver and Auxiliary Archiver roles in a single report, using the Archiver statistics task.

  For more information, see "Viewing Archiver statistics" in the *Security Center Administrator Guide*.

- **Support for Wearable camera evidence report:** In Security Desk and Config Tool, you can now run the Wearable camera evidence report.
- **Illustra driver enabled:** The Illustra driver is now available in the list of drivers after a new installation.
- **Support for G.721 audio in 64-bit Security Desk:** The 64-bit version of Security Desk can now send audio streams from the Client to cameras that receive audio in G.721, using the **Talk** button in the *Camera* widget.

User interface enhancements

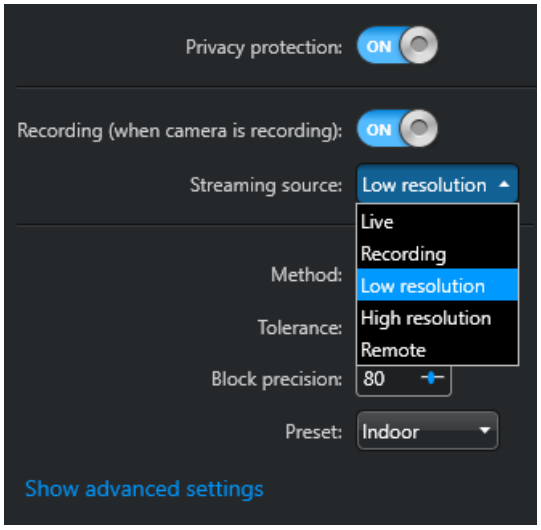
- **Video task enhancements:** The *Video task* is now divided into three pages:



  - **Roles and units:** This page displays all video-related entities in an area view. Video analytics features, such as motion detection, visual tracking, and so on, are now grouped into the *Video analytics* page of a camera.
  - **Archive transfer:** *Archive transfer* is no longer a task; it is now a page in the *Video* task.
  - **Modules:** You can enable and disable the Privacy Protector™ and Camera Integrity Monitor modules on the *Modules* page.

Privacy Protector™ enhancements

- **Stream selection:** You can now select a **Streaming source** for the privacy-protected stream.



Using this approach, you have more flexibility regarding which stream you want to apply the privacy protection to. Although the Archiver role always archives the *Recording* stream as the original (private) stream, you can select a different stream to archive as the anonymized (public) stream.

For more information, see "Configuring privacy protection" in the *Security Center Administrator Guide*.

- **Privacy protection recording schedule:** In the **Privacy protection** tab, when the privacy protection **Recording** option **ON** is specified, the privacy protected stream is now archived following the recording schedule of the original stream.

  For more information, see "Configuring privacy protection" in the *Security Center Administrator Guide*.

Video analytics enhancements

- **Camera tampering detection:** The new KiwiVision™ Camera Integrity Monitor module ensures that your cameras are operational and effective through periodic validations, and notifies your operators when a camera has been tampered with. This is especially useful for large systems with hundreds or thousands of cameras that make it impractical to manually check the image and field of view of each camera.

  The following types of camera tampering can be detected:

  - Obstruction of camera view (partial or complete)
  - Blurred image (due to change of camera focus or smeared lens)
  - Abrupt change in the position of the camera (due to environmental or human causes)

  For more information, see "About camera integrity monitoring" in the *Security Center Administrator Guide*.

Video export and Genetec™ Video Player enhancements

The video export and playback process is made more secure with the following enhancements.

- **No more intermediary decrypted files during playback:** You can now view an encrypted video file directly in Security Desk or Genetec™ Video Player without having to save a decrypted copy of the file on disk.

  NOTE: Starting with Security Center 5.8 GA, the GEK files are no longer used to store encrypted video. Both encrypted and non-encrypted videos are now saved in G64x files. Newer Security Center applications (5.8 GA and later) can read the old GEK files created in version 5.7 and earlier, but the older applications cannot read the new password-protected G64x files created in 5.8 GA and later.
- **Password protection during export:** You can now protect a video file when you export. If you configured a default encryption key for exporting video files in Security Desk, you can override this setting before each video export, either by using a different password or by removing the password.
- **Preventing exported video from being re-exported:** When you re-export an exported video file using the **Save as** command, you can save it in a different format (which removes the encryption) and change the time range. To preserve the originally exported video, the new **Allow the exported video file to be re-exported** option (default=No), has been added to the video export settings. You can only re-export the exported video file if you explicitly select this option. This feature is also exposed by the SDK.

For more information, see "Exporting video" and "Viewing exported video files" in the *Security Center User Guide*.

Enhanced system operability during failover

The following enhancements ensure that Directory and Archiver failover have minimal impacts on your operations:

- **Fast PTZ recovery during Directory failover:** It now takes less than 30 seconds to regain control of your PTZ cameras after a Directory failover.
- **Offline PTZ mode:** Using the offline PTZ mode, you can now retain control over your PTZ cameras when Security Desk loses its connection to the Directory (for example, during a Directory failover). To enable this feature, you must modify the *App.SecurityDesk.config* file.

  For more information, see "Enabling offline PTZ mode" in the *Security Center User Guide*.

Reporting enhancements

- **New report pane column in the Camera configuration task:** You can now filter the results of your *Camera configuration* report with the **Camera retention** column.

Axis enhancements

- **Support for large RTP packets in Axis cameras:** On the *Network settings* page in Config Tool, you can now enable **Large RTP packets** and increase the maximum size sent by an Axis camera.
- **Upgrade SDK:** Upgrade to new Axis dewarping SDK version 4. The upgrade enables the use of the P3807-PVE unit that blends four sensors into one image for a cohesive video stream.

Bosch enhancements

- **Ability to change username when connecting to Bosch cameras:** You can now modify a username by adding a new user to the list of users in the camera's web page.

Access control enhancements

Security Center 5.8 GA includes the following access control enhancements:

General enhancements

- **Unlock the perimeter doors of an area through a hot action:** You can now configure a hot action to unlock an area's perimeter doors with a keyboard shortcut. You can also select the action from the notification tray in Security Desk.

  For more information, see "Configuring and using a hot action to unlock multiple area perimeter doors" in the *Security Center User Guide*.
- **Door templates:** Security Center now has wiring templates for most popular door configurations, which reduce the time it takes to configure multiple similar doors. You can select a template during the door creation process.

  For more information, see "Creating doors" in the *Security Center Administrator Guide*.
- **Improved custom input support for Mercury EP controllers:** You can configure Mercury EP controllers with up to four sets of custom A/D values for supervised inputs.
- **Mercury LP series controller support:** Security Center 5.8 GA introduces support for the Mercury LP series of intelligent controllers. The LP series consists of the following controllers:
  - Mercury LP1501
  - Mercury LP1502
  - Mercury LP2500
  - Mercury LP4502
- **Secure communications for HID units:** HID EVO units can now communicate over TLS 1.2. This enhances the security of the channel between the Access Manager role and HID units running in Secure mode.

Synergis™ IX for ANZ market

- **Unification of access control and intrusion detection in Security Center:** Synergis™ IX brings an innovative approach to both access control and intrusion monitoring. With a broad range of supported hardware at your disposal, the Synergis™ IX system lets you control and monitor a scalable number of intrusion areas, doors, cardholders, and other field devices, in real time, regardless of geographical location.

Cardholder and credential enhancements

- **Native MIFARE DESFire configuration:** You can now create configurations for MIFARE DESFire key cards in Config Tool, which eliminates the need for a third-party card production tool. You can then use these configurations to encode new cards or re-encode previously configured cards, or to add a credential to Security Desk that matches a previously configured MIFARE DESFire card.
- **Raw credentials and native FASC-N card formats for PIV/PIV-I/CIV credentials:** Security Center natively recognizes 75-bit and 200-bit FASC-N credentials, but you can make Security Center display the details of other FASC-N versions by creating custom card formats. Unrecognized credential formats in Security Center are displayed as raw x bits instead of unknown x bits credentials.
- **Visitor pre-registration:** Visitors can now be registered and checked in either when they arrive, or pre-registered in advance to expedite the check-in process.

  For more information, see "Checking in new visitors" in the *Security Center User Guide*.

Reporting enhancements

- **New activation and expiration dates for cardholders and credentials in Import Tool:** Import tool now registers cardholder and credential activation and expiration dates when importing from CSV files or third-party systems.
- **Native double-badge events include cardholder and credential information:** With double-badge activation, a cardholder can unlock a door and trigger a preconfigured event by presenting their credential to the reader twice. The door remains unlocked and the event stays active until the cardholder badges again.

  For more information, see "About double-badge activation" in the *Security Center Administrator Guide*.

LPR enhancements

Security Center 5.8 GA includes the following License Plate Recognition enhancements:

General enhancements

- **Permit restriction support in AutoVu™ Free-Flow:** When setting up AutoVu™ Free-Flow parking lots, you can now use permit restrictions to configure time restrictions for the lots. Previously, permit restrictions were only available for patrol vehicles configured for University Parking Enforcement.

  For more information, see "Adding and configuring parking rules" in the *Security Center Administrator Guide*.
- **IPv6 support for Sharp cameras:** You can now enroll Sharp cameras using either the IPv4 or IPv6 address which are provided in the Sharp Portal.

  NOTE: IPv6 is currently supported by SharpV cameras running SharpOS 12.4 or later.

  For more information, see "Adding a Sharp, SharpV, or SharpX camera to the LPR Manager" in the *Security Center Administrator Guide*.
- **Sharp enrollment using the LPM protocol:** You can now add Sharp cameras to the LPR Manager using the License Plate Management (LPM) protocol to manage the connection. For Sharp cameras running SharpOS 12.7 or higher, the LPM protocol provides a secure and reliable connection to the LPR Manager role.

  For more information, see "Upgrading a SharpV to use the LPM protocol" in the *Security Center Administrator Guide*.
- **Reliable plate read path:** Security Center now ensures that license plate reads are not lost if Archiver activity is high. If the Archiver cannot save license plate reads to the database, the Sharp camera saves

plate reads locally. When communication is re-established, the plate reads are sent to the Archiver database.

Mobile and web apps

- **LPR camera monitoring (Web Client):** If your system includes fixed LPR cameras or patrol vehicles running Genetec Patroller™ software, you can now use Web Client to monitor license plate reads and hits.

  For more information, see "Monitoring patrol vehicles and LPR cameras" in the *Security Center Web Client Quick Start Guide*.
- **Generate reports on license plate reads and hits (Web Client):** Using the new *Plate report* task in Web Client, you can search for a specific license plate to report on, or you can filter the report for plate reads and hits from specific patrol vehicles or fixed LPR cameras.

  For more information, see "Viewing license plate reads and hits" in the *Security Center Web Client Quick Start Guide*.
- **Hotlist management (Web Client):** You can now add a vehicle's license plate to a hotlist in Security Center Web Client, which can then be used to alert officers of wanted individuals or parking violations, or to permit or restrict access to a parking facility.

  For more information, see "Adding license plates to a hotlist" in the *Security Center Web Client Quick Start Guide*.
- **Change user password (Web Client):** You can now change your Security Center password from the user settings in the Web Client interface.
- **Override unlock schedule (Web Client):** When monitoring a door controlled by an unlock schedule in Web Client, there is now an option in the *Monitoring* task tile to manually lock or unlock the door by overriding the schedule.

  For more information, see "Unlocking doors in Web Client" in the *Security Center Web Client Quick Start Guide*.

Resolved issues in Security Center 5.8 GA

Resolved issues are software issues from previous releases that have been fixed in the current release.

The following software issues were resolved in Security Center 5.8 GA.

Solution/Unit	Issue	Description
Access	2145754	When at least one Access Manager role in a system with multiple Access Manager roles is offline, information might be missing in the *Credential management* report.
Access	2138208	In SaaS deployments, magstripe ABA cards do not work offline, unless the firmware of the Synergis™ Cloud Link unit is Synergis™ Softwire 10.10 or later.
Access	2119154	The Global Cardholder Synchronizer role does not work in IPv6.
Access	1919171	Mercury EP and LP: When the panel reconnects to Synergis™ Softwire, the baud rate of reader ports in OSDP mode are reset to 9600.
Access	1917937	Events are kept for longer than the retention period configured on the *Properties* page of the Access Manager role.
Access	1899796	Receiving multiple access control events that use the email logger might cause the Access Manager role to be unresponsive.

Solution/Unit	Issue	Description
Access	1767190	Credentials are only partially enrolled when using the *Credential Management* task to automatically enroll the credentials.
Access	1480180	When a door is configured with more than one door sensor, *Door opened* and *Door closed* events are reported on every input state change.
Access	1113223	When a cardholder badges their credential on a reader inside an area, the cardholder is included in the people count of the area and the *Area presence* report, but not in the *Time and attendance* report.
Access	784592	If a cardholder enters an area, and then their card is swiped outside of the area, they are still considered inside that area in the *Time and attendance* report. **NOTE:** Make sure that the area is fully secured, meaning that people cannot enter or exit the area without swiping their card.
All	2157585	When you enable the **Use specific domain controller** option from the Active Directory role, group synchronization breaks in some cases.
All	1957972	When copying map objects from a geographic map to a georeferenced image map, the position of the map objects might be incorrect after pasting because of the differences in coordinate systems.
All	1704397	System security: You can configure Security Center users to not require passwords.
All	1693040	Server Admin does not enforce any restrictions on user passwords.
All	1142954	When using the *Motion search* task to query for motion events, the query returns results that include a lower motion percentage level than what was configured in the query.
Bosch	2125499	In the *Archive storage details* task, you cannot protect or unprotect video stored on Bosch VRM.
HID	1132888	When using an interlock configuration with a VertX V1000 controller and multiple doors, after lockdown is activated, the door is locked but the reader's LED remains green instead of red.
Intrusion	1458003	Intrusion detection units are created under the root partition, even though you selected a different partition during enrollment.
LPR	2148080	When the language of a remote Security Desk is set to French, you cannot export *Reads* and *Hits* reports with high resolution images to PDF.
LPR	2147987	When there is network latency, the clock on Sharp units is not synchronized with the LPR role.
LPR	2050318	On the *Properties* page of the LPR Manager role, retention periods cannot be set to zero days.
LPR	2020509	The alarm priority displayed in the *Alarm monitoring* task is incorrect when an event-to-action is configured to trigger an alarm when a hit occurs.
LPR	1921996	When creating a hotlist, the username you enter cannot include an underscore.

Solution/Unit	Issue	Description
LPR	1892675	The only way to get Sharp analytics (speed, confidence score, direction of travel, and so on) in Security Center is by creating annotation fields for each, and then adding them as columns in associated report tasks or the *Monitoring* task.
LPR	1632890	After sending live reads, hits, and Genetec Patroller™ positions to Security Center, when you manually offload the data to Security Center, there are errors in some of the files saved to the root folder.
LPR	1537295	Users that are not part of the Administrators user group cannot view the *General settings* page in the *LPR* task.
LPR	1404886	On rare occasions, Security Desk does not load BeNomad map files on a 64-bit client workstation properly.
LPR	642116	In a reads report or a hits report, the protection expiration for protected reads or hits displays the wrong expiration.
Video	2145174	The redirector sends duplicate stream information to a multicast address when earlier versions of Security Desk are connected.
Video	2135521	For cameras configured to record on-motion, the detection mechanism stops detecting motion and recording after GenetecVideoUnitControl32 crashes.
Video	2115553	Hardware acceleration cannot be disabled for Config Tool.
Video	2042968	During edge transfer, only the offline sequences that were recorded after the edge transfer is activated are downloaded from the SD card, instead of all offline sequences up to the retention period.
Video	2025696	When the Media Router redirector cannot start because the specified port it is already in use, the port and application that the redirector tries to use are not specified in the error message.
Video	1922645	The Auxiliary Archiver database can sometimes report start or stop times out of sequence if the windows clock is changed. This can cause playback issues or the timeline might not be not visible until the database events are repaired.
Video	1899688	When you perform an archive transfer backup onto a secondary server, the *No stream source found* error might occur if the secondary server has no archives for a specific camera.
Video	1856166	Archiver performance is negatively impacted because local time is evaluated on every frame received.
Video	1816994	After a network failure, the Media Gateway role does not come back online.
Video	1798836	On large systems, the Media Router or Directory role might suffer a significant performance hit.
Video	1796249	After upgrading from Security Center 5.2 or earlier, from the *Archive transfer* task, you cannot transfer video recorded in 5.2 to another archiver using a transfer group configured for protected video.

Solution/Unit	Issue	Description
Video	1603748	In the Security Desk *Motion search* task, when you query an encrypted camera, the warning *Motion search is not supported for this camera* is displayed. Motion search is not supported because the camera is encrypted, not because the camera does not support motion detection.
Video	1516121	In **Video** > **Archive transfer**, if no video was transferred after an archive transfer, the transfer is listed as *Success* in the transfer details, instead of *No video available*.
Video	1245250	If the video feed is rotated, motion detection zones are not applied to the correct region.
Video	1161966	When manually recording video using **In transit and at rest** encryption, and setting a value for **Time to record before an event**, there is sometimes a short period of video that you cannot play after recording has started.
Video	1161899	On the *Statistics* page in Config Tool, ghost cameras are included in the **Archiving cameras** count, but are not listed when you expand the *Archiving cameras* dialog box for details.
Video	1045965	If you cancel the *Motion search* task, the Archiver does not stop searching for motion, and will finish the motion search processing.
Video	1042345	The Auxiliary Archiver sometimes reports an *Archiving queue full* event, even though the queue is not full.
Web Client	747956	Federated entities cannot be edited in Web Client.

Resolved security-related issues in Security Center 5.8 GA

Resolved issues are software issues from previous releases that have been fixed in the current release.

The following security-related issues were resolved in Security Center 5.8 GA.

Solution/Unit	Issue	Fix
Access	1817228	In the Global Cardholder Synchronizer (GCS) role, a button was added allowing you to erase a previously pinned certificate so that the certificate can be replaced if compromised.
LPR	1962448	Input sanitization is performed when using XML import in the LPR Manager role to import plate reads.
LPR	1919698	A restriction on the file type that can be selected in hotlists and permits was added to protect against unintended code execution.
Web Client	2148700	Web Client Server was updated to protect against potential Denial of Service attacks through SignalR.

About the Genetec™ Update Service

The Genetec™ Update Service (GUS) is automatically installed with most Genetec™ products and enables you to update products when a new release becomes available.

You can use GUS to do the following:

- Update your Genetec™ products when a new release becomes available.
- Check for updates at regular intervals.
- Download update packages in the background. Updates must be manually installed.
- See when the system was last checked for updates.
- Automatically refresh the license in the background to ensure it is valid and the expiration date is updated.

  NOTE: Applies to subscription systems only.
- Enable various features, such as the Genetec™ Improvement Program.
- Review your firmware versions, get notified of vulnerabilities or recommended upgrades, and download firmware updates as recommended by Security Center.
- Automatically update the license after a major Security Center upgrade.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages. If using Internet Explorer, the video might not display. To fix this, open the **Compatibility View Settings** and clear **Display intranet sites in Compatibility View**.

Logging on to Genetec™ Update Service

To log on to Genetec™ Update Service (GUS), you must open the application and enter the GUS password that was provided to you (if one has been defined).

What you should know

- GUS is a Windows service that must be run by an admin account. By default, it runs under the Local System Account.
- The first time you start GUS, you are prompted to setup the password and enter your Config Tool credentials. The Config Tool credentials must be from an admin account. Only administrators have permissions to setup the GUS password.

To log on to the Genetec™ Update Service:

1 Do one of the following:

- Click **Start** > **All Programs** > **Genetec™ Security Center 5.x** > **Genetec™ Update Service**.

  NOTE: If you installed the service manually, it cannot be accessed from the start menu.

- Type `https://localhost:4595` in your web browser.

2 After the initial setup, you can enter your password and click **Sign in**.

Known issues in Security Center 5.8.1.0

Known issues are software issues that have been discovered in the current release or a previous release, and have not yet been resolved.

Generic issues are categorized by solution. Unit-specific issues are categorized by manufacturer and model.

Security Center 5.8.1.0 includes the following known issues:

Solution/ Unit	Issue	First reported in	Description
Access	2151677	5.8 GA	The ability to perform elevator reader shunting in Security Center is controlled by *Maintenance mode* privilege for doors.
Access	1577169	5.7 SR2	In the *Visitor management* task, if a visitor is checked in using two hosts, during the next visitor check-in, only one host from the previous check-in is pre-selected. The warning *Selected host is already part of a two-host delegation* is displayed. **Workaround:** Assign a second host manually.
Access	1191407	5.7 SR1	When you generate a report in the *Cardholder Management* task that includes *Activation date* or *Expiration date*, the report results only include cardholders. The report should also include credentials, which also include activation and expiration dates.
Access	1010579	5.7 GA	Advanced settings for returning visitors are not saved in the *Visitor management* task.
Access	365646	5.4 GA	Mercury EP: On the *Peripherals* page of a controller, the number of synchronized credentials sometimes disappears, such as after the Access Manager restarts.
Access	150069	5.2 SR5	Active Directory: When you are importing credentials from an Active Directory, only the last credential format that is mapped is used.
All	2243891	5.8.1.0	Dashboards: In the *Availability* widget, if you move the **Entity** column, not all components in the column move.
All	1918127	5.8 GA	In certain situations, expansion servers fail to connect to the Directory, despite good network connectivity. While in this state, the message "Server registered-Waiting for Directory response" shows indefinitely in Server Admin. **Workaround:** Restart the Directory.
All	1925181	5.7 SR4	When you restart Genetec™ Server on the server hosting the Federation™ role, you do not receive the *Connection to camera stopped by user* event for federated cameras.
All	1700130	5.7 SR2	If the GenetecUtility32.exe process crashes while you are receiving health events, some of the events might be lost.

Solution/ Unit	Issue	First reported in	Description
All	1523522	5.7 SR2	When a Security CenterFederation™ role is in maintenance mode, its child entities cannot be set to maintenance mode, causing inaccurate health statistics for those entities.
All	1107130	5.7 GA	In the Config Tool*System* task, when selecting the export format for **Scheduled tasks**, "PDF" is listed twice.
All	370163	5.4 GA	In the *Hotlist and permit editor*, if you configure a hotlist to use a remote file path, loading the hotlist will result in an "Invalid credentials" error.
All	235098	5.3 LA	When a lot of alarms are triggered on the system, the alarm count reported in Security Desk might not be accurate. **Workaround:** Log off and on again to see the correct alarm count.
All	259409	5.3 GA	Security Desk: Reports that cannot be filtered by **Custom Fields** are Access control unit events, Access rule configuration, Camera configuration, and I/O configuration.
All	234363	5.3 LA	Macros: If a macro has errors, and you change tabs, it is rolled back to the last error free version.
Axis	2255576	5.8.1.0	Audio from Axis FA54 units cannot be recorded, due to a code defect.
Bosch	2143870	5.8 GA	Video from Bosch VRM cannot be retrieved in Security Desk if Bosch VRM is configured to use HTTP in the Bosch extension of the Archiver role. **Workaround:** Change Bosch extension to use RCP, and then change it back to HTTP.
Bosch	2116878	5.7 SR5	The Bosch VRM license is not renewed in Security Center for Bosch extensions using HTTP. **Workaround:** Configure video to be stored in the internal storage of the unit instead of in Bosch VRM.
Bosch	2082373	5.7 SR5	Bosch units using firmware 6.50: After generating a report from the Security Desk*Archives* or *Forensic search* task, the video associated with the results cannot be played if it is stored in Bosch VRM. **Workaround:** In Config Tool, change the **Protocol** of the Bosch extension to **RCP**.
Bosch	2041783	5.7 SR5	Bosch units using firmware 6.50: From the Security Desk*Forensic search* task, generating a report for events stored on the internal SD card of the unit yields no results. **Workaround:** Do one of the following: • Downgrade the unit firmware to 6.42. • Use edge recording and playback from Bosch VRM.

Solution/ Unit	Issue	First reported in	Description
Bosch	1870446	5.7 SR3	Bosch: RTSPS video streaming does not work if the unit is added to the Archiver using the unit's IPv4 address, and the IP address is defined as *IP* in the server certificate Subject Alternative Name. **Workaround:** Connect the unit using hostname or using HTTP instead of HTTPS.
Bosch	1457390	5.7 SR2	Bosch: For the video sequence list from the camera to be available in Security Desk, edge recording must be active on the camera's web page. **Workaround:** Enable edge recording on the camera: 1. On the camera's web page, navigate to **Configuration** > **Recording** > **Storage Management**. 2. In **Recording Media** > **Managed storage media**, make sure the **Rec.1** or **Rec.2** check box is selected to activate the recording. 3. In **Configuration** > **Recording** > **Recording Status**, make sure the *Status* is *Running* for either one of the recordings.
Bosch	668843	5.5 SR3	Bosch VG5-7220: In the **Video mode** list of the **Hardware** tab of Config Tool, there are no high frame rate (60 fps) options available. **Workaround:** Use the **Installer Menu** on the unit web page to configure the **Max. frame rate** as 60 fps.
Bosch	505537	5.4 SR2	When Bosch Video Recording Manager (VRM) units are configured to use the HTTP protocol, you cannot perform edge playback from the VRM. **Workaround:** Configure the unit to use the Remote Control Protocol (RCP+).
DMP	1262717	5.8 GA	The **Faulty input arming behavior** configured on the *Properties* page of a DMP unit is applied to areas even when there are no faulty inputs associated with the area.
DMP	1245036	5.8 GA	When you add multiple DMP units to Security Center at the same time, the status listed in the *Unit enrollment* window is *Error*, even though the units are successfully added.
Documentation	1896193	5.7 SR3	In the online help guides accessed from Config Tool and Security Desk, on the *Index* page, when you double-click an index entry or select it, and then click **Display**, the linked article is not displayed.
HID	1745730	5.7 SR2	HID event-to-actions for HW Zones: If *Zone Active* is set as the event to trigger the action, the configured action is triggered when the arming state of the zone goes from Disarmed to Armed with the activation input already active. If *Zone Normal* is set as the event to trigger the action, the configured action is not triggered when the arming state of the zone goes from Armed to Disarmed.

Solution/ Unit	Issue	First reported in	Description
HID	1190516	5.7 SR1	For elevators using HID V1000 Networked Controllers, if floors are configured with different access rules, and one floor is out of schedule and should deny access, users cannot access any floors in the building.
HID	1154929	5.7 GA	HID Hardware Zone: If a zone is configured using the AND operator, and the zone state changes from *active* to *trouble*, an additional zone normal event is created at the same time.
HID	1092930	5.7 GA	Modifications you make to the Online Access Rule custom field value are not immediately synched to the unit. If the unit is configured to synch on a schedule, this limitation does not apply.
HID	227614	5.3 LA	HID Edge EVO EH400-K: Readers that use firmware version 2.3.1.605 do not buzz when a door forced event is generated.
ISD	133890	5.2 SR4	JBS-AF-1080P: Playback of a G64 file will freeze when using a speed of 6x or higher.
ISD	133670	5.2 SR4	JBS-AF-1080P: Cannot stream two multicast channels simultaneously in Security Desk.
ISD	131809	5.2 SR4	JBS-AF-1080P: Some of the supported resolutions listed on the unit's web page are not available in Security Center.
ISD	131565	5.2 SR4	JBS-AF-1080P: Changing the IP address, Subnet, or Gateway does not work.
LPR	2264790	5.8.1.0	After generating a report from the *Reads* task in map mode, the first time you select a read from the list of results, the map zooms in on a location without indicating where the read was captured. The next times you select a read from the list, the read is indicated on the map with a circle, but clicking on the circle displays the previous read in the tile bubble.
LPR	2151096	5.8 GA	If a SharpV is added to the LPR Manager using the LPM protocol and is then reconfigured to use the Security Center (legacy) extension, a duplicate offline SharpV is added to the LPR Manager so that associated plate reads can be retrieved.
LPR	2142225	5.8 GA	After disabling **Accept remote reboot requests** for a Sharp camera that is using the LPM protocol, the reboot option for that camera is still visible in Security Center.
LPR	1938566	5.8 GA	When you create a transfer group, you cannot add video units that are under Sharp units as sources. **Workaround:** To transfer from all video units under the Sharp unit, in the *Transfer group properties* dialog box, select the area that the Sharp units with video configured are associated with. This area must also have IP cameras under it.

Solution/ Unit	Issue	First reported in	Description
LPR	1862570	5.8 GA	The Hits report and the Reads report can show duplicate fusion streams for the same legacy Sharp camera. These duplicate streams have the same name, and it is not possible to delete the extra device from the UI. **Workaround:** Recreate the unit.
LPR	1860225	5.8 GA	The Reads/hits per day report might be off by 1 day when reporting on a federated site in a very different time zone.
LPR	1829435	5.8 GA	When sorted by descending timestamp, the Reads report and the Hits report return the first results from the database that match the search criteria, instead of the most recent ones.
LPR	1760241	5.8 GA	In the Reads report, filtering results on an empty user group returns all results instead of none.
LPR	1244123	5.8 GA	Patroller Plate Link: Hits report displays the patroller that made the first read instead of the patroller that enforced the hit.
LPR	2088432	5.7 SR5	The time zone used in the *Reads* report and the *Parking sessions* report is not always correct.
LPR	1197372	5.7 SR5	In a Genetec Patroller™ system where plate reads are offloaded manually, the *Hits* report attributes the hit to the patrol vehicle that performed the initial plate read instead of the patrol vehicle that enforced the hit.
LPR	1026167	5.7 GA	Genetec Patroller™ does not always reconnect to Security Center after a network disconnection has occurred, and the icon is red in Security Desk.
LPR	1020691	5.7 GA	If you save a workspace on a server using Security Center 5.6 and then upgrade to Security Center 5.7, the workspace will be loaded but the task will allow you to generate a report without selecting any entities, without generating an error.
LPR	952306	5.6 SR2	Parking zone management: When a NOPLATE read that is not matched to a parking session is edited, no *Unknown vehicle exited* event is created.
LPR	396367	5.4 GA	Hotlists: When an LPR Manager role stops unexpectedly, the account used to access hotlist files from it is locked out. **Workaround:** Manually unlock the account.
LPR	370163	5.4 GA	In the Hotlist and permit editor, if you configure a hotlist to use a remote file path, loading the hotlist will result in an "Invalid credentials" error.
LPR	100876	5.2 GA	Config Tool: The LPR Manager role status displays as online, even if the root folder path is incorrect.

Solution/ Unit	Issue	First reported in	Description
Video	2251076	5.8.1.0	Video does not restart after an Archiver failover from an IPv6 server to an IPv4 server on a UDP network. **Workaround:** The main server and secondary server must use the same IP version.
Video	2161243	5.8.1.0	When a hostname is entered as the Public address of the Genetec™ Server hosting the Media Gateway role, if the hostname is changed, the Media Gateway role must be restarted for the change to take effect. **Workaround:** Enter an IP address instead of a hostname.
Video	2154237	5.8 GA	Disabling Media Router **Secure communication** might freeze Security Desk tiles displaying federated cameras, if the federated system has **Secure communication** enabled. **Workaround:** Wait 3-4 minutes, or clear and reload the tile.
Video	2144310	5.8 GA	When a ghost camera only has edge-transferred video, that video cannot be played back.
Video	2139459	5.8 GA	Incorrect ONVIF metadata causes the Security Center media player to freeze for at most 12 seconds in forward and for an indefinite duration in reverse playback, depending on the data. **Workaround:** Disable metadata recording.
Video	2132405	5.8 GA	Cannot dewarp playback video when privacy protection is enabled for fisheye cameras.
Video	2025093	5.8 GA	Multicast IPv4 source filtering does not work consistently in some Windows 10 versions, including 1709 and 1803.
Video	1952891	5.8 GA	Selecting **Configure entity** for the Camera Integrity Monitor or Privacy Protector from the entity browser in a report task, takes you to **System** > **Roles** instead of **Video** > **Modules**.
Video	1029592	5.7 SR1	When using Privacy Protection, the recording in the timeline and the recording state presented in Security Desk indicates the state of the original stream even if the privacy-protected stream is shown.
Video	582417	5.5 GA	Failover: When the Record metadata, Redundant Archiving, and Encryption options are enabled for an Archiver, an overlay stream might not play back on exported G64x files after a failover.
Video	547854	5.5 GA	Maps: When viewing a fisheye camera in a map, the video cannot be dewarped.
Video	244781	5.3 LA	System status task: If an Archiver role is configured with a failover server, only the server hosting the role is reported as active in the task, not the one that is recording.

Solution/ Unit	Issue	First reported in	Description
Vivotek	1899054	5.7 SR4	Speed dome PTZ SD9362 and SD9364: After you enroll a video unit in Security Center, the time on the unit is one hour behind the actual time.
Web Client	2157797	5.8 GA	When you generate *Reads* and *Hits* reports in Web Client, thumbnails of federated LPR units are not displayed in the results. **Workaround:** Generate the reports from Security Desk.
Web Client	2106110	5.8 GA	In Web Client, there is no option to add a second host for visitors.
Web Client	2106110	5.8 GA	In Web Client visitor management, you can only replace the current visitor host. You cannot add a second one like in Security Desk.
Web Client	1825562	5.8 GA	When a user password is changed in Security Desk, Config Tool, or Web Client, the user is not disconnected from Web Client.
Web Client	1128361	5.7 GA	Cardholders and credentials that were created on a global partition and that are used for guests, do not have a specific icon in Web Client that distinguishes them from other cardholders.

Limitations in Security Center 5.8.1.0

Limitations are software or hardware issues that cannot be fixed. For certain limitations, workarounds are documented.

Generic issues are categorized by solution. Unit-specific issues are categorized by manufacturer and model.

Security Center 5.8.1.0 includes the following known limitations.

Solution/ Unit	Issue	First reported in	Description
Access	2232371	5.8.1.0	When a door is configured with more than one door sensor, *Door opened* and *Door closed* events are reported on every input state change from offline mode.
Access	2197119	5.8.1.0	On the *Peripherals* page of Synergis™ Cloud Link units, the **Type of reader** for readers controlled by interface modules can be edited, even though modifying the setting in Config Tool does not affect the setting in Synergis™ Softwire.
Access	1992856	5.8 GA	In the *Visitor management* task, before you can add a mobile credential to a visitor, you must enter an email address for that visitor, and then click **Save**.
Access	1938701	5.7 SR4	After a visitor is checked in and then set to inactive, you can delete the visitor, but cannot check out the visitor.
Access	1190526	5.7 SR1	When you add a hardware zone, if the input's initial state is inactive, the input appears as unknown in the *System status* task.
Access	1179902	5.7 GA	Global Cardholder Synchronizer (GCS): If the GCS role is running on an expansion server using Security Center 5.6 or earlier, you will have synchronization problems when the Directory server that it is connected to is upgraded to Security Center 5.7 or higher.
Access	1113100	5.7 GA	GCS: After deactivating the GCS role (it is offline) and then selecting a shared cardholder, the **Security clearance** field is grayed out and read-only, but it should still be modifiable.
Access	1067500	5.7 GA	If an area is configured with interlock, and one of the doors has an unlock schedule, you receive an *Interlock configuration error* message even though the configuration is valid.
Access	1048053	5.6 GA	On a system running an Access Manager role in backward compatibility mode for Security Center 5.5 or earlier, the interface modules of a Synergis™ Softwire unit will be displayed as Offline but its child devices will be displayed as Online. **Workaround:** Upgrade Access Manager.
Access	1039753	5.7 GA	If the GSC role and Federation™ Role run on the same server and point to the same directory, synchronizing federated entities causes the GCS to go into a warning state due to constant synchronization attempts. **Workaround:** Run the Federation™ role and GCS role on separate servers.

Solution/ Unit	Issue	First reported in	Description
Access	1037563	5.7 GA	On a Synergis™ appliance, if you configure the **Interlock** setting to **Single door Unlock** and then enable the visitor escort rule on the same area, access is always denied when the visitor and escort try to enter the area because it is an invalid configuration.
Access	1037274	5.7 SR1	The *Last sync time* displayed on the Global Cardholder Synchronizer role is updated even if changes from the source directory result in no changes to the target directory.
Access	1029849	5.7 GA	GCS: If a global partition already exists on the main server when a GCS role is created on a remote server, this global partition does not appear on the partitions list unless the page is refreshed by switching tabs or adding a another global partition.
Access	1003002	5.7 GA	GCS: When working from the server that is hosting the GCS role, if you change the assigned cardholder of a credential from *global* to *local*, a warning is issued for missing dependencies. You cannot have a shared credential assigned to a local cardholder.
Access	1002738	5.7 GA	GCS: When the GCS role manages many entities, the time it takes to prefetch information from both directories takes a long time.
Access	1000780	5.7 GA	GCS: If the GCS role restarts while in the *conflict* state due to overflow from a license limitation, the conflicting item will be deleted when the role restarts.
Access	956063	5.7 GA	GCS: If a user adds a visitor group containing existing cardholders to a global partition (which is not a recommended action), the visitor group will not be synched properly and you will not be able to add visitors to this group from Security Desk.
Access	697778	5.6 GA	When you search for unused credentials in the *Credential configuration* report, credentials of federated cardholders are not included in the results.
Access	601549	5.5 GA	It is not recommended to use cardholder or credential *Expiration* settings with Federation™ If the cardholder or credential expires at a federated site (for example, when using the *Set expiration on first use* option), the status of the cardholder or credential is not synchronized at the host site.
Access	546220	5.5 GA	Global I/O: For a Security Center 5.5 federated server, the arm/ disarm widget for I/O zones is enabled when the master unit is offline.
Access	506048	5.5 GA	After modifying an assigned output behavior of an IO Zone, you need to perform a manual synchronization on the Master unit for the modified output behavior to be applied.
Access	474260	5.5 GA	Config Tool: The access control unit stays in warning state (yellow) when the door interface is deleted before the door entity.
Access	396679	5.4 GA	Zone: When you arm a zone and configure an **Entry delay**, only the first event and a **Zone armed** event are generated for the zone.

Solution/ Unit	Issue	First reported in	Description
Access	264771	5.3 GA	If perimeter units of an area are managed by more than one Access Manager, multiple events are generated for the same warning. If no perimeter units are configured for an area, an "Entity Warning" event is received when the area state changes from "Running" to "Warning".
Access	262840	5.3 GA	When you upgrade to Security Center 5.3 or later, all door properties that pertain to a Synergis™ appliance are replaced with the default values of the release you are upgrading to.
Access	262293	5.3 GA	Areas that inherit Access control rules from parent areas continue to have those rules take effect even if the parent area has all Access controls turned off.
Access	241207	5.3 LA	Forgiving an antipassback violation for the **All cardholders** group does not work. **Workaround:** Use specific cardholder groups instead.
Access	238045	5.3 LA	Access granted events can display "Unavailable information" in the description column for returning visitors.
Access	194341	5.3 LA	In the Custom card format editor tool, the *Sequence Generator* cannot be used with UTF-8 Wiegand field type. **Workaround:** Use a Hexadecimal or Decimal field type.
Access	154639	5.2 SR5	Active Directory: If you have multiple cardholders with the same credential PIN, and you set one of the PINs to inactive so you could import the cardholders, you will not receive access granted or access denied events in Security Desk. **Workaround:** Make sure that you do not import multiple cardholders with the same PIN.
Access	153384	5.2 SR5	Access Manager: Under specific conditions, when a user presents his card on one side of the door, it is the reader on the other side of the door that flashes green. This behavior only occurs under the following conditions: • At least 2 cardholders with the same PIN, one of which is inactive. • One side of a door is configured as Card and PIN, the other side as Card or PIN. • The cardholder with the invalid PIN presents his card on the Card or PIN side of the door.
Access	153195	4.0 GA	Modifying the members (doors, elevators, captive areas) of an area might disrupt the *Time and attendance* report of that area for a time range before the change.
Access	149745	5.2 SR5	If a visitor is attached to an incident report, when the visitor is checked-out they are removed from the report.

Solution/ Unit	Issue	First reported in	Description
Access	149027	5.2 SR5	You cannot import both PINs and cards from a .csv file using the Import tool. **Workaround:** Import the PINs and the cards separately using two .csv files.
Access	115855	5.3 LA	If you import more than 5000 credentials and cardholders with pictures simultaneously using the Import tool, some credentials might not be associated with their cardholders anymore.
Access	96628	5.2 LA	Security Desk: If you edit a visitor's credential in the *Visitor management* task, and then switch to the next visitor's details page without pressing the save button, your changes are still saved.
Access	83840	5.2 LA	When you export or print the *Access rule configuration* report, the Icon column is not included.
Access	71422	5.2 LA	Multiple credentials might be requested for the same cardholder if the requests were created by users from different partitions.
Access	70694	5.2 LA	You cannot synchronize with the Active Directory when a field contains a non-breaking space.
Access	70538	5.2 LA	If an error occurs while synchronizing with an Active Directory and the synchronization pauses, the synchronization will not complete.
Access	70535	5.2 LA	You cannot synchronize HID H10302 37-bit and HID H10304 37-bit credentials with an Active Directory if they are using the maximum values.
Access	69460	5.2 LA	When you import a user or cardholder from an Active Directory and they are members of the Active Directory role's partition by default, if you manually remove the partition membership from the entity, the partition is not re-added the next time you synchronize.
ACTi	154959	5.2 SR1	KCM and TCM models: These units do not support using a multicast IP address outside the range of 224.5.0.1 to 239.255.255.255.
ACTi	154935	4.0 GA	ACM1100: Setting the Hue option in the camera's Attributes tab in Config Tool has no effect on the unit.
Advidia	177547	5.2 SR7	A-46: You cannot view live video from an MPEG-4 stream.
Advidia	177545	5.2 SR7	A-46: You cannot view the live stream when the Connection type is set to multicast in the Network settings. **Workaround:** Under **Network settings**, beside **Multicast address**, enter the following address: 224.16.17.3.
All	2258206	5.8.1.0	Dashboards: In *Health* widgets, changes to the width and position of table columns are not persisted from 5.8 GA Security Desk clients to Security Desk clients of later versions. **Workaround:** Upgrade all Security Desk clients to 5.8.1.0 or later.

Solution/ Unit	Issue	First reported in	Description
All	2228289	5.8.1.0	From the *Dashboards* task in a 5.8 GA client, if you try opening a *Health dashboard* task that was saved in a later version of Security Center, the *Dashboards* task closes without warning. **Workaround:** Upgrade all Security Desk clients to 5.8.1.0 or later.
All	2119701	5.8 GA	Dashboards: In the *Security checklist* of the *Security score* widget, the status of the **Synchronize all clocks within your system** hardening entry might not be accurate if you use NetTime to synchronize the clocks within your system.
All	2047847	5.7 SR5	Starting in Security Center 5.7 SR4, upgrading the Directory database containing many cardholder pictures might take longer than usual.
All	2031824	5.8 GA	Dashboards: In the *Security checklist* of the *Security score* widget, if the **Do not connect to SQL Server with an account that has administrative privileges** hardening entry is respected, you might get a message saying that the **Encrypt the database file** hardening entry cannot be evaluated. For example, *Media Router does not have sufficient privileges to detect and show the hardening status, user evaluation required.*
All	2031459	5.8 GA	Dashboards: In the *Security checklist* of the *Security score* widget, if the **Do not connect to SQL Server with an account that has administrative privileges** hardening entry is respected and connection encryption is not enabled in Security Center, you get a message saying that the **Use encrypted communication between database servers and Genetec™ services** hardening entry cannot be evaluated. For example, *Media Router does not have sufficient privileges to detect and show the hardening status, user evaluation required.* **Workaround:** In Config Tool, on the *Resources* page of each role that cannot determine the encryption status, enable the **Encrypt connections** option.
All	1962377	5.8 GA	Dashboards: In the *Security score* widget, the **Do not connect to SQL Server with an account that has administrative privileges** hardening entry does not take multiple Directory roles and database failover into account.
All	1870132	5.8 GA	Dashboards: In the *Security score* widget, it can take up to five minutes for new hardening entries to be listed in the *Security checklist*.
All	1716732	5.7 SR2	Non-admin users with the *Add users* privilege might not be able to grant partition access to users they create if they themselves do not have access to all partitions in a given hierarchy.
All	1669420	5.8 GA	You cannot control dashboards using the *Remote* task in Security Desk.
All	1478998	5.7 SR2	When generating a *Health history* or *Health statistics* report, the **Source entity** filter displays all federated entities, instead of only displaying federated cameras.

Solution/ Unit	Issue	First reported in	Description
All	1462536	5.7 SR2	When you reboot or move a video unit from one Archiver to another, in the *Health history* report, the listed Health events are *Connection to camera stopped unexpectedly* and *Connection to unit stopped unexpectedly* instead of *Stopped by user*.
All	1448973	5.7 SR2	In the *System status* task, when you select **Zones** from the **Monitor** list, the query returns no results, even though zones exist in Security Center.
All	1184208	5.7 SR1	On a workstation where .NET 4.6.1 is installed, if you play a video overlay that was generated on .NET 4.6.2, the generator will add the *PixelsPerDip* property to the generated XAML and the player will throw an exception because the property did not exist in older .NET versions.
All	1177861	5.7 SR2	When a role uses an SQL database running on a network drive, the **Notify me when reaching: Disk space** option does not work.
All	1011458	5.6 SR4	Directory failover: When the SQL database used for Directory failover is lost, the Directory Manager role goes into a warning state, but there is no event in the *Health history* task.
All	889969	5.6 GA	Windows 7, 8.1: If the **Resilient connection** option is enabled and the Federation™ role is disconnected from a federated Security Center Directory server that is using Windows version 7 or 8.1, the Federation™ role might not be displayed in a warning state.
All	781950	5.6 GA	Maps: When you are viewing federated maps in Security Desk, KML layers are not displayed.
All	750320	5.6 GA	Maps: If you are using the Security Desk on a remote desktop, ESRI ArcGIS maps might cause Security Desk to freeze. **Workaround:** Disable hardware acceleration for Security Desk, by starting Security Desk from the command prompt using `SecurityDesk.exe -nohwa` as the command line.
All	747939	5.6 GA	Maps: You cannot view federated maps that were created using an ESRI map provider in Security Desk.
All	743511	5.5 SR4	Network routes are not created for federated networks.
All	549272	5.5 GA	Audit trails are not logged when changing values in the Hardware tab of the Synergis™ Unit in Config Tool.
All	385441	5.4 SR3	If the system's video card has more than 4GB of memory, the Hardware information dialog box does not display the correct amount of memory.
All	379423	5.4 GA	Failover: After a Map Manager role fails over, maps that were created using images are blank.
All	279232	5.3 SR1	Diagnostic Data Collection Tool: Performance counters are not installed on Windows XP/2003 32 bit computers.

Solution/ Unit	Issue	First reported in	Description
All	263573	5.3 GA	When you have an archive viewing limit defined in Security Center 5.3, the same limit is defined if and only if you log in to Security Desk 5.3. Archive viewing is not limited to you if you log in to Security Desk 5.2.
All	262129	5.3 GA	A user can have enough privileges to delete an action without having enough privileges to modify that action.
All	260123	5.3 GA	Virtual Zone: A *Normal Zone* event is not triggered when the input is changed from *Trouble* to *Normal*.
All	260106	5.3 GA	Virtual Zone: An *Active Zone* event is triggered within a reactivation threshold time frame. The *Active Zone* event should be triggered only after the reactivation threshold expires.
All	244441	5.3 LA	Security Desk: If a public or private task is opened and you save your workspace when another task is active, when you log in again, the active task is the public or private task, not the task that was active when you saved.
All	241800	5.3 LA	Security Desk: The message "An error occurred while processing entity's past events" is displayed when opening Security Desk while several cameras are monitored.
All	235040	5.3 LA	List of available partitions to which a user can be added depends on whether **Partitions** is expanded in the **Relationships** section of the **Identity** tab.
All	234304	5.3 LA	Incidents report: Custom incident fields don't always update correctly after being modified. **Workaround:** Regenerate the report.
All	219222	5.3 LA	When using remote Security Desk, Auto-locking your workstation might disable remote monitoring.
All	217061	5.2 SR9	Running Skype under Windows 8.1 prevents Server Admin from running, thus blocking the Security Center installation. **Workaround:** Do one of the following: • Close Skype before starting Security Center installation. • Specify a different Web server port (default=80) during installation.
All	212894	5.3 LA	If the primary server is a slower machine than the next available standby server, the Directory role does not fail over to the standby server correctly. **Workaround:** Adjust the failover timer on the standby server. To do this: 1. Open the *GeneralSettings.gconfig* file located in *C:\Program Files (x86)\Genetec Security Center 5.8\ConfigurationFiles*. 2. Add the following line: `<FailoverSettings WaitForLeaderTimeout="00:01:00" PositionTimeoutIncrement="00:00:30"/>`

Solution/ Unit	Issue	First reported in	Description
All	208375	5.3 LA	You cannot attach more than four entities for the *Display an entity in the Security Desk* action; only a maximum of four entities get displayed in Security Desk.
All	205349	5.3 LA	For computers that have Security Center Client installed and are using real-time overclocking (turbo boost mode), the CPU meter does not accurately display the CPU of your computer.
All	200589	5.3 LA	Migration: After migrating, your cameras are not displayed in the same tiles in Security Center as they were in Omnicast™.
All	174862	5.2 SR7	When a playback source such as an Archiver is removed while Security Desk is running, you might experience problems playing back archived video. **Workaround:** Log off from Security Desk and Log back in.
All	171207	5.3 LA	RabbitMQ is not detected as a prerequisite after being manually uninstalled. Rabbit MQ and Erlang libraries are automatically installed by the Security Center 5.3 InstallShield. When you uninstall Security Center 5.3 they are not automatically removed. You can remove them manually, but if you plan on reinstalling Security Center 5.3 at a later time, uninstall Erlang first and then RabbitMQ. Otherwise, when you reinstall Security Center 5.3 the InstallShield does not detect that RabbitMQ is missing and will not install it.
All	156797	5.0 GA	Config Tool: For languages written from right to left, such as Arabic and Persian, the user interface of some tools and configuration tabs in the Config Tool has not been inverted.
All	153252	3.0 GA	Scheduled task with "On startup" recurrence property might not run on startup. To avoid this problem, limit the "On startup" tasks to "Execute a macro" actions.
All	153228	5.0 LA	Security Desk keyboard shortcuts cannot be used (such as space to acknowledge an alarm) when the focus is on a tile displaying a map.
All	153225	3.0 GA	Database backups cannot be purged when the database server is not on the same computer as the server application (Security Center Directory or Synergis™ Access Manager).
All	153223	3.0 GA	Time zone abbreviations are not supported in the printed reports.
All	153222	3.0 GA	Omnicast™ 4 alarm priorities are not converted when federated in the Security Center. All federated Omnicast™ alarms have a priority of 1.
All	153221	3.0 GA	The status of a device (camera or door) shown in a XAML map is not updated on the map when the device goes temporarily offline (red) and back online: **Workaround:** Remove the map from the canvas and drag it back to the canvas.
All	148382	5.2 SR5	Unless the supervisor is the administrator, their password cannot be empty, even though Active Directory users can have empty passwords.

Solution/ Unit	Issue	First reported in	Description
All	142540	5.2 SR5	Directory Failover: For Directory failover to work, all Directory servers must use the same software version (X.Y) and service release (SRx).
All	108161	5.2 SR1	The diagnostic tool reports an error when diagnosing a camera that uses HTTPS.
All	102141	5.2 GA	If you forward an active alarm with a message to a user who is logged off, when that user logs on they will receive the alarm, but not the message.
All	101198	5.2 GA	Windows Server 2012: After you install Security Center, the Server Admin application is not available from the Windows Start menu. **Workaround:** To open Server Admin, type the following URL into your Web browser: *http://localhost/Genetec*. **NOTE:** This issue is not present for Windows Server 2012 R2.
All	100973	5.2 GA	You cannot copy configuration settings to imported Active Directory user groups using the Copy configuration tool. Even though you receive a *Copy process completed* message, the configuration is not copied.
All	84032	5.2 LA	When generating an *Audit trails* report, the only information you are given about threat level configuration changes is if the threat level was added, deleted, or modified.
All	67452	5.2 LA	If an alarm is triggered with a source condition and is forwarded to a Security Desk that has a version older than 5.2 installed, when the alarm is acknowledged, the alarm only appears as acknowledged on the forwarded workstation when Security Desk is restarted.
All	56703	5.1 GA	Security Desk: Not all query filters in reporting tasks are updated live when the system configuration changes, such as when new custom fields or custom events are added. **Workaround:** To view the new query filter options, delete the task and recreate it.
American Dynamics	296381	5.3 SR3	ADCi800-D021: When the connection type is set to Multicast, live audio input for the Microphone does not work.
American Dynamics	279304	5.3 SR1	American Dynamics ADVEIPSD35N goes offline when you request a video and the connection type is configured to multicast.
American Dynamics	217800	5.2 SR9	American Dynamics Illustra 610: Changing the resolution on any video stream causes the unit to reboot.
American Dynamics	154963	5.2 SR1	Changing the resolution or video data format restarts both video streams and there is a 35 second delay before live streaming resumes. As a result, Boost quality is not supported, and Video quality settings on a schedule are affected.
American Dynamics	151646	5.2 SR5	American Dynamics Illustra 400: The MJPEG live stream can only use a frame rate of 7 fps or higher.

Solution/ Unit	Issue	First reported in	Description
Ampleye	130566	5.2 SR4	Ampleye Nox-20, Security Desk: When viewing live video that uses a high resolution, there is a delay and the video is not smooth.
Aperio	540376	5.5 GA	Passage Mode (double-swipe): Passage mode does not work if the door is configured to relock on close.
Arecont	791328	5.6 GA	When you add Arecont video units in Security Center, the lightning frequency value is changed to 60 Hz. **Workaround:** After the unit is added, change the frequency value in Config Tool. For information about configuring the frequency for Arecont units, see the *Security Center Video Unit Configuration Guide*.
Arecont	584113	5.5 SR2	Arecont AV8365DN, AV8185DN: Unit motion detection does not work when streams are set to H.264.
Arecont	400132	5.3 SR4	Arecont AV5585PM unit shows transmission lost errors when its cameras are frequently disconnected during Security Desk task cycling.
Arecont	154961	5.2 SR1	AV20365DN: The Brightness specified in the **Color** tab for channel 1 is applied to all four channels. **Workaround:** Clear the **Equalize Brightness** option in the unit's web page.
Arecont	123948	5.2 SR4	Arecont AV12186DN: After enrolling the unit in Security Center, two of the video streams are displayed upside down in Security Desk.
Axis	1843635	5.8 GA	Security Center does not filter out excluded zones when Axis motion detection is configured on the unit. If these excluded zones are in the first 6 zones monitored by Security Center, the zone will not generate events.
Axis	1586076	5.7 SR2	Axis: When moving a unit to an upgraded Archiver (5.7 GA or later), the unit keeps its old configuration and codec configuration is not available. Codec configuration is only available for units added in Security Center 5.7 GA or later.
Axis	913792	5.6 SR1	P3707-PE: If you are using the AXIS Video Motion Detection (VMD) 3.x application for on-unit motion detection and motion zones are configured, when you rotate the video image the video unit goes offline.
Axis	824875	5.6 GA	Axis T8311 joystick: After you release the joystick, the PTZ motor continues to pan or tilt for about a minute.
Axis	573154	5.5 SR2	Axis P3707-PE: Playing back video recorded on the edge does not work well when you fast forward, rewind, or seek to a specific time.
Axis	342725	5.3 SR2	When performing edge recording, edge playback, or archive transfer (video trickling), you must use firmware 5.50 or higher.
Axis	341115	5.4 SR3	Frame rate might be slower than expected when using RTSP over TCP or RTSP over HTTP in MJPEG.

Solution/ Unit	Issue	First reported in	Description
Axis	154966	5.2 SR3	Q6034-C: When streaming video at high resolutions, the video might freeze or you might see artifacts when there is fast movement in front of the camera. This also might happen when controlling the PTZ.
Axis	154936	5.0 GA	There might be a time delay when receiving data from a device's serial port.
Axis	133664	5.2 SR4	Axis Q7436: When using an H.264 custom format, frame rates higher than 30 fps are not respected and the keyframe interval might not be correct either.
Axis	103089	5.2 SR1	M3006-V: Setting the **Image Rotation** to 90 or 270 on the *Hardware* tab for an H.264 stream causes frame rates to drop.
Axis	100977	5.2 SR1	M3007-P/PV: Streaming at more than 12 frames per second is not supported. It is also recommended to use only two streams at a time, and to disable unit motion detection for streams that aren't using it.
Axis	96200	5.2 GA	Windows 7 and later: Axis 292 units cannot be added to the Archiver.
BCD	896252	5.6 SR4	BCD-GHP-QSI7-MT-8: Machines with Skylake processors use a lot of CPU and are very slow.
Bosch	1956161	5.7 SR4	Edge recording sequences cannot be retrieved from a Bosch unit that is behind a Network Address Translation (NAT) and using firmware 4.00 or higher. **Workaround:** Use firmware 3.52 or 3.53 on the Bosch unit.
Bosch	758066	5.5 SR4	Bosch VG5 units: Video analytics events are not received in Security Center.
Bosch	674379	5.5 SR3	Bosch: On the **Properties** page in Config Tool, changing the **Discovery port** of a unit causes the unit to go offline. **Workaround:** Right-click on the unit and add it again using the new discovery port.
Bosch	352095	5.3 SR3	When you move a Bosch unit from one Archiver to another, the Bosch extension is not removed from the original Archiver. **NOTE:** Delete the Bosch extension manually from the Archiver.
Bosch	268911	5.3 SR1	Bosch NIN-70122: Dewarping is not supported for edge playback.
Bosch	252241	5.3 SR1	Smooth reverse playback is not supported with Bosch MPEG-2 devices.
Bosch	240694	5.3 LA	Bosch VIP XD: When you drag and drop an analog camera sequence into an analog monitor, only the name of the first camera appears in the sequence. Subsequent camera names are not displayed.
Bosch	216420	5.2 SR9	Bosch VIP X16 XF E: The Config Tool settings for the MJPEG video stream are ignored by the unit.

Solution/ Unit	Issue	First reported in	Description
Bosch	202229	5.2 SR8	When configuring the discovery port for a unit or extension, port 1900 is not supported. **Workaround:** Use a Telnet session to reconfigure the discovery port.
Bosch	185163	5.2 SR7	VRM: Trickling or playing back audio is not currently supported.
Bosch	173635	5.2 SR7	XDXF Decoder: When playing a sequence in an analog monitor, the transition between cameras is not smooth.
Bosch	154954	5.2 SR1	X20XF-E, X40XF-E, X1600-XFM4: The Bit rate setting in Config Tool has no effect on the unit. **Workaround:** Use the Maximum bit rate setting to configure the bit rate.
Bosch	154953	5.2 SR1	If the Connection type is set to "Best available", the video might freeze during a camera sequence transition. Also, the camera sequences might not resume if they have been paused for more than 15 seconds. **Workaround:** From the Connection type between Unit and Archiver drop-down list in the Analog monitor Network tab, select Unicast UDP.
Bosch	154950	5.2 SR1	You cannot query a video sequence if the camera is password-protected.
Bosch	154948	5.2 SR1	Flexidome NDN-498-P: Switching the Video data format or Resolution in MJPEG does not work.
Bosch	109469	5.2 SR1	Bosch NDC-274-PT: Region of Interest (ROI) is lost after rebooting the unit.
Bosch	107666	5.2 SR1	Bosch Region of interest (ROI): Unit motion detection applies to entire zone captured by the camera instead of within the ROI area. **Workaround:** • Use software motion detection. • Use the first stream to create the motion detection zone.
Bosch	103836	5.2 SR1	Bosch NWC-0455: Video resolution set on the *Video* tab of Config tool does not match the resolution displayed in the Live video window of Security Desk.
Bosch	76282	5.1 SR2	Bosch MPEG2 units: G64-to-ASF conversion takes longer on Security Center than on Omnicast™.
Canon	104842	5.2 SR1	VB-H41: Streaming multiple MJPEG streams might cause *Waiting for signal error* or corrupted video in Security Desk.

Solution/ Unit	Issue	First reported in	Description
Cobham	139341	5.2 SR6	Cobham NETH264ENC-HD: If you set the unit mode to MPEG4 Dual SD and the streams to UDP Multicast in the unit web page, when you add the unit in Config Tool the streams might be corrupted. **Workaround:** Delete the unit from Security Center, change the unit mode to H.264 in the unit web page, and then add the unit in Config Tool.
Coldstore	259583	5.3 GA	Coldstore: Archives transferred to an Archiver where a Video Mover is installed, won't be moved, if no camera is associated with them.
Dahua	956724	5.7 GA	In Security Center, full PTZ capabilities are sometimes shown as available for cameras that have only zoom capabilities. If you attempt to use a command that is not supported, the camera might reboot.
Dahua	244612	5.2 SR10	CBR and VBR bitrate modes are configurable on the Dahua unit, but Security Center assumes the bitrate should be replaced by image quality. Genetec Inc. cannot correct this problem without adversely affecting previously affected Dahua cameras.
Dahua	244558	5.3 SR1	The rewind function is not available during a unit playback. It generates a "No data available" message and playback stops.
Dahua	244446	5.2 SR10	The Dahua DVR The driver is unable to identify the DVR device product type, or model name, from the Dahua SDK.
DMP	1423670	5.7 SR5	DMP intrusion panels: When you use the keypad of the panel to change the input bypass to **On**, the panel does not send the input state to Security Center.
DMP	281217	5.3 SR1	Trouble messages on armed areas result in incorrect state after disarming the area in alarm. **Workaround:** Do not use trouble messages in "Armed Open" or "Armed Short" input states.
DSC	121718	Plugin - DSC 4.0	When you change the entity name of a DSC unit, the name change is not reflected in any associated partitions and zones. **Workaround:** Delete and recreate the unit with a new name.
Dynacolor	501799	5.4 SR2	Dynacolor Z4SA-D video units have one input pin. When added to Security Center, the system shows 16 input pins for the camera.
Euklis	254090	5.3 SR1	Dewarping: Without a direct connection (same subnet) from the Config Tool to the camera, the dewarping lenses cannot be configured.
Euklis	170471	5.2 SR7	KLIS 360-5M-IR: There is a delay of up to ten seconds when viewing a dewarped image in Security Desk.
Hanwha	2195594	5.8 GA	SPE-1610 units: After starting an MJPEG stream, the audio does not work for an undetermined time because of a camera resource limitation.

Solution/ Unit	Issue	First reported in	Description
Hanwha	1892004	5.7 SR4	In Config Tool, after adding the SPE-1610 encoder using the Unit enrollment tool, only 5 of the 16 video channels are displayed in the area view.
Hanwha	1924256	5.7 SR4	SPE-1610 encoders: Within the first minute after adding the unit in Config Tool, not all the cameras can start streaming in Security Desk at the same time.
HID	1154809	5.7 GA	HID Online Access Rule: When a door has two access rules with one field set to true and the other field set to false, if the unit goes offline, the access control rules do not work properly on the door.
HID	1113092	5.7 GA	When an area controlled by an HID unit has interlock enabled and a lockdown input is activated, an access request for a cardholder that has access to the door results in an access granted event being reported even though the door does not unlock.
HID	1105099	5.7 GA	HID: When zone input is active before the zone becomes armed, there are no events indicating that the zone is in an active state at the time the zone was armed.
HID	1035525	5.7 GA	If an HID unit is offline, event-to-actions for Hardware zones do not trigger an output on a *Zone armed/disarmed* event.
HID	1015091	5.7 GA	If the tamper input for an HID unit has been triggered, the unit will be in a warning state even if the input is configured as shunted (disabled).
HID	976511	5.6 SR2	Backward compatibility: HID VertX V100,V200,V300 units appear offline when the *Access Manager* role is on an expansion server running Security Center 5.5 and the main server is running Security Center 5.6.
HID	945037	5.6 SR2	When Card and PIN is enabled for a reader, and the cardholder enters a valid pin but does not swipe their card, the event raised is **Access Denied Unknown Credential**. It should be **Access Denied Invalid PIN Credential**.
HID	890066	5.6 SR2	Edge EVO: If the configured *Door relock after opening* time is greater than the *Grant time*. The *Door relock after opening* is not respected.
HID	889123	5.6 GA	VertX EVO units, Edge EVO EH400: If the reader setting of a door is configured as **Use card and PIN** and the settings are synchronized with the unit, then if you present your card at the reader but do not enter a PIN, the timeout event is not received in Security Desk.
HID	875893	5.6 GA	Legacy controllers: Firmware 2.2.7.300 and earlier have a memory leak issue that occurs during synchronization that might cause the synchronization to fail and the controller to reboot.

Solution/ Unit	Issue	First reported in	Description
HID	875891	5.6 GA	If you use the *Unit Firmware Update tool* to upgrade a unit that has **Secure mode** disabled, then the unit will go offline after the upgrade. **Workaround:** For EVO units, issue the firmware upgrade from Config Tool. For legacy units, log on to the unit's webpage after the firmware upgrade, and manually enable FTP and Telnet capabilities.
HID	875885	5.6 GA	HID Edge and VertX controllers have a vulnerability that allows someone logged on as the *root* user to execute code remotely. The vulnerability could be exploited using the controller's UDP discovery service to inject commands into the controller, which compromises the controller's security. Authentication is not required to exploit this vulnerability. For more information, see the Knowledge Base article KBA01448.
HID	875884	5.6 GA	Firmware 2.3.1.793 for VertX EVO and 2.3.1.927 for Edge EVO are vulnerable to the *Heartbleed* bug. This vulnerability has been fixed in version 3.3.1.1168 and later.
HID	875883	5.6 GA	You cannot downgrade the firmware of an HID unit after upgrading it to 2.3.1.841 for Edge EVO, or to 2.3.1.791 for VertX EVO.
HID	799463	5.7 SR5	HID: If a door is opened while the unit is offline, REX On/Off events are reported in Security Desk when the unit comes back online, even though the **Ignore REX event while door is open** option is enabled on the unit.
HID	349528	5.3 SR2	HID: Antipassback using HID controllers will only work if the cardholder has one credential. If the cardholder has more than one credential the unit will manage them individually.
HID	234495		Elevator outputs that are controlled by an HID unit do not change state on an “Access Granted” event when the Access Manager sends a database changeover command with Pre-Index to the unit.
HID	204539		VertX V2000: If the **Reader buzzer behavior** of a door is set to **Suppressed when door closes** and a **Door forced open** event is generated, the reader beeps once.
HID	204531		VertX V2000: If the **Reader buzzer behavior** of a door is set to **Suppressed when door closes** and a **Door forced open** event is generated, the reader starts buzzing but the LEDs do not start blinking.
HID	201163	5.3 LA	If the **Time to ignore REX after door closes** value is set to 0, the door still unlocks if the REX is activated, and the event is not shown in Security Desk.
HID	201155	5.3 LA	Edge EVO: The **Door relock** setting is not respected. **Workaround:** For Edge EVO units, the **Door relock** value must be lower than the **Standard grant time** for the door.
HID	201121	5.3 LA	VertX EVO, Edge EVO: The **Reactivation threshold** value for zones is not respected.

Solution/ Unit	Issue	First reported in	Description
HID	184305	5.3 LA	You cannot monitor live output states from the *System status* task.
HID	153220	5.0 GA	HID units do not support Reactivation threshold settings for zones entities.
HID	153214	5.0 LA	HID: PIN credential active state is ignored when used with a CARD & PIN reader.
HID	153211	4.0 GA	Elevator control: Configuring an exception to unlock schedule (controlled access) on a floor without a corresponding unlock schedule (free access) might cause the VertX controller to stop sending events to the Access Manager.
HID	151645	5.2 SR5	HID Edge EVO EH400: After enrolling a standalone Edge EVO EH400 controller, two ghost readers appear in Config Tool.
HID	96527	5.2 LA	HID VertX: If the wire of a 4-state supervised input is physically cut or shortened, then the **Input state** field in the *Peripherals* tab in Config Tool is always set to **Trouble (open circuit)**.
HID	79324	5.2 LA	For HID VertX units configured to use hard antipassback, if the cardholder is granted access but does not enter the area, the people count is still affected, and *First person in* or *Last person in* events could still be triggered.
HID	79154	5.2 LA	For HID VertX units, the Access manager role only supports entry detection when the access controller is online. When the access controller is offline, every Access granted event is associated with an Entry assumed event, even if the cardholder did not enter the area.
HID	57119	3.0 GA	You must stop the Access Manager before starting a unit swap operation in the Config Tool. After the swap is completed, the Access Manager can be restarted.
HID	57118	3.0 GA	The HID Edge device (EdgeReader or EdgePlus) can only be used to control a single door. You cannot use two HID Edge devices to configure a door with two readers. The supported configuration for an Edge device is a card-in/REX-out door.
HID	57116	3.0 GA	The HID VertX V1000 inputs and outputs cannot be used for the following purposes: • A door REX, door sensor, door lock • Elevator control or floor tracking • Interlock, including the override or lockdown functions • Readerless door • IO linking (Zone) • Door buzzer

Solution/ Unit	Issue	First reported in	Description
HID	57115	3.0 GA	Battery fail inputs: If the VertX V1000 Battery Fail input is used to monitor battery failure, then the Battery Fail inputs on all interface modules (V100, V200, V300) controlled by the V1000 must only be used for monitoring battery failure. Similarly, if the V1000 Battery Fail is used as a general purpose input, the Battery Fail interface modules must only be used for general purpose inputs.
HID	57114	3.0 GA	AC fail inputs: If the VertX V1000 AC Fail input is used to monitor AC, then the AC Fail inputs on all interface modules (V100, V200, V300) controlled by the V1000 must only be used for monitoring AC. Similarly, if the V1000 AC Fail is used as a general purpose input, the AC Fail interface modules must only be used for general purpose inputs.
HID	57113	3.0 GA	When a **Door unlock schedule override** is removed, there is a delay of 40 seconds before the door's unit is fully programmed.
HID	57112	3.0 GA	Unit discovery does not show the new name you give to a unit (in the unit, Identities tab) until the unit is rebooted or its power is cycled.
HID	56493	5.1 GA	HID VertX V1000: On the first attempt, Security Center might not be able to add a VertX V1000 unit (2.2.7.78). The first time you try to add a VertX V1000 (2.2.7.78) to Security Center, an error appears. Security Center will then reboot the unit. After the unit is rebooted, the second time you try to add the unit, Security Center is able to add the unit to the system.
Honeywell	355279	5.3 SR3	Honeywell access control panels are labeled as Mercury panels in Security Center.
Honeywell	57921	5.2 GA	The *Intrusion detection area input trouble* event does not report which input triggered the event.
Honeywell	57661	5.2 GA	The Galaxy Dimension control panel does not respond well to multiple input triggers that occur within one second of each other. As a result, you might lose your connection to Security Center. **Workaround:** Do not trigger more than one input at a time.
Honeywell	57517	5.2 GA	Clicking the buttons on the intrusion detection area widget might have no effect, depending on your control panel input configuration. For more information about configuring input functions, see the *Honeywell Galaxy Dimension Installer Manual*.
Honeywell	57492	5.2 GA	The Intrusion Manager role cannot report the *Entry delay started* control panel event.
Honeywell	57491	5.2 GA	When an expansion module is connected or disconnected from the Galaxy Dimension panel, you are not notified of the corresponding input and output states in Security Center.
Honeywell	57485	5.2 GA	Security Center does not support the Galaxy configuration "Re-ordering of the on-board RIO, SW3, dip-switch 8".
Honeywell	57484	5.2 GA	Offline logs are not supported.

Solution/ Unit	Issue	First reported in	Description
Honeywell	57040	5.2 GA	For some input functions such as "Final" and "Intruder", the Galaxy Dimension control panel does not send notifications to Security Center when the input state changes from "Normal" to "Active". Therefore, these inputs should not be used for virtual zones. Please note that not all inputs functions have been tested, there might be others that behave in the same manner.
Honeywell	56828	5.2 GA	Delay Arming (master or perimeter) is not supported.
Honeywell	56703	5.1 GA	When you create custom events for intrusion detection panels, the event list for many reports is not updated properly. **Workaround:** Delete the task and create a new task.
Honeywell	55922	5.2 GA	If an input is triggered from Security Center (from triggered intrusion alarm or the heartbeat monitoring feature), the input settings are overwritten with the values configured in Security Center. **Workaround:** Make sure the input configuration is the same in Security Center as on the control panel.
Intelbras	279341	5.3 SR1	Because of the long configuration time of the Intelbras HDCVI 1016 (5 minutes), the entity enters a "transmission loss" warning state when requesting video for the first time.
Intelbras	193064	5.2 SR7	VD 5016: Viewing multiple live streams in Security Desk does not work.
Interlogix	57661	5.2 GA	The Galaxy Dimension control panel does not respond well to multiple input triggers that occur within one second of each other. As a result, you might lose your connection to Security Center. **Workaround:** Don’t trigger more than one input at a time.
Interlogix	55922	5.2 GA	If an input is triggered from Security Center (from triggered intrusion alarm or the heartbeat monitoring feature), the input settings are overwritten with the values configured in Security Center. **Workaround:** Make sure the input configuration is the same in Security Center as on the control panel.
Intrusion	1040730	5.5 SR5_CU8	If a DMP or Honeywell intrusion detection unit is removed while the unit is online, it cannot be re-added. Instead, the *Unit enrollment* window displays the message *Already added*, even though the unit is no longer in Security Center. **Workaround:** Restart the Intrusion Manager role.
LPR	2157592	5.8 GA	When auto-discovery is enabled and the IP address of a SharpV changes, the new address is not automatically discovered by the LPR Manager role. **Workaround:** Edit the IP address field for the SharpV in Config Tool.

Solution/ Unit	Issue	First reported in	Description
LPR	2135795	5.8 GA	When the server hosting the LPR Manager role is behind a NAT, you can configure the public address of the NAT in Server Admin. However, there is no way to configure the port of the NAT associated to the LPM protocol port of the LPR Manager. **Workaround:** Configure the port of the LPM protocol on the *Properties* page of LPR Manager role such that it is the same as the port of the NAT. For example, if the port available on the NAT is *9876*, then you must configure the LPM protocol port on the role to also be listening to *9876*, and then configure your NAT accordingly.
LPR	2115810	5.8 GA	Specifying the legacy control port when adding a Sharp unit that supports the LPM protocol, forces the unit to connect with legacy connectivity.
LPR	2098714	5.8 GA	An offline duplicated unit is created when downgrading a unit from the LPM protocol to the Security Center extension (legacy).
LPR	1762978	5.8 GA	If a unit is moved from one role to another while the original role is down, that unit will not connect to the new role until the first role comes back online or the user presses the Reconnect button on the Sharp.
LPR	1756959	5.7 SR3	If you upgrade the Archiver server to Security Center 5.7 SR1, while the Directory and LPR Manager server is still at Security Center 5.7 GA, plate reads are no longer received from Sharp cameras.
LPR	1126908	5.7 GA	If you do not upgrade all Archiver databases before upgrading your LPR database, you might have to restart the Genetec™ Server service in order to be able to save images and data.
LPR	1050767	5.7 GA	When a user belongs to a partition that does not have access to the Archiver, but does have access to the LPR Manager, the LPR Manager displays the warning "No Archiver is currently selected", and the partitioned-off Archiver is not displayed.
LPR	958943	5.6 SR2	Parking Management: When an entrance read is incorrect and does not match the exit read, editing the entrance read to match the exit read will not complete the parking session. The session remains open until the maximum session time is reached.
LPR	900273	5.6 SR2	If a Sharp camera is deleted while the LPR Manager role is offline, the associated fusion stream information and protected data is not deleted with the Sharp camera. **Workaround:** Do not delete a Sharp camera while the LPR Manager role is offline.

Solution/ Unit	Issue	First reported in	Description
LPR	893909	5.6 SR2	The Report Manager role has a default timeout value of six minutes, which is problematic for LPR reports that take over six minutes to complete. **Workaround:** Change the timeout value of the Report Manger role: 1. Open the *GeneralSettings.gconfig* file in the configuration folder with a text editor. The default configuration folder is found under the Security Center installation folder (*C:\Program Files (x86)\Genetec Security Center 5.6\ConfigurationFiles*). 2. Increase the <*ReportGeneration Timeout="timeoutInMs"* /> value. For example, if you want a twenty minute timeout value, enter <*ReportGeneration Timeout="1200000"* />.
LPR	800458	5.6 SR1	You cannot assign a hotlist to multiple parking zones if they are managed by different LPR Manager roles.
LPR	795758	5.6 SR1	After moving a parking zone from one LPR Manager role to another, you cannot query old parking sessions and activities for the parking zone.
LPR	726177	5.6 SR1	The *Hotlist changed* event is not generated for hotlists that are only assigned to a Genetec Patroller™. The hotlist must be assigned to an LPR Manager role.
LPR	372523	5.4 GA	In the *Monitoring* task, when viewing in *map mode*, switching between maps clears the list of events.
LPR	372151	5.4 GA	In Security Desk's *Maps* task or in Config Tool's *Map designer*, if you unselect a layer that shows reads from a fixed Sharp camera, new reads are still displayed on the map. **Workaround:** To stop new reads from being displayed on the map, you can right-click the Sharp camera in the *Maps* task and select **Hide events**. Alternatively, you can block all license plate reads by selecting *Options* > *Events* and clearing the **License plate read** checkbox.
LPR	333734	5.4 GA	When a failover occurs, the LPR role does not reconnect with Fixed Sharps if the Sharps are configured with the "force connect" option.
LPR	276391	5.3 SR1	Hotlist Editor: You cannot search values in any date or time field.
LPR	258387	5.3 GA	MLPI: License plate reads that are saved as XML files by the *Genetec.LicensePlateManagement.MLPI.SmartDevice.exe* do not apply the same formatting as the *ReadTemplate.xml* in the Security Center installation package.
LPR	257122	5.3 GA	When the LPR Manager role comes back online after losing connection with Security Center, the Fixed Sharp immediately sends stored potential hits before the LPR role has had a chance to parse all associated hotlists. Therefore some hits might be missed.

Solution/ Unit	Issue	First reported in	Description
LPR	156794	4.0 SR1	Security Desk - The timestamp associated to a hit does not correspond to the time the hit was raised, but the time the patrolling officer took action on the hit (Accepted, Rejected, or Not enforced).
LPR	156793	4.0 GA	*Inventory management* task and *Inventory report* tasks in the Security Desk use a lot of memory. To avoid performance issues while running a query on a large parking facility inventory (40K places or more), it is recommended to delete all tasks unrelated to MLPI from your task list before launching the query.
LPR	156792	4.0 GA	AutoVu™ LPR: While parsing hotlist or permit data files, parsing errors such as the use of wrong delimiter characters, are not indicated.
LPR	94758	5.2 LA	MLPI: The local time on the handheld computer is not synchronized with the server, which might cause issues. For example, if the LPR Manager receives an XML read to be imported, but the read has a future timestamp, the read is ignored.
Maps	933287	5.6 SR2	Backward compatibility: When a Security Desk client machine is running Security Center 5.5 but is connected to a 5.6 server, you cannot view an Esri map in a tile.
Moxa	219200	5.4 SR2	When the Moxa Vport 36 camera is configured for multicast streaming, the camera might lose the connection with Security Center if the stream is started and stopped many times.
Panasonic	2237020	5.8.1.0	Panasonic units: Not all the color settings on the web page of the unit are available on the *Color* page of the unit in Security Center.
Panasonic	1747544	5.7 SR3	Panasonic WV-X4171: When the capture mode of the camera is set to Fisheye + Quad PTZ, in Security Desk, if you use the zoom in the PTZ widget the tile does not enter the dewarp mode. **Workaround:** In the Camera widget, click **Toggle digital zoom** before using the zoom in the PTZ widget.
Panasonic	985438	5.6 SR4	Panasonic WV-V2530 and V-series: Streaming video in RTSP over HTTP in H.264 or MJPEG format does not work.
Panasonic	240890	5.2 SR10	The Panasonic WV-SNF310J does not support peripherals, such as audio and I/O, whereas the WV-SNF310 does. When WV-SNF310J is added to Security Center, the peripherals are present, but they do not function.
Panasonic	177466	5.3 LA	The **Sensitivity** option for motion detection is not supported for Panasonic cameras.
Panasonic	157051	5.2 SR6	Panasonic WV-SFV631L: The resolution values for JPEG streams that are available in Config Tool are limited to the values that are set in the unit's web page.
Panasonic	154965	5.2 SR2	Panasonic units do not support the MJPEG format for video trickling.

Solution/ Unit	Issue	First reported in	Description
Panasonic	147206		Panasonic WV-SC588: Playback video that was recorded on the unit's Security Desk card cannot be retrieved in Security Center. **Workaround:** Record video on the Archiver; do not use edge recording.
Panasonic	103777	5.2 SR1	Panasonic units do not support edge playback requests or trickling for MJPEG video.
Panasonic	103519	5.2 SR1	WV-SP306: Audio output is not in sync with the video. **Workaround:** Workaround: Perform a factory reset on the unit's web page, reassign the IP address of the unit, then add the unit again in Config Tool.
Pelco	973871	5.7 GA	After changing video quality settings on ES532L or ES5350 units, you receive *transmission lost* messages and live video stream requests.
Pelco	541386	5.4 SR3	IMM12027: Panorama images are distorted when a fast moving object covers all four cameras at the same time. **Workaround:** Clear the "Camera 1" monitoring tile and start a new monitoring session in the same tile.
Pelco	240102	5.3 LA	The "Max zoom factor" is limited to 200 in Config Tool even though the camera can support higher values. **Workaround:** Click 'Calibrate' to obtain a higher zoom factor. The value will be displayed in red in Config Tool because it exceeds 200, however you will be able to zoom to that value.
Pelco	219337	5.2 SR9	Pelco: Disconnecting a camera from the Pelco NET5504 encoder will not trigger 'Signal lost' events.
Pelco	107622	5.2 SR1	Pelco Sarix Spectra HD D5220: The **Auto Iris** command in the Specific commands of the Security Desk PTZ widget does not change the brightness.
Pelco	107449	5.2 SR1	Sarix Spectra HD D5220: Setting the Frame rate to 1fps on the Video tab causes intermittent image loss.
Pelco	88072	5.2 LA	When you add Pelco cameras or change their configuration in Security Center, you might receive a Transmission lost warning while the configuration is pushed to the camera.
Pelco	40540	5.0 GA	Pelco TXB-N: Key frame interval not applied when Archiver Video Quality is set to Custom.
Samsung	1730724		SRTP over Multicast and SRTP with RTSP over HTTPS connection types are not supported for Hanwha SRTP-ready devices.
Samsung	1004844	5.6 SR4	Samsung SRM-872: When playing back video sequences from two different cameras, the footage from one of the cameras will jump to match the time of the other camera.
Samsung	982885	5.6 SR4	Samsung SRM-872: When daylight savings time is enabled on the unit, video sequences that are played back from the *Archives* task, start one hour in advance of the **Start time**.

Solution/ Unit	Issue	First reported in	Description
Samsung	771640	5.6 SR4	SRM-872: PTZ control does not work for camera connected to the SRM-872 network video recorder.
Samsung	744585	5.5 SR4	Samsung SNO-8081R: The unit cannot stream video at 60 FPS in Security Center if the **SSDR** option is **ON** in the unit web page.
Samsung	744528	5.5 SR4	SNO-808IR: The video stream pixelates and freezes when the resolution is set to 2592 x1464 or 2592 x 1944.
Samsung	744231	5.5 SR4	SNO-818IR: If you are using **Multicast** as the **Connection type** for the microphone, audio does not work. **Workaround:** Make sure that multicast for audio is enabled on the unit web page for the *Mobile* profile.
Samsung	573927	5.5 SR2	Samsung: Cycling through Samsung Wisenet lite series cameras in the Monitoring task causes cameras to fail.
Samsung	555772	5.6 SR4	SRM-872: In Config Tool, configuring the **Output relay settings** on the **Peripherals** tab of the unit has no effect.
Samsung	508634	5.5 SR4	Samsung SRM-872: You can only view a maximum two edge playback video streams simultaneously.
Samsung	507334	5.5 SR2	Samsung: Performing an Archive transfer sometimes fails unexpectedly.
Samsung	505978	5.6 GA	SRM-872: Audio out is not supported.
Samsung	392516	5.4 SR2	You cannot configure the alarm input on Samsung SNP-5200 cameras. Events generated from the camera input are not reflected in Security Center.
Samsung	280529	5.3 SR1	Sometimes Samsung SNP-6201 goes offline when changing connection type.
Samsung	277890	5.3 SR1	Samsung SNP-3120P: Unit motion detection sensitivity and zone parameters cannot be configured by Config Tool.
Samsung	269752		When configuring multiple motion detection zones, only the first one supports threshold values.
Samsung	262539	5.1 SR3	Video streaming is not available on models SNB-7000 when configured at 3 megapixel MJPEG.
Samsung	154180	5.2 SR6	Samsung SNP-3750: The "Clear preset" PTZ command is not supported. **Workaround:** Clear the PTZ presets from the unit's web page.
Samsung	147987	5.2 SR5	SNP-6200H: Audio output is choppy, even when the volume is set to the maximum in the unit’s web page.
Sanyo	154970	5.2 SR3	VDC-DP7584: The aspect ratio is not correct for streams that have a resolution of 720x240.

Solution/ Unit	Issue	First reported in	Description
Sentry 360	60841	5.1 GA	When using the dewarping feature in Security Desk, the overview image displays the first frame when the camera was dropped in the tile.
Sentry 360	60840	5.1 GA	When using the dewarping feature in Security Desk, the overview image does not match the zoom regions.
Sentry 360	60839	5.1 GA	When using the dewarping feature in Security Desk, if you zoom using your mouse wheel button, it zooms to the center of the image, not where your mouse is pointing.
Sipelia™	2162083	5.8 GA	Map features in Sipelia™ 2.8 GA and earlier do not work in Security Center 5.8 GA. **Workaround:** If you upgrade to Security Center 5.8 GA, you must upgrade Sipelia™ to version 2.8 SR1 to use its map features, such as making and answering calls from maps.
Siqura	154951	5.2 SR1	C-60E: The Motion on threshold is not supported on the unit. Therefore, you might receive motion on events from values that differ from the motion blocks you specified.
Sony	1018905	5.6 SR4	When the **Matching decision** filters in the **VMF settings** are configured on the cameras web page, either no event, or the wrong event is triggered in Security Center.
Sony	526578	5.5 GA	Sony: When using the RM-NS1000, the Pause button does not work in Live mode. **Workaround:** Run Security Desk in 32-bit. To do this, navigate to *C:\Program Files (x86)\Genetec Security Center 5.5\SecurityDesk32.exe.*
Sony	352466	5.4 GA	Gen 5 PTZ cameras: When recording on the edge, the cameras can become unresponsive and sometimes spin uncontrollably.
Sony	347660	5.3 SR2	Sony SMC-VM77R2: When you add or modify a VMF **Filter type** on the unit's web page, you need to reconnect to the unit in Security Center to see the events in Security Desk.
Sony	328076	5.3 SR2	Sony SMC-VM77R2: When using the 4K 30p resolution, hardware motion detection, camera tampering, and face detection are not supported.
Sony	237097	5.2 SR10	Motion detection on the Sony SNC-DH280 does not work on the MPEG-4 stream; this stream is too noisy. Instead, the user must use the H.264 stream or perform hardware motion detection.
Sony	196874	5.3 LA	Sony SNC-VB600B: Edge playback starts buffering when you fast forward faster than 4x or rewind faster than -4x.
Sony	156119	5.2 SR6	Sony SNC-HM662, firmware 1.1.0: AAC audio input on H.264 streams only emits low frequency sounds.
Sony	154968	5.2 SR3	Sony 5th Generation: For certain units only one codec can be on for motion detection to work, the others must be turned off.

Solution/ Unit	Issue	First reported in	Description
Sony	154967	5.2 SR3	Sony 5th and 6th Generation: When performing hardware motion detection with multiple zones, the **Motion on threshold** setting for the first zone is used for all zones.
Sony	154425	5.2 SR6	Sony SNC-HM662: When you dewarp the camera image using a digital zoom preset, the image is dewarped differently in *Monitoring* task versus the *Archives* task.
Sony	119575	5.2 SR3	Sony: Changing codecs on a 6th generation camera while it is actively streaming causes an error and transmission is lost. **Workaround:** Stop all streams and then configure the codecs.
Sony	106638	5.2 SR1	SNT EX-154: No motion detection events are received in Security Center if the unit's web page has the *Motion detection* tab open.
Sony	104672	5.2 SR1	SNC-ER585: When moving the mouse pointer over a tile that is being used to monitor live video in Security Desk, the image freezes.
Sony	74587	5.1 SR2	Sony 5th generation video units: The resolution of the second stream cannot be higher than the resolution of the first stream.
Speco	343664	5.3 SR3	Speco 02B5: Unit motion detection events are not displayed.
Speco	343644	5.3 SR3	Speco 02B5: Input pin state changes are not detected and Alarm in events are not displayed.
Synergis™ appliance	210748	5.3 LA	After installing a new system, you might see messages in the Access Manager log saying that the Access Manager could not connect to a Synergis™ appliance, even if you did not try to enroll a Synergis™ appliance. This is because Security Center attempts to automatically enroll Synergis™ appliances that were discovered on the port.
Synergis™ appliance	206282	5.3 LA	If you connect to the Synergis™ Appliance Portal from the **Portal** tab of the Synergis™ appliance unit in Config Tool, and you select another access control unit in the area view, your web session is lost.
Synergis™ IX	1959846	5.8 GA	When using Synergis™ IX, you can assign an intrusion area's secured area to any access control area. This leads to being able to assign an entering or exiting intrusion area on a door that is not controlled by ICT hardware.
Verint	91773	5.2 LA	Verint S1801E-R: You cannot toggle between single and quad monitor mode in Config Tool. **Workaround:** Change the monitor mode from the unit's web page.
Video	2250588	5.8.1.0	ONVIF cameras: When sending PTZ auxiliary commands from a 5.7 client to a camera on a 5.8 Archiver, the wrong commands are sent. **Workaround:** Upgrade the clients to 5.8.

Solution/ Unit	Issue	First reported in	Description
Video	2226885	5.8.1.0	When playing back from edge with many high resolution cameras at the same time, the unit playback cache of the Archiver might exceed the configured 2GB value and consume too much disk space.
Video	2216291	5.8.1.0	When an Archiver with multiple agents is in warning, in the *System status* report, all servers for that Archiver are shown in warning, even though only one of the agents is affected.
Video	2138528	5.8 GA	The Auxiliary Archiver role does not support an Azure SQL Database.
Video	2101810	5.8 GA	When an earlier system federates with Security Center 5.8, users see a generic error message when trying to view a camera that is encrypted in transit from Archiver.
Video	2101544	5.8 GA	It is possible to set an Archiver running in backward compatibility mode to encrypt **In transit from Archiver**, but the option has no effect.
Video	2055790		When an earlier system federates with Security Center 5.8, or an earlier client connects to Security Center, 5.8 users see a generic error message when trying to view a camera that is encrypted in transit from Archiver.
Video	2045458	5.7 SR5	Sony SNC-HMX70 and Bosch cameras with a built-in fisheye lens: On the web page of the unit, changing the application variant from **Normal** to **Dewarp** might cause the streams of that unit in Config Tool to disappear and reappear continuously or remain offline. **Workaround:** Delete the video unit from Config Tool before modifying the application variant on the web page of the unit, then re-add the unit.
Video	2020516	5.8 GA	Using Boost Quality when Privacy Protection is enabled can force the camera into a learning phase where everything is privacy protected.
Video	1963368	5.8 GA	When **Scramble entity names** is enabled for a user, real camera names are still visible to that user in the stream status for playback video. **Workaround:** Remove the *View video stream status* privilege from users that see scrambled entity names.
Video	1961781	5.8 GA	Several storage entities are visible in the Archiver statistics when an LPR role is linked to an Archiver.
Video	1925596	5.7 SR4	If you add a microphone to a camera, the microphone is not included in the cache until the token expires.
Video	1922952	5.8 GA	After changing the configuration of the Camera Integrity Monitor role, camera integrity monitoring only starts at the next camera check interval.
Video	1919141	5.8 GA	After defining Privacy Protection Exclusion Zones for a camera, the zones fail to adapt to the new field of view when rotating the video from that camera.

Solution/ Unit	Issue	First reported in	Description
Video	1915782	5.8 GA	The Archiver statistics report shows information for the entire system and is not limited by privilege or partition.
Video	1904826	5.7 SR5	Live SRTP video freezes on the primary Archiver server when the secondary Archiver server is performing redundant archiving. **Workaround:** Do not activate redundant archiving, or use unicast UDP instead of multicast.
Video	1903768	5.8 GA	Unable to view camera streams that are encrypted in transit when connecting an earlier version of Security Desk to a 5.8 Directory.
Video	1796269	5.8 GA	When a camera is added to an Archiver that is set to encrypt in transit, live streams from that camera are not encrypted when privacy protection is enabled.
Video	1757030	5.8 GA	MP4 video exported from a Bosch VIP X1600 does not play well in VLC media player. **Workaround:** Use another media player.
Video	1706499	5.7 SR2	In the Security Desk *Monitoring* task, when privacy protection is enabled and you use the PTZ controls, the whole video becomes blur for over twenty seconds and the PTZ controls might stop working. **Workaround:** Disable privacy protection.
Video	1700823	5.7 SR2	In the *Monitoring* task, if a tile displays the message *Insufficient security information*, and then you install the encryption certificate on the client machine, you must manually add or remove the camera from the tile to refresh the stream.
Video	1700125	5.7 SR2	Privacy protection: On the camera's *Privacy protection* page, under *Advanced settings*, the **Startup learning period** that you set might not match how long is actually spent analyzing the video to learn the background. For example, if you set the option to 60 seconds, the **Startup learning period** might take less time to complete. **Workaround:** Increase the value of the **Startup learning period** to compensate for the discrepancy.
Video	1582418	5.7 SR4	In the *Live video* window of a PTZ camera in the Config Tool *Video* task, the coordinates you entered for the **Move absolute** option are not respected.
Video	1563930	5.7 SR2	If you modify the video rotation of a camera encoding in wavelet in Config Tool, an error is displayed when you try to view the video stream in Security Center.
Video	1478882	5.7 SR2	When the conversion of video from a Body-Worn Camera (BWC) is in progress, launching a query from the Security Desk *Archives* task does not return up-to-date results.
Video	1475877	5.7 SR2	When video resolution is set to 4K, configuring the camera's image rotation in Config Tool or generating a thumbnail in Security Desk causes an increase in CPU usage.

Solution/ Unit	Issue	First reported in	Description
Video	1244216	5.7 SR1	If you disable the Privacy Protection feature, you cannot view any of the original non-blurred video. If you then re-enable Privacy Protection, the original non-blurred video is available.
Video	1165630	5.7 GA	If the Archiver restarts while a camera that has edge recording is being blocked and an operator is monitoring the camera, the camera might be shown as unblocked until the tile is reloaded in the Security Desk *Monitoring* task.
Video	1163477	5.7 GA	If you block operation while an Archiver is in a *Database lost* event, it can result in unblocked sequences for lower level users.
Video	1126582	5.7 SR1	If the Privacy Protection license has been exceeded the video tile displays a message indicating that there are not enough licenses. If you then remove Privacy Protection, the original video stream is not displayed.
Video	1112282	5.7 GA	After updating to Security Center 5.7 GA, the multicast addresses of your cameras might change.
Video	1104038	5.7 GA	When performing short archive transfers with encryption between Archiver roles, for example at every minute, you might not be able to view the full video being transferred because of missing encryption key information.
Video	1052298	5.7 GA	If you have roles installed on multiple machines and you change the RTSP port of the Media Router, an exception is logged in the Event Viewer.
Video	1050756	5.7 GA	If an Archiver goes offline while you are viewing playback video and then you switch to viewing live video during the downtime, live caching might not work once the Archiver comes back online.
Video	1046280	5.7 SR2	After transferring video from a BWC to Security Center, small gaps might be displayed on the video timeline, even though no video is missing.
Video	1042164	5.7 GA	If the redirector is using a port for RTP, but that port is already in use, the redirector is unable to connect to the port properly and you receive a *Stream unavailable* error message when trying to view live video.
Video	1037719	5.7 GA	If you add a bookmark to a camera that contains only edge recordings, you are able to select **Protect video from deletion** and select a retention period even though edge recordings cannot be protected from deletion. No warning is issued.
Video	1029605	5.7 GA	When performing a diagnosis on a unit that is offline, you receive the error messages *Ping failed* and *Authentication scheme rejected from agent*, even if basic authentication is used for this unit.
Video	1029576	5.7 SR1	When a camera that is configured to be encrypted uses Privacy Protection, the original stream is encrypted but the privacy protected stream (the blurred one) is not encrypted.

Solution/ Unit	Issue	First reported in	Description
Video	1019840	5.7 GA	If a recording problem occurs while a camera is in Maintenance mode, after you disable Maintenance mode the camera is not shown in yellow and no longer indicates there is a problem.
Video	999439	5.6 SR4	If you try to add a camera shortly after removing it, an *Already added* event is triggered, and the camera cannot be added.
Video	942703	5.7 SR2	Video from BWCs is archived according to the retention period configured on the Archiver that the video is stored on. If you change the Archiver assigned to the camera's User, the retention period does not change for the video stored on the original Archiver, even though the **Inherit from Archiver** setting is selected.
Video	900815	5.7 GA	If a camera has edge recording and this camera is being blocked, an operator is still able to view video footage by selecting the specific playback source from the camera.
Video	888189	5.6 GA	Security Desk: The **Select playback source** option in the tile menu commands does not always display all the playback sources for a camera. **Workaround:** Select **All sources** to see the full list of playback sources.
Video	796783	5.6 GA	If an Auxiliary Archiver is recording a video stream that is being redirected from a remote site that has a maximum bandwidth limit set, and the bandwidth limit has been reached, the video stream is lost but the recorded video file is not closed right away. As a result, there might be gaps in the timeline of the video file.
Video	771688	5.6 GA	If you are duplicating video files on another Archiver using archive transfer and the transfer progress is slow due to limited bandwidth, you are not notified.
Video	737510	5.5 SR4	ONVIF cameras: The *Best available* connection type is not supported for ONVIF cameras, but the option is still available if you add the unit using the Unit enrollment tool.
Video	697952	5.6 GA	If the PTZ protocol of a camera does not support absolute pan or tilt positions, then if a failover occurs on the Map Manager role, the FOV of the PTZ camera might not show the correct orientation on the map, and moving the FOV might not move the PTZ motor.
Video	600655		Digital PTZ presets created in the current version may not be available in older Security Desk versions.
Video	499286	5.5 GA	When exporting a video that is recorded from multiple sources, audio or metadata can be missing from the export.
Video	486339	5.4 SR2	For systems that include Axis and Panasonic cameras that support sensitivity by zone and that are configured to perform motion detection on the unit, upgrading Security Center from a version earlier than 5.3 LA (including Omnicast™) to any version higher or equal to 5.3 LA will reset each of the camera's motion zones sensitivity to 99%.

Solution/ Unit	Issue	First reported in	Description
Video	387302	5.4 GA	After changing the start multicast address of the Media Router, the camera multicast address is not updated. **Workaround:** Manually update the multicast address in Config Tool.
Video	352715	5.4 GA	Live and playback video stop working when the Archiver memory reaches 1.2 GB. **Workaround:** Install Microsoft KB 2588507 to fix the issue.
Video	349497	5.3 SR2	Export: If a camera is associated to both an Archiver and an Auxiliary Archiver, and configured to record audio on one and not the other, audio might not be included in the exported file. **Workaround:** Make sure to perform the export from the source camera that is configured to record audio.
Video	263498	5.3 GA	Security Desk: When you drag a report result into a Monitoring task tile, only the live feed is played. If the report result has only playback video, the tile waits for an offline source to play live video feed instead.
Video	263438	5.3 GA	Security Desk: When you drag and drop a G64 video file on a tile that previously had a camera with fisheye lens configuration, the digital zoom displays a fisheye zoom instead of a normal digital zoom.
Video	263320	5.3 GA	Security Desk: Paused G64 video automatically resumes and loses digital zoom when you switch between *Monitoring* tasks. This behavior is also seen when dragging and dropping paused tiles between screens running Security Desk in full screen mode.
Video	261764	5.3 GA	The Change title pattern pop-up is not near the **Change tile pattern** button when you use the hotkey shortcut (Ctrl+p).
Video	261744	5.3 GA	Vault: Encrypted files with extension .gek always display a length of 23:59:59.
Video	257289	5.3 GA	The Genetec™ Video Player is displaying an error when it starts, sometimes showing a .NET Framework initialization Error message. **Workaround:** Delete the following folder: *C:\Users\username\AppData\Roaming\Thinstall\Genetec Video Player 5.3 GA.*
Video	256524	5.3 GA	When playing back video in the Monitoring task, the time zone for a camera does not always display correctly.
Video	254643	5.3 GA	Archive transfer: When transferring archives to a newly created Archiver, if the transfer is interrupted, the status might indicate that the transfer was completed even though it never restarted after the interruption.

Solution/ Unit	Issue	First reported in	Description
Video	217745	5.2 SR9	ONVIF cameras: Fixed cameras are sometimes discovered as PTZ cameras. **Workaround:** Use one of the following options: • Leave it as is, with limited Digital PTZ due to usage of on-board controls. • Add the unit with Manufacturer= "ONVIF" and Product type= "Without PTZ".
Video	215485	5.3 LA	Bookmarks might disappear from the timeline when clicking the **Previous bookmark** button.
Video	211625	5.3 LA	Hardware acceleration: On high performance computers, NVIDIA GPU decoding works better when Intel Quick Sync is disabled.
Video	211232	5.3 LA	Hardware acceleration: If you install a new NVIDIA driver when hardware acceleration is enabled in Security Desk and you are monitoring a camera using an NVIDIA encoder, then your Windows screen turns blue and cannot be restarted. **Workaround:** Recover your Windows system.
Video	210012	5.3 LA	Security Desk: The **Stop recording** button for PTZ patterns does not appear if recording is started using a keyboard shortcut.
Video	208788	5.2 SR9	Changing the connection type might trigger a transmission lost event in Security Center before the video can be seen again from the camera.
Video	205161	5.3 LA	If you are viewing multiple cameras in synchronized playback using the Remote task and you start seeking in the timeline, the timestamps and timelines on the local Security Desk do not update properly.
Video	204681		The camera configuration report task does not work with Omnicast™ federated cameras.
Video	192595	5.3 GA	Hardware acceleration: GPU always shows 0% even though the usage ratio is unavailable when using QuickSync.
Video	155581	5.2 SR5	If you are federating an Omnicast™ system and the user that the Federation™ role uses to log on to the remote system lacks the privilege to view playback video, Security Center users can still view playback video from the federated Omnicast™ cameras.
Video	153240	5.2 SR5	When exporting federated video from an Omnicast™ 4.7 system, the progress bar does not show the progress.
Video	153236	5.0 LA	All cameras in a federated camera sequence are displayed on the Federation™ host even though the user account used to connect to the federated Directory does not have access to all of them.
Video	153232	5.0 LA	Federated camera sequences cannot show video from cameras that are blocked to any user on the remote system, regardless of the privileges of the user account used to connect to the federated Directory.

Solution/ Unit	Issue	First reported in	Description
Video	148655	5.2 SR5	When federating a Security Center system with a user that has an **Archive viewing limitation** of 5 minutes, the *Archives* report in Security Desk only displays results for the last 5 minutes, but more than the last 5 minutes of video can be viewed.
Video	148030	5.2 SR5	If the **Archive viewing limitation** option for a user is changed to a specific value in Config Tool, and then they try to view playback video in the canvas, the video thumbnails span the whole tile, even if they cannot view the associated video.
Video	143478	5.2 SR4	SQL 2012: Database creation issues when installing SQL 2012. **Workaround:** Check the SQL permissions and make sure the NTAuthority\SYSTEM user is set to sysadmin.
Video	129622	5.2 SR6	PTZ motors must be connected to a serial port on the same Archiver as the camera.
Video	100778	5.2 GA	When you add a bookmark to live video of a federated Omnicast™ 4.7 camera, the bookmark timestamp is generated when you click **OK**, not when you click **Add bookmark**.
Video	100768	5.2 GA	For federated Omnicast™ cameras, the video tile statistics overlay does not display the **Encoding type**, and the **Source field** is incorrect.
Video	97038	5.2 SR4	When federating a PTZ camera from an Omnicast™ 4.8 system to Security Center, the PTZ preset names might not be federated.
Video	94722	5.2 LA	In Omnicast™, you can only block live video. Therefore, if you are viewing playback video from a federated Omnicast™ video stream in Security Center and it is blocked by a user on the Omnicast™ side, the video is not blocked in Security Center until the camera is changed to live video mode.
Video	91564	5.2 LA	Software motion detection is not supported on Auxiliary Archivers. Therefore, when viewing playback video, there is no visual indication of motion on the timeline if the video archive was only recorded on an Auxiliary Archiver (no green bars).
Video	88994	5.2 GA	If you switch the audio format to AAC audio while the video stream is displayed in a Security Desk tile, the sound is either distorted or doesn't work. **Workaround:** Clear the video stream from the tile before changing the audio format. Then, in the camera widget, click the **Listen** button twice to reset the audio.
Video	88764	5.2 LA	When using digital zoom, you cannot select a preset again if it was the last preset you selected before moving the camera image. **Workaround:** In the **Digital zoom presets** section of the camera widget, click **Reload** to move the camera image to the current preset position.
Video	78880	5.1 SR2	Security Desk: When playing back Omnicast™ 4.8 federated video, the rewind speed starts at -10x instead of -1x.

Solution/ Unit	Issue	First reported in	Description
Video	77721	5.1 SR2	Edge playback: Audio playback is not supported on edge recording unit.
Video	76946	5.1 SR1	Motion detection: On high resolution cameras, Config Tool does not display as many motion blocks as the Archiver can detect.
Video	70560	5.2 LA	If you associate a camera with an alarm and the analog monitor that is a recipient of the alarm does not support the camera, when the alarm is triggered, the video is not displayed on the analog monitor.
Video	70532	5.2 LA	When you add a camera sequence to an analog monitor in Security Desk and one of the cameras is not supported, that camera is skipped in the sequence.
Video	64274	5.1 SR2	Edge recording: Thumbnails are not available if the video is only recorded on the edge unit. **Workaround:** To see thumbnails in any kind of video reports (Bookmarks, Camera events, and so on), the video must be trickled to the Archiver.
Video	54437	5.0 SR1	When displaying an HTML map in a bottom tile, and switching a camera in another tile to playback mode, the map overlaps the video thumbnails.
Video	52172	5.1 GA	When attempting to back up an Auxiliary Archiver that is installed on an expansion server to a file on that computer, you might receive an error because the SQL Server might not have permission to back up to that location. **Workaround:** Back up to a folder the SQL Server has access to.
Video	40314	5.0 GA	Alarm playback loop is permanently set in Security Desk. The alarm playback loop is set between the following time ranges: • Start time: Alarm trigger minus pre-trigger setting. • End time: Alarm trigger plus 10 seconds.
VideoIQ	154958	5.2 SR1	If you boost the video quality or modify the video stream (for example, change the frame rate) in Config Tool, you might lose the video stream connection for 30 seconds.
Vivotek	368949	5.4 GA	Vivotek IP9171-HP : You cannot view playback video that was recorded on the edge. **Workaround:** View the playback from the unit's web page.
Vivotek	365649	5.4 GA	FD9371-EHTV, IP9171, IP9171-HP: When performing a factory reset, the Vivotek Application Development Platform required for the Genetec™ Protocol might be accidentally deleted. **Workaround:** Reinstall the Vivotek Application Development Platform with firmware 1.0.1.4 or later.
Vivotek	287549	5.3 SR2	Vivotek IB8381: When querying the of list of video sequences on the unit's SD card, the UTC start and end times are incorrect.

Solution/ Unit	Issue	First reported in	Description
Web Client	1002566	5.7 SR5	You cannot trigger federated alarms, even if you have the *Trigger alarm* privilege.
Web Client	998171	5.7 GA	Removing a feature from Config Tool does not remove it from Web Client.
Web Client	793868	5.6 GA	You cannot view video from federated Omnicast™ 4.x cameras in Web Client.
Web Client	750609	5.6 GA	After you drag a camera to a canvas tile, the timeline is not displayed until you move your mouse outside of the tile, and then hover your mouse back over the tile.

Security Center 5.8 system requirements

System requirements are the recommended hardware and software components that are required for your product and system to run optimally.

For the latest Security Center 5.8 system requirements, refer to the *Security Center System Requirements Guide*.

In order to determine which configuration is best suited for your application, contact our Sales Engineering team at salesengineering@genetec.com.

Supported video units in Security Center 5.8.1.0

Security Center 5.8.1.0 supports many video units.

For details such as firmware and certification level of the video units supported by Security Center, see our Supported Device List.

NOTE: Some of the supported video units require additional configuration before they can be added in Security Center, or for their unit features to work in Security Center. For more information about these configuration steps, see the *Security Center Video Unit Configuration Guide*. The latest version of this document is available on the Genetec™ TechDoc Hub.

Supported HID hardware in Security Center 5.8.1.0

Security Center 5.8.1.0 supports HID VertX and Edge product lines. It also supports the old (Legacy) and new (EVO) product generations.

Supported HID controller firmware in Security Center 5.8.1.0

We recommend a specific firmware version for each generation of HID controllers, old (Legacy) and new (EVO). Using earlier firmware versions might cause issues with your system.

Security Center works best when the HID controllers are running the recommended certified firmware versions.

Supported firmware	Legacy controllers	EVO controllers
Recommended certified firmware	2.2.7.568	3.8.0[1]
Minimum supported firmware	2.2.7.568	3.5.x

[1]As of Security Center 5.8, HID units running firmware version 3.7.0.108 or later in secure mode communicate with the Access Manager using TLS 1.2 encryption over TCP port 4433. HID units running an earlier firmware version or in regular mode communicate with the Access Manager using HID encryption.

For more information about port changes, see "Ports used by Synergis™ applications" in the *Security Center Administrator Guide*.

Previously supported firmware versions

To learn about the issues with the previously supported firmware versions, see *Limitations in Security Center*.

Upgrading HID EVO firmware

Specific upgrade paths must be followed to upgrade the following HID EVO units from the firmware versions indicated to the recommended firmware version:

- Edge EVO: 2.3.1.603 or 2.3.1.605
- VertXEVO: 2.3.1.542 or 2.3.1.673

For the upgrade procedure, see the *Security Center Administrator Guide*.

Supported interface modules for VertX controllers in Security Center 5.8.1.0

Security Center 5.8.1.0 supports the following interface modules with the HID controllers.

BEST PRACTICE: Install the following Program and EEPROM firmware on the interface modules.

HID interface unit	Program	EEPROM
VertX V100 (V2000 has a V100 board built-in) EdgePlus/EdgeReader	113	110

HID interface unit	Program	EEPROM
VertX V200	106	105
VertX V300	107	104

Supported badge printers in Security Center 5.8.1.0

Security Center uses Windows printer drivers and is therefore compatible with printers that are supported by the Windows operating system. If you purchase a badge printer from Genetec Inc., additional support is provided.

Additional support is offered for the following badge printers purchased from Genetec Inc.:

Manufacturer	Model
HID FARGO	DTC1250e
	DTC4500e
	HDP5000
	HDP8500

Supported Honeywell Galaxy intrusion detection devices in Security Center

Security Center supports specific Honeywell Galaxy Dimension intrusion detection devices.

For each device, the corresponding firmware and certification level is listed.

Model	Device type	Firmware	Certification
A234	RS-232 Lead Kit		Certified
C072	Rio Expander module		Certified
CP037	Keypad		Certified
E080-2	Galaxy Ethernet Module	version 2.11	Certified
E080-4	Galaxy Ethernet Module	version 3.02	Certified
GD-48	Intrusion panel	version 6.7	Certified
GD-96	Intrusion panel	version 6.7	Supported by design
GD-264	Intrusion panel	version 6.7	Supported by design
GD-520	Intrusion panel	version 6.7	Certified
Flex-100	Intrusion panel	version 3.37	Certified

Supported DMP intrusion detection devices in Security Center

Security Center supports specific DMP intrusion detection devices.

For each device, the corresponding firmware and certification level is listed.

Model	Device type	Firmware	Certification
XR500N	Intrusion panel	version 212	Certified
XR500E	Intrusion panel	version 212	Certified
XR100N	Intrusion panel	version 212	Supported by design
XR150DN	Intrusion panel	version 171	Certified
XR550DN	Intrusion panel	version 171	Certified

NOTE:

- Certified panels support arming and disarming an Area System. The following options are not certified with this integration:
  - ALL/PERIMETER
  - HOME/SLEEP/AWAY
  - HOME/SLEEP/AWAY WITH GUEST
- XR550DN panels support four profiles per user. Currently, only the first profile is supported by Security Center.

Supported upgrade paths to Security Center 5.8.1.0

Security Center supports direct upgrades and two-step upgrades to the latest software version. When upgrading, it is important to know your required upgrade path.

Direct upgrades

A direct upgrade to Security Center 5.8.1.0 is supported from the following software versions:

- Security Center 5.8 GA
- Security Center 5.7 GA and all SRs
- Security Center 5.6 GA and all SRs
- Security Center 5.5 GA and all SRs

Two-step upgrades

A two-step upgrade to Security Center 5.8.1.0 is supported from the following software versions:

- Security Center 5.4 GA and all SRs
- Security Center 5.3 GA and all SRs
- Security Center 5.2 GA and all SRs

To maintain backward compatibility during a two-step upgrade, supported systems are first upgraded to Security Center 5.5 SR5 and then directly upgraded to Security Center 5.8.1.0.

Older version upgrades

To upgrade Security Center 5.1 and earlier, contact your representative of Genetec Inc..

Supported Omnicast™ migrations in Security Center 5.8.1.0

To upgrade an Omnicast™ system to Security Center 5.8.1.0, use the 5.5 Omnicast™ Migration tool.

For more information, see the Omnicast™ Migration Guide 5.5.

Security Center 5.8.1.0 compatibility

Product compatibility indicates that the product can support and run with specific versions of other products.

Security Center 5.8.1.0 is compatible with the following:

NOTE: Product release versions listed include all subsequent service releases and hotfixes, unless otherwise specified.

Product	Compatible versions
ALPR (AutoVu™)	
Genetec Patroller™	6.3, 6.4, 6.5
SharpOS	10.2, 11.4, 11.5, 11.6, 11.7, 12.4, 12.5, 12.6, 12.7, 12.8
Sharp hardware	Sharp 2.0, Sharp 3.0, SharpX, SharpXS, Sharp XSU, SharpV, SharpV ITS
Access control (Synergis™)	
Synergis™ Softwire[a]	10.7, 10.8, 10.9, 10.10
Security Center modules	
Sipelia™	2.8 SR1
Mobile access	
Genetec™ Mobile app	5.0.0 and later
Genetec Mission Control™	
Genetec Mission Control™	2.12.0

[a] For a list of supported interface modules and unit firmware, see the *Synergis™ Softwire Release Notes* and *Synergis™ Master Controller Release Notes*, which are available on the Genetec™ TechDoc Hub.

Backward compatibility requirements for Security Center

Security Center 5.8.1.0 is backward compatible with many Security Center components from the three previous major versions.

IMPORTANT: Security Center 5.8 is backward compatible with the three previous *major versions*. A server or workstation that is three major versions behind can connect to the 5.8 Directory, but one that is four major versions behind cannot. To retain backward compatibility when upgrading your system in stages, no part of Security Center can be more than three major versions apart. For systems that are three to six major versions behind, use a two-step upgrade process that maintains backward compatibility.

The requirements for Security Center backward compatibility are as follows:

- **Upgrading to the latest version:** When upgrading, you must always upgrade the main server hosting the Directory role and Config Tool. Always upgrade each expansion server hosting a role type that is not backward compatible.
- **Using new features:** To use the new features introduced in version 5.8.1.0, upgrade your Security Center servers.
- **Role assigned to multiple servers:** If a role is assigned to multiple servers, such as in a failover configuration, all of its servers must be running the same version of Security Center.
- **Directory assigned to multiple servers:** All Directory servers must use the exact same *minor version*, meaning that all four digits of the version number must be the same. For example, if you upgrade to Security Center 5.8.1.0, you must upgrade all Directory servers to 5.8.1.0.
- **SQL Server:** Because Security Center 5.8 is not compatible with Microsoft SQL Server 2005, you must install a more recent version of the database server (see the system requirements for a list of compatible versions). For more information on how to upgrade your SQL Server, refer to your Microsoft documentation.

IMPORTANT: Because adding backward compatible connections slows down the performance of the Directory, it is recommended only as a temporary solution before you are able to upgrade all servers and workstations.

Backward compatibility between Security Center roles

Each new version of Security Center includes new role features that might not be compatible with earlier versions. The Security Center roles that are backward compatible are outlined in the following table.

IMPORTANT: All expansion servers hosting a role that is not backward compatible must be upgraded to the same version as the main server hosting the Directory.

Not all roles and tasks can run in backward compatibility mode. The following tables show which 5.8 roles and tasks are backward compatible.

5.8 role	Backward compatible with 5.5, 5.6 and 5.7
Access Manager	Yes
Active Directory	Yes (starting from 5.6)
Active Directory Federation Services	No
Archiver	Yes
Auxilliary Archiver	Yes
Camera Integrity Monitor (hidden)	No (introduced in 5.8)

5.8 role	Backward compatible with 5.5, 5.6 and 5.7
Directory Manager	No
Global Cardholder Synchronizer (GCS)	No
Health Monitor	No
Intrusion Manager	Yes
LPR Manager	Yes
Map Manager	Yes
Media Gateway	No (renamed from *RTSP Media Router* in 5.5 SR1)
Media Router	No
Mobile Server	No (introduced in 5.8)
Omnicast™ Federation™	Yes
Plugin (all instances)	No
Point of Sale	No
Privacy Protector™ (hidden)	Yes (introduced in 5.7 SR1)
Report Manager	No
Reverse Tunnel	No (introduced in 5.7 SR2)
Reverse Tunnel Server	No (introduced in 5.7 SR2)
Security Center Federation™	Yes
Wearable Camera Manager	No (introduced in 5.7 SR2)
Web Server	Yes (introduced in 5.6)
Web-based SDK	Yes
Zone Manager	Yes

Backward compatibility with Security Center tasks

The Security Center 5.8 tasks that are backward compatible with Security Desk 5.5, 5.6 and 5.7 are summarized in the following table.

Task category	Task type	Backward compatible with Security Desk 5.5, 5.6 and 5.7
Operation	Monitoring (live and playback video)	Yes
	Maps	Yes

Task category	Task type	Backward compatible with Security Desk 5.5, 5.6 and 5.7
	Dashboards	No (introduced in 5.8)
	Health dashboard	No (introduced in 5.8.1.0)
	Remote	No
	Cardholder management	Yes
	Credential management	Yes
	Visitor management	Yes
	People counting	Yes
	Hotlist and permit editor	Yes
	Inventory management	Yes
Alarm management	Alarm monitoring	Yes
	Alarm report	Yes
Investigation	Incidents	Yes
	Transactions	No
	Zone activities	Yes
Investigation > Access control	Area activities	Yes
	Door activities	Yes
	Cardholder activities	Yes
	Visitor activities	Yes
	Area presence	Yes
	Time and attendance	Yes
	Credential activities	Yes
	Credential request history	Yes
	Elevator activities	Yes
	Visit details	Yes
Investigation > Asset management	Asset activities	No
	Asset inventory	No

Task category	Task type	Backward compatible with Security Desk 5.5, 5.6 and 5.7
Investigation > Intrusion detection	Intrusion detection area activities	Yes
	Security video analytics	Yes (introduced in 5.7 SR2, renamed from *KiwiVision intrusion detector* in 5.7 SR5)
Investigation > LPR	Hits	Yes
	Hits (Mutli-region)	Yes
	Reads	Yes
	Reads (Mutli-region)	Yes
	Patroller tracking	Yes
	Inventory report	Yes
	Daily usage per Patroller	Yes
	Logons per Patroller	Yes
	Reads/hits per day	Yes
	Reads/hits per zone	Yes
	Zone occupancy	Yes
	Parking sessions	Yes (introduced in 5.6)
	Parking zone activities	Yes (introduced in 5.6)
Investigation > Video	Archives	Yes
	Bookmarks	Yes
	Motion search	Yes
	Camera events	Yes
	Video file explorer	Yes
	Forensic search	Yes
Maintenance	System status	Yes
	Audit trails	Yes
	Activity trails	Yes
	Health history	Yes
	Health statistics	Yes
	Hardware inventory	Yes

Task category	Task type	Backward compatible with Security Desk 5.5, 5.6 and 5.7
Maintenance > Access control	Access control health history	Yes
	Access control unit events	Yes
	Cardholder access rights	Yes
	Door troubleshooter	Yes
	Access rule configuration	Yes
	Cardholder configuration	Yes
	Credential configuration	Yes
	I/O configuration	Yes
Maintenance > Intrusion detection	Intrusion detection unit events	Yes
Maintenance > Video	Camera configuration	Yes
	Archiver events	Yes
	Archiver statistics	No (introduced in 5.8)
	Archive storage details	Yes
	Wearable camera evidence	No (introduced in 5.8)

Supported Federation™ features for Security Center 5.8.1.0

Security Center 5.8 can federate and be federated by other Security Center systems running different versions.

The following Federation™ scenarios are supported:

- **Backward Federation™:** Security Center 5.8.1.0 can federate:
  - Security Center 5.5, 5.6, and 5.7.
  - Omnicast™ 4.6, 4.7 and 4.8 systems.
  - Stratocast™ systems.
- **Forward Federation™:** Security Center 5.8 can be federated by:
  - Security Center 5.7 and 5.8 systems.

IMPORTANT: A system running the most current release of Security Center can:

- Federate systems up to three versions back.
- Be federated by a system running the previous version of Security Center.

  For example, Security Center 5.8 systems can federate Security Center 5.5, 5.6, 5.7, and 5.8 systems. A Security Center 5.5 system can only federate 5.6 systems, not 5.8 systems.

For more information about the limitations of federated entities, see the *About federated entities* section of the *Security Center Administrator Guide*. These limitations apply to both forward and backward federated systems.

Omnicast™ compatibility in Security Center 5.8.1.0

Product compatibility indicates that the product can support and run with specific versions of other products.

Security Center 5.8.1.0 is compatible with the following Omnicast™ components.

	Omnicast™ 4.x Archiver service	Without Archiver service	More than 30 cameras	Omnicast™ federations
Security Center 5.8	No[a]	Yes[b]	No[c]	4.6, 4.7, and 4.8[d]

[a.] The Security Center 5.8 Archiver role and the Omnicast™ 4.x Archiver service cannot run on the same server.

[b.] If the Archiver role is not running on the Omnicast™ server, then Security Center 5.8 can coexist on the same server as Omnicast™.

[c.] If Omnicast™ supports more than 30 cameras, it is best practice to host Security Center and Omnicast™ on different computers.

[d.] The Security Center Media Router cannot stream video from federated Omnicast™ systems. Video streams from federated Omnicast™ systems are streamed directly to the Security Desk client using the Omnicast™ Compatibility Pack. This means that the Security Desk client must be able to connect directly to the Omnicast™ server. For information about installing the Omnicast™ Compatibility Pack, see the *Security Center Installation and Upgrade Guide*. The latest version of this document is available on the Genetec™ TechDoc Hub.

2

Installation and upgrade notes

This section includes the following topics:

Features that impact an upgrade to Security Center 5.8.1.0

It is important to know about Security Center 5.8 features that will change how you interact with the system after an upgrade.

Note the following when upgrading to Security Center 5.8.1.0:

- **New .NET Framework requirements:** Starting with Security Center 5.8 GA, .NET Framework 4.7.1 is included in Security Center. The minimum Windows 10 version supported is 1607 (Windows 10 Anniversary Update). The Security Center installation will fail with older versions of Windows 10.
- **Enhanced complexity requirements for main server password:** Starting with Security Center 5.8 GA, when you update the main server password used by Server Admin, the new password must meet all of the following criteria:
  - At least 8 characters long
  - 1 or more upper case letters
  - 1 or more lower case letters
  - 1 or more numerical characters
  - 1 or more special characters
  - No spaces or double quotation marks.
- **Changed default port for redirectors:** Starting with Security Center 5.8 GA, TCP port 960 replaces TCP port 5004 as the initial default port for stream requests.

  If you are upgrading from Security Center 5.6 or 5.7, your redirectors will continue to use TCP port 5004 and no action is needed.

  If you are upgrading from Security Center 5.5 or earlier, your redirectors will use TCP port 960. Ensure that port 960 is open in addition to port 560 for firewall and network address translation purposes, or you might not be able to view live video streams from remote sites.
- **Changed Logon dialog box:** Starting with Security Center 5.7 SR2, you can no longer leave the **Directory** field blank in the *Logon* dialog box. You must enter the name or IP address of the main server you want to connect to. If your client application is running on the main server, you can also enter `Localhost` as the Directory name.
- **Deprecated custom temporary access rules based on custom fields:** Temporary access rules are supported natively in Security Center 5.7 SR1 and later. Because custom and native temporary access rules cannot be used together, we recommend that you use our native solution. If you are currently using the custom solution in Security Center 5.6, and want to upgrade to Security Center 5.7 SR1 or later, contact our Technical Assistance Center (GTAC) for help.
- **Introduced native double-badge events:** If you have event-to-actions configured for double-swipe in Security Center 5.7, you must reset your event-to-actions to use the *Double badge on* and *Double badge off* events in Security Center 5.8 GA or later. For more information, refer to "Creating event-to-actions" in the *Security Center Administrator Guide*.
- **Introduced new license for restricted cameras:** Starting with Security Center 5.6 GA, there is a new license option called *Number of restricted cameras*. Cameras developed by some manufacturers have been restricted due to a higher cybersecurity risk profile; these cameras require a special connection license, in addition to the normal camera license. If you have restricted cameras on your system after upgrading to Security Center 5.8, these video units will stop working and the Archiver will be in a warning state until you license the restricted camera connections.

  To view a list of manufacturers that require a restricted license, use the **Restricted** *License Type* filter on the Supported Device List.
- **Introduced new port for Archiver roles:** Starting with Security Center 5.6 GA, Archivers require two ports: one port for live and playback stream requests (TCP 555) and one port for edge playback stream requests (TCP 605). If you are upgrading from Security Center 5.5 or earlier, make sure that port 605 is open in addition to port 555 for firewall and network address translation purposes, or you might not be able to view playback video streams from edge devices.

- **Recommendations for running the Global Cardholder Synchronizer (GCS) role:** If your system is a *sharing guest*, make sure of the following:
  - The *sharing host* system is running the same version, or a later version of Security Center.
  - You have recorded a list of the global partitions you want to synchronize, in case you must apply them after the upgrade.
  - If the GCS role is running on an expansion server, perform one of the following two options:
    - Move the GCS role to the main server hosting the Directory role.
    - Keep the GCS role on the expansion server, but deactivate the role until both the main and expansion servers are running the same version of Security Center.
- **Supported integrated software:** Plugin users might need to upgrade their integrated software to a version supported by Security Center 5.8.1.0. For more information, refer to Supported plugins in Security Center.

For instructions about how to upgrade Security Center, see the *Security Center Installation and Upgrade Guide*.

Differences between Security Center 5.x and 5.8 privileges

Beginning in Security Center 5.7 GA, most privileges that were reserved exclusively to administrators, such as adding users, can now be granted individually. Some actions, such as modifying the logical IDs, that used to be covered under generic privileges, now require specific privileges, because they might affect the entire system.

Privileges that are no longer exclusive to administrators starting in 5.7

Starting in Security Center 5.7 GA, users no longer need to be members of the Administrators user group to perform the following actions.

Administrative privileges > *System management*:

- **View network properties:** Allows the user to view network properties (also grants access to the *Network view* task).
  - **Modify network properties:** Allows the user to modify network properties, and to add and delete network entities.
- **View partition properties:** Allows the user to view partition properties (also grants access to the *User management* task).
  - **Modify partition properties:** Allows the user to modify partition properties.
    - **Add partitions:** Allows the user to add partitions.
    - **Delete partitions:** Allows the user to delete partitions.
- **View role properties:** Allows the user to view role properties (also grants access to the *System* task, *Roles* view).
  - **Modify role properties:** Allows the user to modify role properties.
    NOTE: If a role belongs to multiple partitions, changing any role property (for example, deactivating the role) affects all partitions, not just the ones the user has access to.
    - **Add roles:** Allows the user to add roles.
    - **Delete roles:** Allows the user to delete roles.
- **View server properties:** Allows the user to view server properties (must be combined with *View network properties* privilege).
  - **Modify server properties:** Allows the user to modify server properties.
    - **Delete servers:** Allows the user to delete servers.
- **View user group properties:** Allows the user to view user group properties (also grants access to the *User management* task).
  - **Modify user group properties:** Allows the user to modify user group properties.
    NOTE: Users can never grant privileges that they do not have. For example, a user cannot add a member to a user group if the user group has privileges that they do not have. If a privilege operation requires more privileges than the user has, the operation will be denied.
    - **Add user groups:** Allows the user to add user groups.
    - **Delete user groups:** Allows the user to delete user groups.
- **View user properties:** Allows the user to view user properties (also grants access to the *User management* task).
  - **Modify user properties:** Allows the user to modify user properties.

    - **Add users:** Allows the user to add users.
    - **Delete users:** Allows the user to delete users.
- **View general settings:** Allows the user to view general settings.

  NOTE: All general settings have a system-wide scope, so exercise great care when making any changes.

  - **Modify custom field definitions:** Allows the user to add, modify, and delete custom field definitions and custom data types.
  - **Modify custom events:** Allows the user to add, modify, and delete custom events, and change event colors.
  - **Modify event-to-actions:** Allows the user to add, modify, and delete event-to-actions.
    If you upgraded from 5.6 or earlier to 5.8, users who used to be able to modify event-to-actions by virtue of their *System* task privilege will no longer be able to, unless they are explicitly granted the *Modify event-to-actions* privilege in the new system.
  - **Modify logical IDs:** Allows the user to modify the logical ID of entities (must be combined with *Modify entity properties* privileges).
    If you upgraded from 5.6 or earlier to 5.8, users who used to be able to modify logical IDs by virtue of their *Modify entity properties* privilege will no longer be able to, unless they were administrators or partition administrators in the old system.
  - **Modify password settings:** Allows the user to modify user password settings.
  - **Modify activity trail settings:** Allows the user to configure which activity types should be logged.
  - **Modify audio files:** Allows the user to modify audio files, and to add and delete custom ones.
  - **Modify incident categories:** Allows the user to add, modify, and delete incident categories.
  - **Modify enabled features:** Allows the user to enable and disable licensed features.
  - **View macro properties:** Allows the user to view macro properties.
    NOTE: Only administrators can add, modify, and delete macros.

Action privileges > *Alarms*:

- **Acknowledge alarms:** Allows the user to acknowledge alarms (*this is not a new privilege*).
  - **Forcibly acknowledge alarms:** Forcibly acknowledge alarms that have an active condition attached.

Privileges that are no longer exclusive to administrators starting in 5.8

Starting in Security Center 5.8 GA, users no longer need to be members of the Administrators user group to perform the following actions.

Administrative privileges > *System management* > *View general settings*:

- **View threat levels:** Allows the user to view threat levels.
  - **Modify threat levels:** Allows the user to modify threat levels.
    - **Add threat levels:** Allows the user to add threat levels.
    - **Delete threat levels:** Allows the user to delete threat levels.

Task privileges > *Administration*:

- **Video:** Allows the user to run the *Video* task (*this is not a new privilege*).
  - **Archive transfer:** Allows the user to perform archive transfers from the *Video* task.
- **Access control:** Allows the user to run the *Access control* task (*this is not a new privilege*).
  - **General settings:** Allows the user to view and modify access control configuration settings such as custom card formats and HID Mobile Access.

Task privileges > *Tools*:

- **Import tool:** Allows the user to launch the Import tool.

Privileges that remain exclusive to administrators

The following privileges remain exclusive to members of the *Administrators* user group.

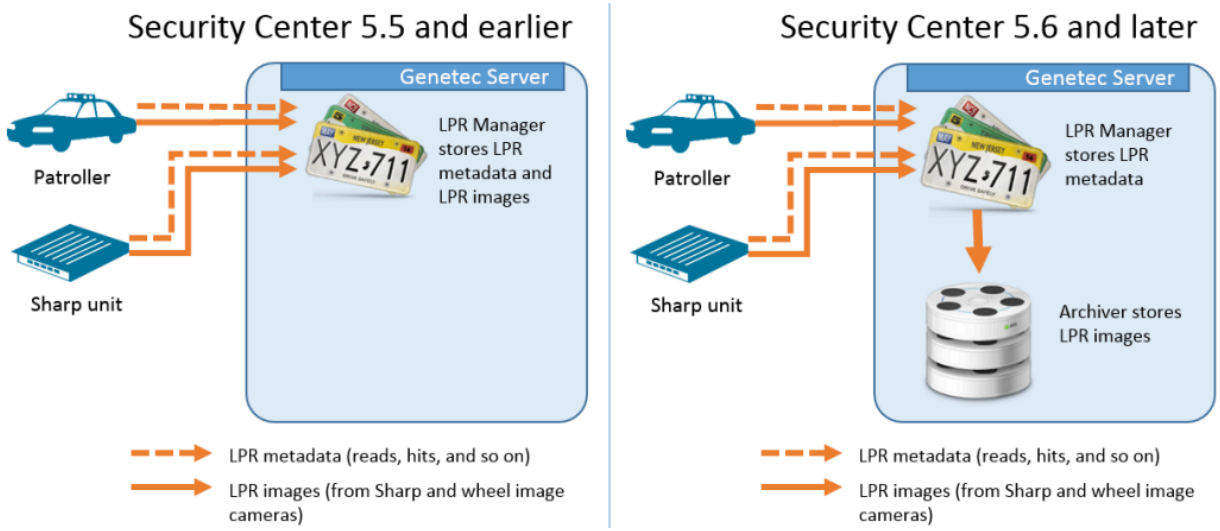
- Adding, modifying, and deleting macros.
- Creating generic event-to-actions (without a specific source entity).
- Running the *Diagnostic data collection tool*.

Differences between LPR Manager 5.x and 5.8

Beginning in Security Center 5.6, the LPR Manager must work in tandem with an Archiver. After upgrading an LPR Manager from 5.5 or earlier to 5.8, the role might be in the warning state (yellow). To make the LPR Manager operational, you must assign an Archiver role to it.

Data management: Before and After

The following diagram shows how data are stored before and after Security Center 5.6.



Feature differences

Characteristics	LPR Manager 5.5 and earlier	LPR Manager 5.6 and later
Data management	The LPR Manager stores both the LPR images (captured by context cameras, LPR cameras, and wheel imaging cameras), and the LPR metadata (reads, hits, timestamps, Patroller positions, and so on) in a database.	The LPR Manager stores the LPR metadata (reads, hits, timestamps, Patroller positions, and so on) in a database. The Archiver stores the LPR images (captured by context cameras, LPR cameras, and wheel imaging cameras) on disk in G64 files.
Data retention periods	Data retention periods configured in LPR Manager properties.	Data retention periods configured in LPR Manager properties. The Archiver follows the LPR Manager's data retention settings.
Automatic cleanup	Once per day.	Every 15 minutes for LPR metadata. Every 5 minutes for LPR images.
SQL Server Express capacity	Limited to 10 GB per database (roughly 160,000 reads with images).	Limited to 10 GB per database, but stores up to 6 million reads because the image data are no longer stored in the database.
Performance	-	Updated data structure to improve query performance.

Characteristics	LPR Manager 5.5 and earlier	LPR Manager 5.6 and later
Configuration	LPR Manager configuration tabs.	LPR Manager configuration tabs. Archiver **Resources** tab. Media Router **Properties** tab.
Role failover	In Config Tool, assign a secondary server to the LPR Manager role, and make sure the LPR Manager database is accessible over the network from both servers.	No changes to the LPR Manager failover configuration. The Archiver failover is configured separately and independently of the LPR Manager. Each server assigned to the Archiver role must have its own archive database. This means that when the Archiver role fails over to the secondary server, the data managed by the primary server is not available. **BEST PRACTICE:** To simplify the failover configuration, we recommend assigning the same primary and secondary servers to both the LPR Manager and the Archiver roles, provided that these servers meet the combined load requirements.
Backup and restore	The LPR Manager database is backed up and restored like any role database.	The LPR Manager database is backed up and restored like any role database. The Archiver database is only used to store the catalog of the G64 files stored on disk. To protect your LPR data, you must back up both the Archiver database and the G64 files. **NOTE:** The *Archive transfer* task does not yet support G64 files containing LPR images. If you restore the G64 files to a different disk, you must re-index these files in the Archiver database using the *VideoFileAnalyzer.exe* tool.

Limitations about GCS roles when upgrading to 5.8

If you are using the Global Cardholder Synchronizer (GCS) role in your system, there are important limitations that you must be aware of when you upgrade your system to 5.8.

The Global Cardholder Management (GCM) module was rewritten in Security Center 5.7 GA to improve efficiency and scalability. Because of this enhancement, the Security Center 5.7 Directory is no longer backward compatible with earlier versions of *Global Cardholder Synchronizer (GCS)* roles.

For a GCS role (*sharing guest*) to connect to a *sharing host* running Security Center 5.8, the following criteria must be met:

- The minimum Security Center version of the sharing guest is 5.7.
- The Security Center version of the sharing host is equal to, or higher than its sharing guests.

Example

The following table shows the compatibility between sharing hosts and sharing guests running different versions of Security Center:

Sharing host version	Sharing guest version	Compatible
5.8	5.8	Yes
5.8	5.7	Yes
5.8	5.6 or earlier	No
5.7	5.8	No
5.7	5.7	Yes

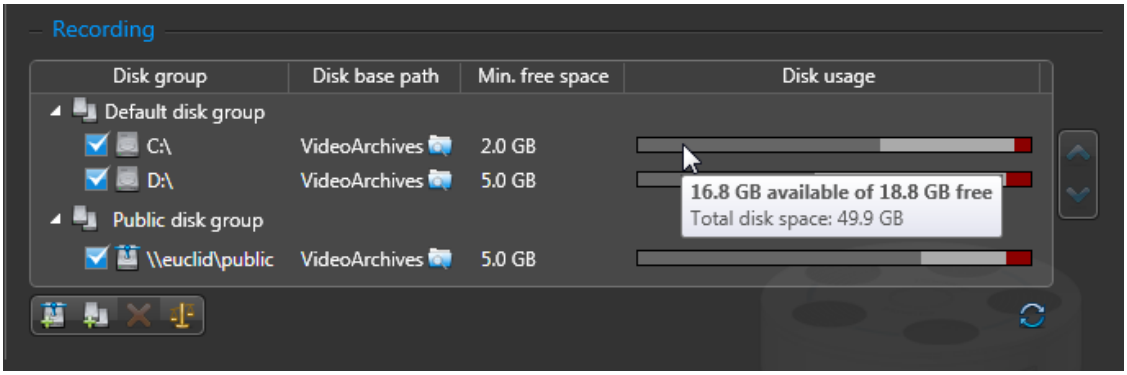
For more information about GCM, see the *Security Center Administrator Guide*.

Archive storage

In Security Center, video recordings are stored on disk, in small G64 files that each contain one or more short video sequences.

Like the archive database, the archive file storage is specific to each server. The location of the video files and the description of the *video sequences* they contain (source camera, beginning and end of sequence) are stored in the database catalog managed by the *Archiver* or *Auxiliary Archiver*.

Both local drives and network drives can be used to store video. In the **Resources** tab for the archiving role, all local drives on the host server are listed by default and grouped under *Default Disk Group*, as shown in the following image:



Disk space cannot be allocated to video archives in advance. Instead, archiving roles can only use a limited amount of the available disk space. This limit is set by the **Min. free space** attribute for each disk. The recommended minimum free space is at least .2% of the total disk space.

IMPORTANT: You must ensure that the service user running the Archiver or Auxiliary Archiver role has write access to all the archive root folders assigned to the role.

Archive storage requirements

Because the Archiver role and Auxiliary Archiver roles can control a different number of cameras, you must evaluate the storage requirements for each of these roles separately.

The storage requirements are affected by the following factors:

- Number of cameras to archive.
- Archive retention period: amount of time to keep the archives online.
- Percentage of video files protected from automatic deletion.
- Percentage of recording time, which depends on the selected archiving mode: continuous, on motion, manual, scheduled, or off. Continuous recording consumes disk space faster than the other archiving modes.
- Frame rate: higher frame rate recordings need more storage space.
- Image resolution, which depends on the video data format: higher resolution recordings need more storage space.
- Percentage of movement: most video encoding schemes compress data by storing only the changes between consecutive frames. Scenes with a lot of movement require more storage than scenes with little movement.
- Audio: including audio increases the required storage space.
- Metadata from features such as *video analytics*, *privacy protection*, and *fusion stream encryption*. Included metadata can increase the required storage space.

TIP: Regularly checking the disk usage statistics is the best way to estimate future storage requirements, and to make quick adjustments.

Storage requirement for LPR images

The images associated with the reads and hits are stored on disk in G64 files by an Archiver. You can estimate the disk space required to store these images if you know the average number of reads and hits processed by the LPR Manager per day.

For every license plate read or hit processed by the LPR Manager, the Archiver stores a set of four images:

- One context camera image (in either high resolution or low resolution)
- One LPR camera image (cropped to show only the license plate)
- One context camera thumbnail image
- One LPR camera thumbnail image

The size of the image set depends on the model of the Sharp camera and whether the context camera is configured to take images in high resolution or low resolution.

Use the following formula to estimate the disk space you need for the desired image retention periods.

```
Disk space = (ReadsPD x ImageSize x ReadIRP) + (HitsPD x ImageSize x HitIRP)
```

where:

- **ReadsPD:** Average number of reads per day.
- **ImageSize:** Estimated image size per read (depends on the Sharp model and configuration).
- **ReadIRP:** Read image retention period (see LPR Manager's **Properties** tab).
- **HitsPD:** Average number of hits per day.
- **HitIRP:** Hit image retention period (see LPR Manager's **Properties** tab).

If your patrol vehicles are equipped with wheel imaging cameras, double the number of hits per day in your formula (there is typically one wheel image per hit).

The following table gives you the rough estimates of the image size per read based on the Sharp model and configuration.

Type of image	Sharp VGA or XGA	SharpV
Context camera image (high res. config.)	~50 KB	~120 KB
LPR camera image (cropped)	~3 KB	~3 KB
Context camera thumbnail image	~3 KB	~3 KB
LPR camera thumbnail image	~1 KB	~1 KB
Total image size per read (high res. config.)	~57 KB	~127 KB
Context camera image (low res. config.)	~18 KB	-
LPR camera image (cropped)	~3 KB	~3 KB
Context camera thumbnail image	~3 KB	~3 KB
LPR camera thumbnail image	~1 KB	~1 KB
Total image size per read (low res. config.)	~25 KB	-

NOTE: If a read or hit is protected and must be kept beyond its specified retention period, it will require more disk space for its associated images than what is calculated for a single event. Because the Archiver stores multiple LPR images in a single G64 file, if one image in the file is protected, then all other images in the file are also protected. This uses up more disk space over time. However, an image whose corresponding read or hit has been deleted can no longer be read because the G64 files are encrypted.

If the Archiver is assigned to more than one LPR Manager, add the numbers for all LPR Manager roles together.

Glossary

Archiver
The Archiver role is responsible for the discovery, status polling, and control of video units. The Archiver also manages the video archive and performs motion detection if it is not done on the unit itself.

Archive transfer
The *Archive transfer* task is an administration task that allows you to configure settings for retrieving recordings from a video unit, duplicating archives from one Archiver to another, or backing up archives to a specific location. Starting from Security Center 5.8 GA, the *Archive transfer* task is part of the *Video* administration task.

Auxiliary Archiver
The Auxiliary Archiver role supplements the video archive produced by the Archiver role. Unlike the Archiver role, the Auxiliary Archiver role is not bound to any particular *discovery port*, therefore, it can archive any camera in the system, including cameras federated from other Security Center systems. The Auxiliary Archiver role cannot operate independently; it requires the Archiver role to communicate with video units.

encryption certificate
An encryption certificate, also known as a *digital certificate* or *public key certificate*, is an electronic document that contains a public and private key pair used in Security Center for *fusion stream encryption*. Information encrypted with the *public key* can only be decrypted with the matching *private key*.

fusion stream encryption
Fusion stream encryption is a proprietary technology of Genetec Inc. used to protect the privacy of your video archives. The Archiver uses a two-level encryption strategy to ensure that only authorized client machines or users with the proper certificates on smart cards can access your private data.

Genetec™ Update Service
The Genetec™ Update Service (GUS) is automatically installed with most Genetec™ products and enables you to update products when a new release becomes available.

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

privacy protection
In Security Center, privacy protection is software that anonymizes or masks parts of a video stream where movement is detected. The identity of individuals or moving objects is protected, without obscuring movements and actions or preventing monitoring.

Privacy Protector™
The Privacy Protector™ role requests original video streams from Archiver roles and applies data anonymization to the original video streams. The privacy-protected (anonymized)

	video stream is then sent back to the Archiver role for recording.
server	A server is a type of entity that represents a server machine on which the Genetec™ Server service is installed.
sharing guest	A sharing guest is a Security Center system that has been given the rights to view and modify entities owned by another Security Center system, called the sharing host. Sharing is done by placing the entities in a global partition.
sharing host	Sharing host is a Security Center system that gives the right to other Security Center systems to view and modify its entities by putting them up for sharing in a global partition.
video analytics	Video analytics is the software technology that is used to analyze video for specific information about its content. Examples of video analytics include counting the number of people crossing a line, detection of unattended objects, or the direction of people walking or running.
video sequence	A video sequence is any recorded video stream of a certain duration.

Where to find product information

You can find our product documentation in the following locations:

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

Technical support

Genetec™ Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a customer of Genetec Inc., you have access to TechDoc Hub, where you can find information and search for answers to your product questions.

- **Genetec™ TechDoc Hub:** Find articles, manuals, and videos that answer your questions or help you solve technical issues.

  Before contacting GTAC or opening a support case, it is recommended to search TechDoc Hub for potential fixes, workarounds, or known issues.

  To access the TechDoc Hub, log on to Genetec™ Portal and click TechDoc Hub. Can't find what you're looking for? Contact documentation@genetec.com.

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

Additional resources

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

- **Forum:** The Forum is an easy-to-use message board that allows clients and employees of Genetec Inc. to communicate with each other and discuss many topics, ranging from technical questions to technology tips. You can log on or sign up at https://gtapforum.genetec.com.
- **Technical training:** In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to http://www.genetec.com/support/training/training-calendar.

Licensing

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

Hardware product issues and defects

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