Genetec™ Security Center.

Lenel OnGuard Plugin Guide 5.2.2

Click here for the most recent version of this document.

Document last updated: December 01, 2025

Genetec™

Legal notices

©2025 Genetec Inc. All rights reserved.

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

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

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

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

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

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

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

Genetec products, services, and innovations are protected by patents and other intellectual property rights in various jurisdictions, including the United States. For a detailed list of patents owned by Genetec Inc., visit www.genetec.com/patents.

All specifications are subject to change without notice.

Document information

Document title: Lenel OnGuard Plugin Guide 5.2.2

Original document number: EN.550.006-V5.2.2.B(2)

Document number: EN.550.006-V5.2.2.B(2)

Document update date: December 01, 2025

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

About this guide

This guide describes how to integrate OnGuard access control systems in Security Center.

This guide supplements the documentation provided with Security Center. It assumes that you are a certified user of Security Center, Synergis™, and Omnicast™, and that you are familiar with the configuration and use of the following:

- Security Center systems
- OnGuard

For specific information regarding third-party hardware, software, and systems, refer to their manufacturer's documentation and website.

To get your certification, refer to our list of Security Center courses at https://www.genetec.com/support/training/certification-courses.

Notes and notices

The following notes and notices might appear in this guide:

- **Tip:** Suggests how to apply the information in a topic or step.
- **Note:** Explains a special case or expands on an important point.
- **Important:** Points out critical information concerning a topic or step.
- **Caution:** Indicates that an action or step can cause loss of data, security problems, or performance issues.
- **Warning:** Indicates that an action or step can result in physical harm, or cause damage to hardware.

IMPORTANT: Content in this guide that references information found on third-party websites was accurate at the time of publication, however, this information is subject to change without prior notice from Genetec Inc.

Contents

Preface

Legal notices. . . . ii
About this guide. . . . iii

Chapter 1: Introduction to the OnGuard plugin

What is the OnGuard plugin?. . . . 2
How the OnGuard plugin works with Security Center. . . . 3
Integration overview. . . . 4
OnGuard terminology. . . . 6

Chapter 2: Release notes

What's new in version 5.2.2. . . . 8
Resolved issues in version 5.2.2. . . . 8
Known issues. . . . 9
Limitations. . . . 10
Product compatibility. . . . 12
System requirements. . . . 13
License options. . . . 14
Supported features. . . . 15
Supported devices. . . . 16
Synchronized entities and properties. . . . 17
Custom events added by the OnGuard plugin. . . . 20

Chapter 3: Deploying the OnGuard plugin

Ports used by the OnGuard plugin. . . . 22
Upgrading. . . . 23
Upgrading from version 5.x.x. . . . 24
Upgrading from version 4.x. . . . 24
Upgrading from version 3.x. . . . 25
Downloading and installing the plugin. . . . 26
Performing a silent installation of the plugin. . . . 28
Required privileges. . . . 30
Creating the plugin role. . . . 33
Scheduling database backups and cleanups. . . . 34

Chapter 4: Setting up failover and Federation™

Enabling failover on the plugin role. . . . 38
Enabling partial failover on the proxy. . . . 40
Setting up Federation to monitor remote OnGuard entities. . . . 41

Chapter 5: Configuring the plugin

Configuring the proxy service. . . . 44
Connecting to the OnGuard server. . . . 46
Maintaining a connection between Security Center and OnGuard. . . . 47
Selecting which cardholder information is sent through the proxy. . . . 48
Enabling live synchronization of entities. . . . 50

Starting a manual synchronization. 52
Configuring OnGuard plugin alarm settings. 54
Disabling OnGuard custom events in Security Center. 56
About linking cameras to OnGuard entities. 57
Linking Security Center cameras to OnGuard inputs. 59

Chapter 6: Monitoring OnGuard events

Contextual menu commands available for OnGuard entities. 62
How OnGuard alarms work with Security Center. 65
How OnGuard actions are triggered in Security Center. 66
Supported reports. 67

Chapter 7: Maintenance and troubleshooting

OnGuard plugin installed but missing from Security Desk and Config Tool. 69

Glossary 70

Where to find product information 72

Technical support 73

1

Introduction to the OnGuard plugin

This section includes the following topics:

- "What is the OnGuard plugin?" on page 2
- "How the OnGuard plugin works with Security Center" on page 3
- "Integration overview" on page 4
- "OnGuard terminology" on page 6

What is the OnGuard plugin?

The OnGuard plugin is an access control plugin that integrates OnGuard access control systems with Security Center. Using the OnGuard plugin, you can monitor access control entities, alarms, and events from your OnGuard system directly in Security Center.

Administrator tasks using Config Tool

Using the plugin you can do the following:

- Connect to OnGuard integrated access control systems.
- Select the entities, devices, alarms and events from the OnGuard system that you want to synchronize with Security Center entities and events.
- Select the OnGuard events that you want to receive in Security Center. Events can be received as custom events from OnGuard, or as the Security Center event that the custom event is mapped to.
- Configure how OnGuard alarms are triggered and acknowledged in Security Center.
- Configure the number of historical logged events that you want imported when performing a manual synchronization with the OnGuard system.
- View the progress of OnGuard entities, alarms and events as they are synchronized with your Security Center system.
- Assign Security Center cameras to OnGuard input entities.
- Trigger actions and outputs in OnGuard using hot actions, and event-to-actions.
- Configure event-to-actions in Security Center using OnGuard events and alarms.
- Federate Security Center systems: monitor entities, alarms and events of a OnGuard system connected to a federated Security Center system.

Operator tasks using Security Desk

- Display live access control events from OnGuard in Security Desk with detailed cardholder information.
- Monitor and acknowledge OnGuard alarms using the *Alarm monitoring* task in Security Desk.
- Monitor live and playback video related to access control events received from OnGuard in the *Monitoring* task of Security Desk.
- Lock and unlock doors in OnGuard from Security Desk.
- Generate Security Center reports to search for past events and alarms.
- Deactivate an OnGuard cardholder from Security Desk.

IMPORTANT: If you are connecting to OnGuard Enterprise, it is recommended that you first speak with your Genetec™ representative, as the plugin will behave differently and offer different functionality.

For information about monitoring entities, alarms and events, and triggering actions and output in Security Desk, see the *Security Center User Guide*. You can access this guide by pressing F1 in Security Desk.

For information about creating event-to-actions in Config Tool, see the *Security Center Administrator Guide*. You can access this guide by pressing F1 in Config Tool.

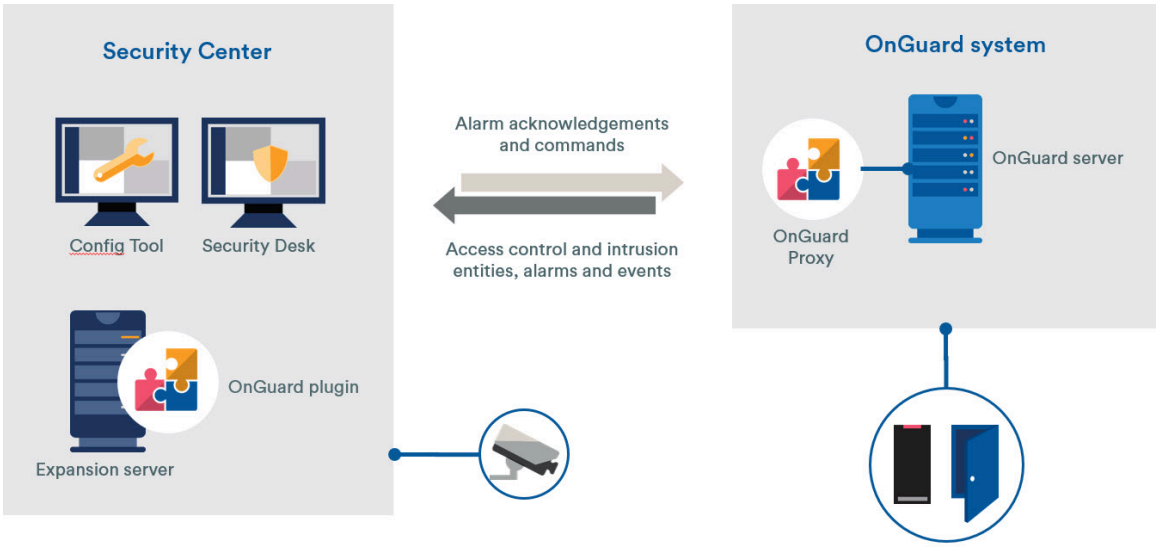
Related Topics

What's new in version 5.2.2 on page 8
Integration overview on page 4

How the OnGuard plugin works with Security Center

The OnGuard plugin integrates OnGuard access control systems with Security Center.

The OnGuard system sends access control events to Security Center through the OnGuard plugin. The plugin forwards these events, and converts them into Security Center events and alarms. It also receives Security Center queries and report requests.



Components of OnGuard integration

- **OnGuard plugin:** The OnGuard plugin is installed on a Security Center server and runs as a plugin role.
- **Config Tool:** The OnGuard plugin is also installed on a Config Tool workstation. The Security Center administrator uses Config Tool to create and configure the plugin role.
- **Security Desk:** The OnGuard plugin is installed on all Security Desk workstations.
- **OnGuard proxy:** The proxy is installed as part of the plugin on the OnGuard server. The proxy connects Security Center to the OpenAccess API, which retrieves information from the OnGuard database and sends it to Security Center. The proxy should be installed on a workstation within the OnGuard ecosystem to access the OpenAccess API.
- **OnGuard server:** The OnGuard server hosts the OnGuard services, including the OpenAccess API service.

Related Topics

Integration overview on page 4

Integration overview

You can integrate OnGuard into Security Center using the OnGuard plugin by following a sequence of steps.

The following table lists the tasks required for the integration with Security Center, and how to verify that the integration was successful.

Step	Task	Where to find more information
Understand prerequisites and key issues before deploying		
1	Learn what you can do using the plugin.	• What is the OnGuard plugin? on page 2.
2	Before installing the plugin, read the release notes to learn about the new features, the known issues, and the limitations.	• What's new in version 5.2.2 on page 8. • Known issues on page 9. • Limitations on page 10.
3	Learn about the different components and how they connect together.	• How the OnGuard plugin works with Security Center on page 3.
4	Ensure that the server where the plugin will be installed meets the recommended system requirements and is running a compatible version of Security Center.	• Product compatibility on page 12 • System requirements on page 13.
Prepare Security Center		

5	In Security Center, create a georeferenced map. Maps can enhance your situation awareness as you represent and control your security devices directly on maps.	• Refer to the following topics in the *Security Center Administrator Guide*:
		  • Creating maps
		  • Creating maps by connecting to a GIS
		  • Georeferencing a map image
		  • Supported map objects

6	Verify that the Security Center license has a valid certificate for the plugin. Go to the Config Tool homepage, click **About** > **Certificates**, and confirm that OnGuard is in the list.	• Your license information is included in the license update email that we sent you. This email includes links to the download package and other license information. • To acquire a license, see License options on page 14.
Deploy the plugin		
7	On a Security Center server, download the plugin and install it.	• Downloading and installing the plugin on page 26.

Step	Task	Where to find more information
8	Grant users the privileges that they need to use the plugin. • Required privileges on page 30. • Administrators need the *Add roles*, *Delete roles*, and *Plugins* privileges. • Security Desk operators do not need special privileges to use this plugin.	• Refer to "Assigning privileges to users" in the *Security Center Administrator Guide*. • For a list of all available privileges, refer to the Security Center privileges spreadsheet for your version.
9	In Config Tool, create the OnGuard plugin role.	• Creating the plugin role on page 33.
10	Schedule regular cleaning and backing up of the plugin database.	• Scheduling database backups and cleanups on page 34.
Configure the plugin		
11	Change the plugin configuration to suit your particular needs.	• Configuring the proxy service on page 44. • Connecting to the OnGuard server on page 46. • Selecting which cardholder information is sent through the proxy on page 48. • Maintaining a connection between Security Center and OnGuard on page 47. • Configuring OnGuard plugin alarm settings on page 54. • Disabling OnGuard custom events in Security Center on page 56. • About linking cameras to OnGuard entities on page 57. • Linking Security Center cameras to OnGuard inputs on page 59.
12	Synchronize Security Center with the OnGuard system.	• Enabling live synchronization of entities on page 50. • Starting a manual synchronization on page 52.

OnGuard terminology

OnGuard uses specific terms. Here are the definitions of some common terms and their equivalents in Security Center.

OnGuard	Security Center
Cardholder	Cardholder
Visitor	Visitor
Panel	Access Control unit or Intrusion detection unit
Reader	Reader and Door
Input	Input
Output	Output
Area	Area
Intrusion Door	Door
Intrusion Area	Intrusion Area
Intrusion Zone	Alarm Panel Input
Alarm Definition	Alarm
Onboard Relay	Alarm Panel Output
Offboard Relay	Alarm Panel Output

Related Topics

Integration overview on page 4

2

Release notes

This section includes the following topics:

- "What's new in version 5.2.2" on page 8
- "Known issues" on page 9
- "Limitations" on page 10
- "Product compatibility" on page 12
- "System requirements" on page 13
- "License options" on page 14
- "Supported features" on page 15
- "Supported devices" on page 16
- "Synchronized entities and properties" on page 17
- "Custom events added by the OnGuard plugin" on page 20

What's new in version 5.2.2

The OnGuard plugin 5.2.2 is a patch release that includes software enhancements that improve functionality and reliability.

General enhancements

- **View source input of OnGuard alarms in Alarm monitoring task:** You can now view the source input of an OnGuard alarm in the *Alarm monitoring* task. If the source input isn't synchronized with Security Center, the source column displays its synchronized parent entity. For more information, see How OnGuard alarms work with Security Center on page 65.
- **Unit replacement automatic input mapping:** After using the Unit replacement tool to replace a camera, mapped inputs are now automatically updated in the *Plugins* task **Cameras** tab if the plugin is online. If the plugin is offline when the replacement happens, the input mappings must be updated manually.

  IMPORTANT: This feature is only supported for the following Security Center versions:

  - 5.12.2.4, 5.13.0.1, and their subsequent patch releases.
  - 5.13.1.1 and later.

Related Topics

What is the OnGuard plugin? on page 2
Integration overview on page 4

Resolved issues in version 5.2.2

The following issues are resolved in the OnGuard plugin 5.2.2.

Issue	Description
4708025	The OnGuard plugin does not have multi-role support. You can only have one OnGuard plugin role per system.
4663282	The plugin role doesn't show a *disconnected* warning when the proxy loses connection with the OnGuard server.
4572196	When using a dual-panel interface board, only one of the child readers goes offline when the reader interface board disconnects. The second panel continues to appear online.
4556717	If a user enters the wrong username or password while logging into the proxy, the proxy repeatedly tries reconnecting to Lenel without allowing the user to intervene.
4533923	Frequent opening and closing of an OnGuard door slows down the directory's performance.
4503007	The OnGuard plugin deletes cardholders slowly at the rate of 50 cardholders per minute. Deleting a large batch of cardholders negatively impacts the directory's performance.
4470426	The OnGuard events with an OnGuard door or a non-door input as the source aren't reported with the correct timezone in Security Desk.
4416713	Lenel Open Access logs show errors when all cardholder fields are removed from a credential using the Lenel FormsDesigner configuration tool.

Known issues

The OnGuard plugin 5.2.2 includes the following known issues.

Issue	First reported in	Description
4503466	5.2.1	Live events in the *Monitoring* task are reported with the OnGuard server timezone instead of Security Desk timezone.
3255029	5.1.0	If a reader or alarm sub-panel goes offline in OnGuard, their parent panel in Security Center doesn't show a yellow warning state.
3240116	5.1.0	The **Occurrence period** field always shows events as **Online** in *Monitoring* and reports tasks regardless of the actual status.

Related Topics

Integration overview on page 4

Limitations

The OnGuard plugin 5.2.2 includes the following known limitations.

Issue	First reported in	Description
4663650	5.2.2	The proxy could take five minutes or more to recognize when the OpenAccess API service disconnects on the server. The proxy still shows a **Connected** status in the plugin role during this time.
4321331	5.2.0	OnGuard 5.2.2 doesn't support connecting the proxy to a filepath located in a mapped drive. The action fails with an `invalid filepath` error.
3297892	5.1.0	Sending an OpenDoor command from Security Center to the OpenAccess API returns an *Open Door Command* event only after the door is relocked.
3244200	5.1.0	It can take up to 30 seconds for the OnGuard system to detect a disconnection with the OnGuard proxy. Security Center doesn't receive events that occur during that time. This causes a mismatch between the events sent from OnGuard and those received by Security Center.
2990244	5.1.0	When the synchronization of a Bosch intrusion panel occurs in OnGuard, the OnGuard system and the OpenAccess API crash. **Workaround:** In your OnGuard system, mark Bosch panels as disabled to avoid synchronization.
2989689	5.1.0	If the status of a panel changes, its status is updated in Security Center. However, the running state of inputs and outputs on the panel isn't updated in Security Center until a synchronization occurs.
2989278	5.1.2	The **State** field in the Global Cardholder Synchronizer role *Peripherals* page and *System status* task remains empty for OnGuard intrusion inputs.
2975439	5.1.0	Redefining the predefined cardholder field types using the FormsDesigner app from OnGuard isn't supported.
2632671	5.1.0	Cardholder pictures aren't recompressed when imported into the Security Center Directory database from OnGuard. Host the Directory database on an SQL Standard Server or better if cardholder pictures are large, or if large volumes of cardholder pictures are being imported from the OnGuard system.
2563421	5.0	Visitors aren't supported through Federation™. As a result, visitor activities on federated sites can't be reported.
370910	4.0	When a cardholder opens and closes doors, the door status doesn't change in the Security Desk door widget.
370877	4.0	The armed or disarmed status of an intrusion detection area isn't available in the Security Desk widget.
340486	4.0	If any alarms are modified in the OnGuard system using the Active alarm checkbox, the changes aren't reflected in Security Center. **Workaround:** Restart the proxy service and the OpenAccess service.

Related Topics

Integration overview on page 4

Product compatibility

To be eligible for technical support, you must install the plugin with versions of Security Center and third-party software that are certified or supported by design.

For the latest compatibility information, see Supported plugins in Security Center on the Genetec™ TechDoc Hub.

On sites with large cardholder pictures or large volumes of cardholder pictures, the Security Center Directory database should be hosted on a SQL Standard Server or better to ensure Directory operation is not impaired due to maximum database size limits.

Related Topics

Integration overview on page 4
License options on page 14

System requirements

To ensure that the OnGuard plugin 5.2.2 performs as expected, the plugin must be installed on a computer that meets the recommended specifications for Security Center.

Refer to the *server requirements* and *client workstation requirements* topics in the Security Center system requirements for the version of Security Center that you are using.

On sites with large cardholder pictures or large volumes of cardholder pictures, the Security Center Directory database should be hosted on a SQL Standard Server or better to ensure that Directory operation is not impaired due to maximum database size limits.

On sites with large volumes of offline events (3 million or more), the proxy service should be installed on a workstation running a 64-bit operation system.

Related Topics

Integration overview on page 4

License options

Before installing the plugin, you must update your Security Center license to include a certificate for the plugin. To update your license, contact us and provide the part numbers listed in this topic.

Genetec Inc. license

Part number	Description	Requirements
GSC-1PLEN	• You need one license part for every 750 OnGuard readers.	• Synergis™ Professional or Enterprise • Omnicast™ Professional or Enterprise

NOTE: You can verify the number of readers being used on the *About* tab of the plugin role in Config Tool.

OnGuard license

To connect the OnGuard plugin to the OnGuard system, you must obtain a LenelS2 OnGuard API annual license for your OnGuard system.

IMPORTANT: The DataConduIT license part that was used for OnGuard 4.0 cannot be used for OpenAccess. You must obtain the OpenAccess license part.

OnGuard part number	Description	Requirements
IPC-011-GENTC01	LenelS2 OnGuard API annual license.	For more information, contact your LenelS2 value added reseller.

Does your Security Center license include all the options you need?

In addition to a certificate for your plugin, ensure that your Security Center license includes all the options you expect to use in Security Center. If an option is missing, an error message is displayed when the server tries to create or modify the entity related to that option.

For a list of available license options, see License options in Security Center.

Related Topics

Integration overview on page 4
Product compatibility on page 12

Supported features

Discover the features that are supported by Security Center for an integration with OnGuard.

For a list of features supported by your plugin, download the feature comparison PDF from the TechDocs Hub.

Feature comparison for access control plugins

Related Topics

Integration overview on page 4

Supported devices

The OnGuard plugin 5.2.2 supports devices that can be registered using one of the OnGuard entity types listed below.

- Lnl_AlarmInput
- Lnl_AlarmOutput
- Lnl_Panel (access control and intrusion detection only)
- Lnl_Reader
- Lnl_ReaderInput1
- Lnl_ReaderInput2
- Lnl_ReaderOutput1
- Lnl_ReaderOutput2
- Lnl_IntrusionDoor
- Lnl_IntrusionZone
- Lnl_OnboardRelay
- Lnl_OffboardRelay

Related Topics

Integration overview on page 4

Synchronized entities and properties

It is important to know which entities and related properties can be synchronized by the OnGuard plugin.

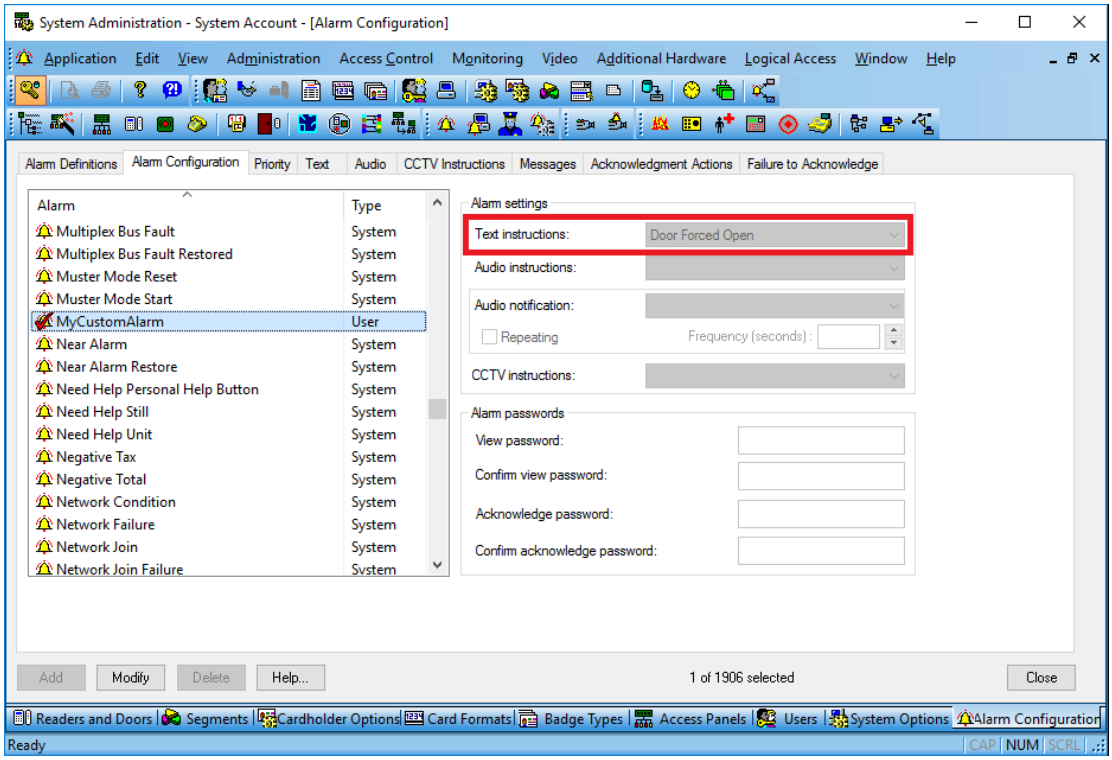
The following table lists entities and properties that are synchronized in Security Center and whether or not they are automatically synchronized in real time.

NOTE:

- Cardholder groups and partitions in Security Center are not synchronized with OnGuard.
- Cardholder and visitor entities and their related properties are synchronized in real time.
- Custom fields in cardholder profiles are overwritten when a synchronization occurs.
- There are many types of panels in OnGuard, the plugin only synchronizes access control unit and intrusion detection panels.
- For each reader in OnGuard, one reader and one door entity is created in Security Center.
- Modifications to the names of OnGuard panels or devices are automatically pushed to Security Center when a synchronization occurs.

IMPORTANT:

- The default proxy setting for polling the hardware status of OnGuard devices is False, which can cause incorrect device status reports after a manual synchronization.
- In order for entities to be updated automatically, you must enable live synchronization.
- For entities that cannot be updated automatically, you must perform a manual synchronization.
- After Security Center and OnGuard are initially connected, a manual synchronization is required to pull entities from OnGuard to Security Center.
- When hardware is deleted in the OnGuard system, a manual synchronization is required in order to delete the associated entities in Security Center.
- In order to receive cardholder updates, you must select the **Generate software events** option on the OnGuard system. This is found on *System options* form in the *System Administration* task.
- In the OnGuard System Administration application, user created alarms must have the "Text instructions" setting configured to be synchronized through the OnGuard plugin integration.



OnGuard entity	Security Center entity	Properties that are synchronized	Properties can be synchronized automatically
Lnl_Cardholder	Cardholder	All related properties	Yes
Lnl_Visitor	Visitor	All related properties	Yes
Lnl_Panel	Access Control unit or Intrusion detection unit	• AC and battery state • Tamper state • Running state	Yes
Lnl_Reader	Reader and Door	• Door open and door lock state based on event. • Running state based on event.	Yes
Lnl_ReaderInput1	Input	• Input state • Running state based on event.	Yes
Lnl_ReaderInput2	Input	• Input state • Running state based on event.	Yes
Lnl_ReaderOutput1	Output	• Output state	Yes
Lnl_ReaderOutput2	Output	• Output state	Yes
Lnl_Area	Area	• Name • Area type	No
Lnl_IntrusionDoor	Door	• Name	Yes
Lnl_IntrusionArea	Intrusion Area	• Name	No
Lnl_IntrusionZone	Input	• Running state based on event.	Yes
Lnl_AlarmDefinition	Alarm	• Name • Description • Priority	No
Lnl_AlarmInput	Input	• Input state • Running state based on event.	Yes

OnGuard entity	Security Center entity	Properties that are synchronized	Properties can be synchronized automatically
Lnl_AlarmOutput	Output	• Output state • Running state based on event.	Yes
Lnl_OnboardRelay	Alarm Panel Output	• Name • Output state	Yes
Lnl_OffboardRelay	Alarm Panel Output	• Name • Output state	Yes

Related Topics

Starting a manual synchronization on page 52

Custom events added by the OnGuard plugin

Events that are configured in your OnGuard system are imported as custom events in Security Center when a synchronization occurs. Therefore, the list of custom events is different for each installation.

Custom events can be used as query filters in activity reports or to create event-to-actions.

Related Topics

Integration overview on page 4

3

Deploying the OnGuard plugin

This section includes the following topics:

- "Ports used by the OnGuard plugin" on page 22
- "Upgrading" on page 23
- "Downloading and installing the plugin" on page 26
- "Performing a silent installation of the plugin" on page 28
- "Required privileges" on page 30
- "Creating the plugin role" on page 33
- "Scheduling database backups and cleanups" on page 34

Ports used by the OnGuard plugin

Before installing the OnGuard plugin, you must ensure that the required ports are open on all network switch routers and firewalls, and that no other applications are using these ports.

Ports used by the plugin

Application	Inbound	Outbound	Configurable	Port usage
Plugin role		1312/TCP	Yes	Connection to the proxy service.

NOTE: Port 1312 is the default port used by the proxy. It can be changed in the configuration page of the proxy.

Ports used by the proxy service

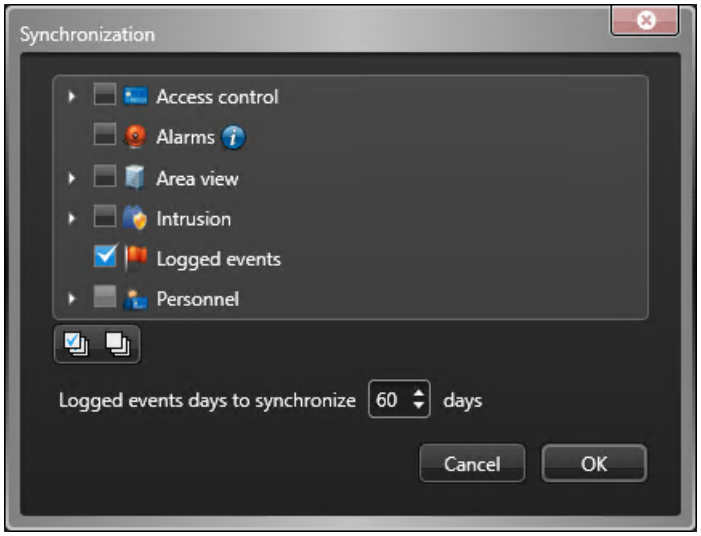
Application	Inbound	Outbound	Configurable	Port usage
Plugin role	1312/TCP		Yes	Connection from the plugin role.
Proxy communication		8080/TCP	Yes	Connection to OnGuard OpenAccess API.

Upgrading

To upgrade theOnGuard plugin to version 5.2.2, follow one of the procedures indicated here, depending on which version you are upgrading from.

Before you begin

1. Add the LenelS2 OnGuard API license to the OnGuard server license.
   IMPORTANT: If the license is not added, the OnGuard plugin 5.1.0 is unable to connect to the OpenAccess API. The OnGuard plugin 5.1.0 does not communicate using the DataConduIT API used by the OnGuard plugin 4.0. To verify the license part required, see the license requirements.
2. Back up the Directory and plugin databases.
   IMPORTANT: The information in the plugin database is lost during the upgrade. Following the upgrade, you can recover up to 365 days' worth of data by manually synchronizing the logged events from the OnGuard system. It is recommended that you recover the same amount of data that you typically retain because the retrieval process can be long, can drive up CPU use, and can impact your system. In addition, during this process, you cannot receive feedback about the percentage of data recovered, time, etc.

   Data (stored as journal logs) that is older than 365 days remains in the backup, but you cannot access the data using the reporting tools in Security Center.
3. Read the release notes to learn about important information for this release.
4. Confirm that your versions of Security Center, the OnGuard, and the plugin are compatible.

What you should know

- The Directory database contains all your entities. An upgrade from version 4.x or later keeps all existing entities, including events-to-action and map positioning.
- The plugin package must be upgraded on all Security Center client and server computers.
- For versions earlier than 5.0, the plugin role configuration cannot be migrated and is lost during the upgrade. After installation, you must reconfigure your plugin settings.

Procedure

- Do one of the following:
  - Upgrade from version 5.x.x.
  - Upgrade from version 4.x.
  - Upgrade from version 3.x.

Related Topics

Starting a manual synchronization on page 52

Upgrading from version 5.x.x

You can do a full upgrade of the OnGuard plugin from any 5.x version directly to version 5.2.2.

Procedure

1 Deactivate the plugin role.
2 Stop the Genetec™ Server service, and close Security Desk and Config Tool.
3 If you have made changes to any configuration files, back up the files elsewhere on the system.
4 Install the latest version of the plugin.
5 Activate the plugin role.
6 Using Windows Explorer, delete the file *C:\ProgramData\Genetec\OnGuard\EventMappingConfiguration.json* on the proxy server.

NOTE: If you do not delete this .json file, Security Center cannot raise any events added in the upgraded version.

7 Restart the proxy server.

NOTE: a new .json file is automatically created on startup.

8 If you backed up your configuration files in step 3, compare the files and manually reapply your changes.

The plugin is ready for use.

After you finish

- Verify your proxy configuration.

Upgrading from version 4.x

You can do a partial upgrade of the OnGuard plugin from version 4.0 directly to version 5.2.2.

Procedure

1 Deactivate the plugin role.
2 Stop the Genetec™ Server service, and close Security Desk and Config Tool.
3 From the Windows **Program and Features**, uninstall the plugin.
4 Install the latest version of the plugin.

5 In the *Resources* tab of the plugin, do the following:
   a. From the **Database server** list, select the server that you created the new plugin role database on.
   b. From the **Database** list, select a new database to use with the plugin role.
      NOTE: Due to changes in the database format, the existing plugin role database cannot be used after the upgrade.
   c. Click **Apply**.
6 Activate the plugin role.
   The plugin is ready for use.

After you finish

- Configure the proxy.

Upgrading from version 3.x

To upgrade the OnGuard plugin from version 3.x to version 5.2.2, you must copy your configurations and manually recreate the role because of major architecture changes between versions 3.x and 4.0.

What you should know

Changes in the plugin make it impossible to upgrade existing configurations from versions earlier than 4.0.

Procedure

1 Take notes and screenshots of your plugin configuration.
2 Deactivate the plugin role.
3 Stop the Genetec™ Server service, and close Security Desk and Config Tool.
4 Install the latest version of the plugin.
5 On your database server, create the database for the plugin role to use.
   IMPORTANT: To avoid overwriting your backup database, use a name that is different from the name of the database in the previous plugin version.
6 Create a new plugin role using the configuration notes you took in step 2.
7 When the integration using the new plugin works as expected, delete the version 3.x plugin role.
   The plugin is ready for use.

After you finish

- Configure the proxy.

Downloading and installing the plugin

To integrate OnGuard into Security Center, you must install the OnGuard plugin on a Security Center server and on all client workstations.

Before you begin

Ensure the following:

- Your server meets the recommended system requirements.
- A compatible version of Security Center is installed.
- Add the OpenAccess API license to the OnGuard server license.
- Install and configure the OpenAccess service on your OnGuard server.

What you should know

- Although it is possible to host the plugin role on any server, it is best practice to host that role on a dedicated expansion server for best system performance.
- For your operators to have access to the features of this plugin, you must install this plugin on all Security Center client workstations.

Procedure

1 Open the GTAP Product Download page.

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

3 Search for your package by name and download it.

4 Click the downloaded *.exe* file to unzip it.
By default, the file is unzipped to *C:\Genetec*.

5 Stop all Genetec applications, including Genetec™ Server, Security Desk, and Config Tool.

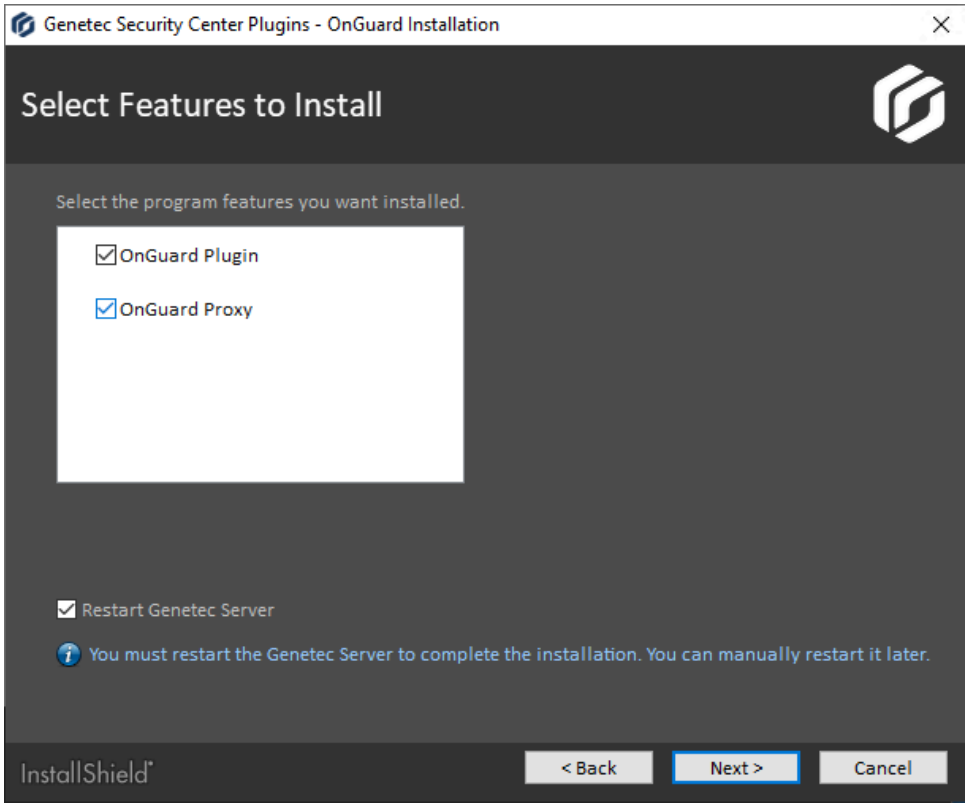
6 Stop the Genetec™ Server service.

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

8 Follow the installation instructions.

9 On the *Select Features to Install* page, select both the **OnGuard Plugin** and **OnGuard Proxy**.

NOTE: The proxy is required to connect the plugin to the OpenAccess API.



10 On the *Proxy Server Password* page, enter the password that will be used to connect from the plugin to the OnGuard proxy server.

Take note of this password, as it is required to configure the proxy.

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

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

After you finish

Create the OnGuard plugin role.

Related Topics

Integration overview on page 4
Configuring the proxy service on page 44

Performing a silent installation of the plugin

You can automate the process of installing the OnGuard plugin by installing it in silent mode.

Before you begin

- Read and understand Downloading and installing the plugin.
- Ensure the following:
  - Your server meets the recommended system requirements.
  - A compatible version of Security Center is installed.
- Create a folder for the log files on your local machine, for example, `C:\Genetec\Logs`

What you should know

- A silent installation installs the plugin using its default settings, without user interaction.
- Silent installations are ideal for deploying the plugin package to Security Center client workstations because the plugin package is necessary for plugin-specific functions to work in Security Desk and Config Tool.

Procedure

1 Open the GTAP Product Download page.

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

3 Search for your package by name and download it.

4 Click the downloaded *.exe* file to unzip it.
By default, the file is unzipped to *C:\Genetec*.

5 In Windows, right-click the **Command Prompt**, and then select **Run as administrator**.

6 In *Command Prompt*, navigate to the directory with the *.exe* file:
`cd C:\Genetec\OnGuard_vx.x.x_bxx.0\OnGuard Packages`, where `OnGuard_vx.x.x_bxx.0` corresponds to your version.

7 Enter the command for one of the following use cases, where `<file path>` is the path to the folder you created:

IMPORTANT: Enter the commands without line breaks or hard returns except at the end of the line.

- For Security Center client workstations and servers using the client applications, and servers used to host the plugin role, install the plugin only:

```
"Genetec OnGuard Setup.exe" /silent /DebugLog"<file path>\debug.log" /
log"<file path>\" /ISFeatureInstall=Plugin ISInstallDir_OnGuard="C:\Program
 Files (x86)\Security Center Plugins\OnGuard" RESTART_GENETEC_SERVER=1
```

NOTE: For OnGuard plugin version 5.1.0 and lower, the plugin-only command installs both the plugin and proxy.

- For a server intended to host the proxy service, install a proxy only:

```
"Genetec OnGuard Setup.exe" /silent /DebugLog"<file path>\debug.log" /
log"<file path>\" /ISFeatureInstall=Proxy ISInstallDir_OnGuard="C:\Program
 Files (x86)\Security Center Plugins\OnGuard" PROXYPASSWORD=<password>
 RESTART_GENETEC_SERVER=1
```

- For a server intended to host the proxy service, and to act as a Security Center client workstation and server, install the plugin and proxy:

```
"Genetec OnGuard Setup.exe" /silent /DebugLog"<file path>\debug.log" /
log"<file path>\" /ISFeatureInstall=Plugin,Proxy ISInstallDir_OnGuard="C:
\Program Files (x86)\Security Center Plugins\OnGuard" PROXYPASSWORD=<password>
 RESTART_GENETEC_SERVER=1
```

When the installation is complete, Security Center restarts.

NOTE: If you do not want the Genetec™ Server to restart immediately after the silent install, omit the command `RESTART_GENETEC_SERVER=1`. In this case, the plugin is not available until you manually restart the Genetec™ Server.

The plugin is ready for use.

After you finish

(Optional) If you need to do a silent uninstall, do steps 5 and 7, and enter the following command in step 7:

```
"Genetec OnGuard Setup.exe" /silent /DebugLog"<path to log file>\<log filename>" /
log"<path to log files>\" -remove
```

Required privileges

For administrators to install and configure the plugin in Config Tool, and for operators to monitor the OnGuard in Security Desk, the correct user privileges must be granted to their user accounts.

Privileges added by the OnGuard plugin

The following table lists the privileges added to Security Center when the plugin is installed. If these privileges are missing from the privileges list, the plugin is not installed on your local computer.

Although every company's organization is unique, we typically assign Config Tool and Security Desk privileges to users who install the plugin and set up the Security Desk workstations for operators. Operators are usually granted access to Security Desk privileges. Some privileges are required by all users.

Privilege	Description	Application	User role
Access control and intrusion detection units			
Set clock	Allows the user to set the clock on access control and intrusion detection units.	CT	Admin
Download database	Allows the user to download the database of access control and intrusion detection units that are connected to OnGuard.	CT	Admin
Download firmware	Allows the user to download firmware for access control and intrusion detection units that are connected to OnGuard.	CT	Admin
Reset use limit	Allows the user to reset the use limit of access control and intrusion detection units that are connected to OnGuard.	CT	Admin
Connect	Allows the user to connect to access control and intrusion detection units.	CT	Admin
Disconnect	Allows the user to disconnect from access control and intrusion detection units.	CT	Admin
Cardholders			
Deactivate OnGuard cardholder	Allows the user to deactivate cardholders.	CT, SD	All
Intrusion areas			
Arm/disarm	Allows the user to arm or disarm intrusion areas.	CT, SD	All
Silence alarms	Allows the user to silence alarms in intrusion areas.	CT, SD	All
Inputs and outputs			
Activate/deactivate/pulse/ toggle outputs	Allows the user to activate, deactivate, pulse, or toggle outputs on hardware devices that are connected to OnGuard.	CT, SD	All

Privilege	Description	Application	User role
Bypass/unbypass inputs	Allows the user to bypass or unbypass inputs on hardware devices that are connected to OnGuard.	CT, SD	All
Mask/unmask inputs	Allows the user to mask or unmask inputs on hardware devices that are connected to OnGuard.	CT, SD	All
Readers and doors			
Open	Allows the user to open doors that are connected to OnGuard.	CT, SD	All
Set reader/door mode	Allows the user to set the reader or door mode on readers or doors that are connected to OnGuard.	CT, SD	All
Set biometric verify more	Allows the user to set the biometric verify mode on readers or doors that are connected to OnGuard.	CT, SD	All
Set first card unlock mode	Allows the user to set first card unlock mode on readers or doors that are connected to OnGuard.	CT, SD	All
Download firmware	Allows the user to download firmware for readers or doors that are connected to OnGuard.	CT, SD	All

Legend for applications:

- **SD:** Security Desk
- **CT:** Config Tool

Privileges common to all plugins and extensions

Administrators have access to all privileges. However, if you create a user account from the Provisioning template and you want this user to add and configure your plugin, that user needs the following Security Center privileges.

Privilege	Description	Application	User role
Plugins	Allows the user to run the Plugins task.	CT	Admin
View license	Allows the user to view the Security Center license.	CT	Admin
View role properties	Allows the user to view role properties.	CT	Admin
Modify role properties	Allows the user to modify role properties.	CT	Admin
Add roles	Allows the user to add roles.	CT	Admin
Delete roles	Allows the user to delete roles.	CT	Admin
View server properties	Allows the user to view server properties.	CT	Admin
Modify custom field definitions	Allows the user to add, modify, and delete custom field definitions and custom data types.	CT	Admin

Privilege	Description	Application	User role
Modify custom events	Allows the user to add, modify, and delete custom events.	CT	Admin
Modify event-to-actions	Allows the user to add, modify, and delete event-to-actions.	CT	Admin

General privileges

Application privileges grant access to the Security Center applications.

Privileges	Description	Application	User role
Print/export reports	Allows the user to print and save reports to files.	SD	All
Remove entries from a report	Allows the user to remove selected entries from reports in Security Desk.	SD	Admin
Report incidents	Allows the user to report incidents in Security Desk.	SD	Integrator, Operator
Modify reported incidents	Allows the user to modify incident reports and incident packages in Security Desk.	SD	Admin

Security Center access control privileges

Search for all "access control" privileges. Go through the list and grant or deny access as required for each user.

Security Center video privileges

The OnGuard plugin uses cameras and video. Search for all "video" privileges. Go through the list and grant or deny access as required for each user.

Security Center asset management privileges

The OnGuard plugin is used to manage assets. Search for all "asset" privileges. Go through the list and grant or deny access as required for each user.

Related Topics

Integration overview on page 4

Creating the plugin role

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

Before you begin

Download and install the plugin.

Procedure

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

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

The plugin creation wizard opens.

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

If you do not use expansion servers in your system, the **Server** option is not displayed.

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

a) Enter the **Entity name**.

b) Enter the **Entity description**.

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

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

d) Click **Next**.

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

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

6 Click **Close**.

After you finish

In the *Resources* tab of the plugin, select the database server that will be used by the plugin role. If you are using SQL Server authentication to access the server, enter the user name and password.

Related Topics

Integration overview on page 4

Scheduling database backups and cleanups

It is important to protect your data by scheduling regular database backups. Also, regularly clean your database to remove old data so that the database does not grow beyond its capacity. If the database is full, your integration might stop working.

Before you begin

Ensure you have the following privileges:

- View role properties
- Modify role properties
- Administration > Plugins

What you should know

The plugin role database stores the following:

- Events that occur in the OnGuard system (timestamp of the event being raised, entities attached to the event, etc.)
- Active alarm triggers and those pending acknowledgment.

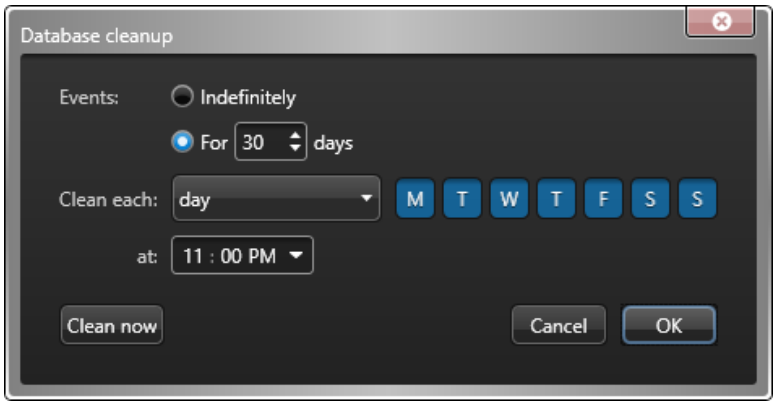
The Directory database stores the plugin configuration and related entity types.

Procedure

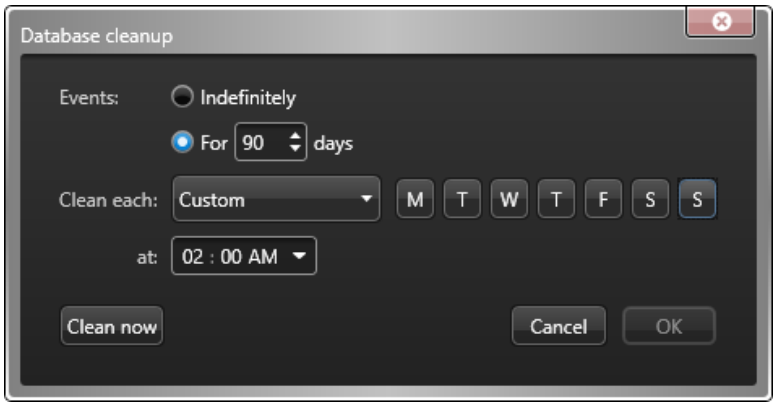
1 From the Config Tool homepage, open the *Plugins* task.

2 From the entity browser, select the OnGuard plugin role and click the *Resources* tab.

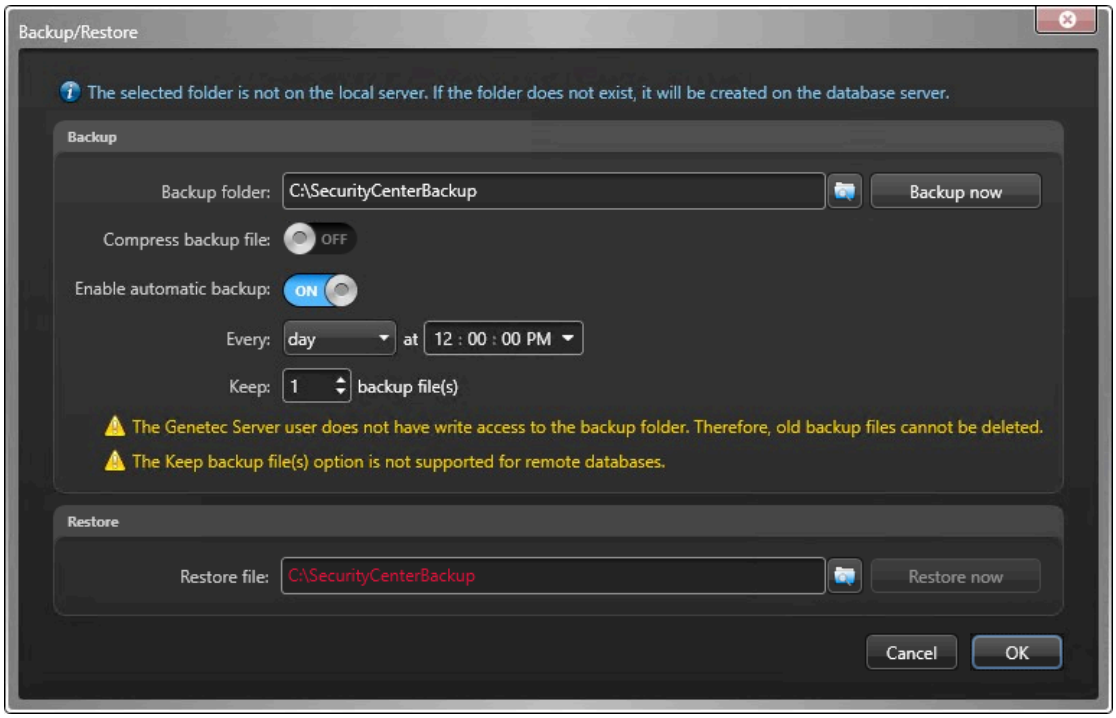
3 Click **Cleanup** (), choose how long to keep events and when to delete old data, and then click **OK**.



NOTE: By default, the **Keep data** setting is set to 30 days and the **Clean each** setting is set to **custom** and has no clean up day specified. This means that data will never be cleaned up unless you select a day on which it will occur.



4 Click **Backup/Restore** (), choose the location for backup files, enable automatic backups at least once per week, and then click **OK**.



5 Click **Apply**.

Related Topics

Integration overview on page 4

4

Setting up failover and Federation™

This section includes the following topics:

- "Enabling failover on the plugin role" on page 38
- "Enabling partial failover on the proxy " on page 40
- "Setting up Federation to monitor remote OnGuard entities" on page 41

Enabling failover on the plugin role

To improve the availability of your plugin role, you can add a secondary server on standby. If the primary server hosting the role becomes unavailable, the role is automatically transferred to the secondary server.

Before you begin

- Ensure that you have an expansion server available. To learn how to add expansion servers to your system, see the *Security Center Administrator Guide*.
- If your plugin role is hosted on the main server, move it to an expansion server. For more information, see "Moving roles to other servers" in the *Security Center Administrator Guide*.

  NOTE: If you must host the plugin role on the main server, you must also configure the Directory failover. For more information, see Directory failover and load balancing.
- Ensure that the plugin role and the plugin role database are not hosted on the same server. For more information, see Connecting roles to remote database servers.

TIP: You can access the *Security Center Administrator Guide* by pressing F1 in Config Tool.

What you should know

For more information, see Role failover.

IMPORTANT: Security Center does not handle the failover of role databases. For roles that connect to a database, the database server must be hosted on a third computer, separate from the servers hosting the role. All role servers must have read and write access to the database server. To protect your data, perform regular backups of the role database.

Procedure

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

2 From the entity browser, select the OnGuard plugin role and click the *Resources* tab.

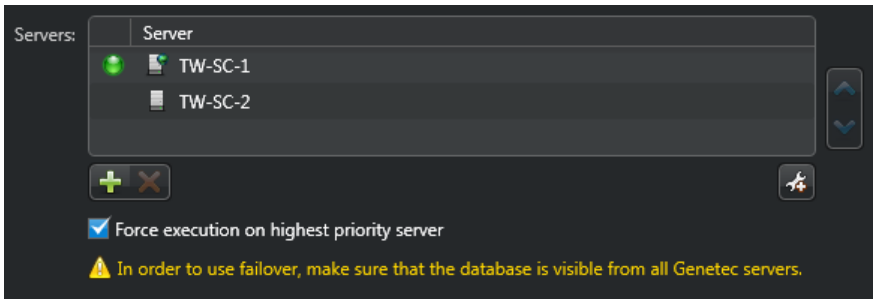
3 Under the **Servers** list, click **Add an item** ( ).

A dialog box opens, listing all remaining servers on your system that are not yet assigned to this role.

4 Select the server that you want to add as a secondary server and click **Add**.

The secondary server is added below the primary server. The green LED indicates which server is hosting the role.

NOTE: The servers are listed in the order that they are picked if a failover occurs. When the primary server fails, the role automatically switches to the next server on the list.



5 To change the priority of a server, select it from the list, and click the or buttons to move it up or down the list.

6 If you want the primary server to retake control after it is restored from a failover, select the **Force execution on highest priority server** option.

To minimize system disruption, the role remains on the secondary server after a failover occurs, by default.

7 Ensure that the role is not connected to a database on the local machine.

You can determine that the database server is local to your machine if the name of the **Database server** starts with "(local)". If it does, rename the database server to match the remote server you prepared in advance for your plugin role.

a) Back up your plugin role database and restore it on a server that is not hosting your plugin role.

b) Enable remote access to the plugin role database that you restored.

c) Change the **Database server** to the server hosting your plugin role database.

For example, `REMOTESERVER\SQLEXPRESS`.

8 Click **Apply**.

After you finish

If your parsers are deployed remotely, configure a proxy server to redirect traffic to the standby server.

Enabling partial failover on the proxy

To improve the availability of your plugin, you can add a secondary proxy server on standby. If the primary server hosting the proxy becomes unavailable, functionality is automatically transferred to the secondary server.

Before you begin

- Configure a secondary proxy service.
- Ensure that both proxy services have the startup type set to **Automatic** in the Windows *Services* application. For information, see Setting the startup type of a Windows service to Automatic.
- Ensure that both proxies have the same password configured.

What you should know

- Only partial failover is supported for the proxy service. The two proxies must not be active at the same time. There will be some downtime between stopping one proxy and starting the other.
- To enable partial failover for the proxy service, both proxies must have access to the folder containing the role's database and configuration files. This folder cannot be located in a mapped drive.

  IMPORTANT: To ensure the security of your system, only the users running the proxy service should have **Read/Write** permissions for this folder.
- This procedure must be applied to all the proxies on your system.

Procedure

1 In Windows, open the *Services* application.

2 Right-click on the proxy service and select **Stop**.

3 In Windows, right-click the **Command Prompt** program, and then select **Run as administrator**.

4 Run the following command, where `<folder where files are located>` is the file path to where your shared files are located :

```
sc.exe config Genetec.Plugins.OnGuardProxyService binPath="C:\Program Files
 (x86)\Security Center Plugins\OnGuard\Proxy\Genetec.Plugins.OnGuard.Proxy.exe /
filepath:\"<folder where files are located>\""
```

5 Start the proxy service.

6 Open the proxy web page and enter the OpenAccess password.

BEST PRACTICE: The OpenAccess password is only entered once when the failover is enabled. It isn't required to re-enter the password every time you open the proxy web page.

7 In Config Tool, open the *Plugins* task.

8 In the *Plugins* task, select the OnGuard plugin from the entity browser, and click the **Properties** tab.

9 Add your secondary proxy server.

Apply this procedure to all the proxies in your system.

Setting up Federation to monitor remote OnGuard entities

You can configure Federation™ host so that operators can monitor live events and generate reports for OnGuard entities.

Before you begin

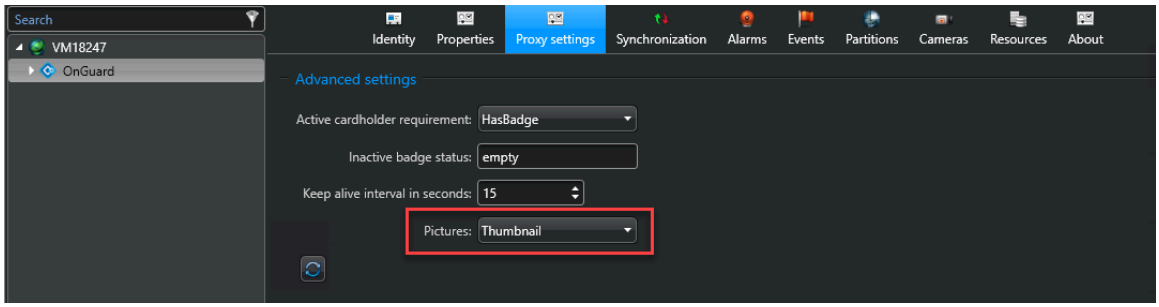
- Understand Federation™.
- Read the release notes to learn about known issues and limitations that affect the use of Federation™ for this plugin.

What you should know

- **WARNING:** If you are synchronizing cardholder pictures, you must confirm that the Federation host system's Directory database server is capable of holding all of the cardholder pictures. Failure to verify this capability before federating may result in system failure of the Federation host if the Directory database isn't able to contain all of the cardholder pictures.

  To ensure that the Directory database can contain all of the cardholders, do one of the following:

  - Upgrade the Federation host Directory to SQL Standard or better (SQL Express 2014 imposes a 10 GB database size limit).
  - Move all cardholders into a separate partition and create a Federation user that does not have access to the cardholder partition.
  - Synchronize OnGuard cardholder thumbnails instead of full pictures. This setting can be selected in the *Proxy settings* of the plugin.



- Federated sites require licenses for the readers on the site.
- When using Federation to generate reports from a remote system, the value of the **Source** field is left blank.
- Controlling the OnGuard entities from the Federation host in not supported.
- Commands that are added by the plugin can not be sent to federated systems. This includes things like setting clocks, downloading databases, setting reader modes, etc.

Procedure

1 Open Config Tool on the server that hosts Federation.

2 Add the OnGuard base license (part number GSC-1PLEN).

3 Install the OnGuard plugin.

4 Set up a Security Center Federation™. For more information, see the Federation™ chapter in the *Security Center Administrator Guide*.

Create a Federation role for each remote site that hosts the OnGuard plugin role.

5 Expand the Federation host role and confirm that the entities are listed in the entity browser.

6 If the entities are missing, restart the Main server for the Federation host.

7 In the **Monitoring** task, add entities to the event monitoring list.

The entities from federated sites appear in the entity browser.

5

Configuring the plugin

This section includes the following topics:

- "Configuring the proxy service" on page 44
- "Connecting to the OnGuard server" on page 46
- "Maintaining a connection between Security Center and OnGuard" on page 47
- "Selecting which cardholder information is sent through the proxy" on page 48
- "Enabling live synchronization of entities" on page 50
- "Starting a manual synchronization" on page 52
- "Configuring OnGuard plugin alarm settings" on page 54
- "Disabling OnGuard custom events in Security Center" on page 56
- "About linking cameras to OnGuard entities" on page 57
- "Linking Security Center cameras to OnGuard inputs" on page 59

Configuring the proxy service

To transfer information between Security Center and your OnGuard system, you must configure a proxy to connect the plugin to the OpenAccess API, which retrieves information from the OnGuard database.

Before you begin

- Download and install the OnGuard plugin.
- Obtain OnGuard user credentials which have access to the OpenAccess API and the necessary rights.

  NOTE: It is recommended that you perform tests using your system administrator account.

What you should know

- The proxy is installed as part of the plugin.
- The configuration page for the proxy opens in a web browser when the installation of the plugin is complete.

Procedure

1 In your web browser, open the proxy configuration page at *https://<IP address of the Security Center server hosting the plugin>:<Web server port>/config/*.

The default web server port is 1312.

NOTE: You must be a Windows administrator on the server that hosts the web page for the proxy.

2 In the *Third-party configuration* section, enter the following:

- **Endpoint:** The IP address and port number of the OpenAccess API. This is typically entered as *https://<IP address of the server hosting the OpenAccess API>:<Port used to communicate with OpenAccess API>*. For example, this could be *https://192.168.1.2:8080/*.
- **Username:** The username required to log into OpenAccess.

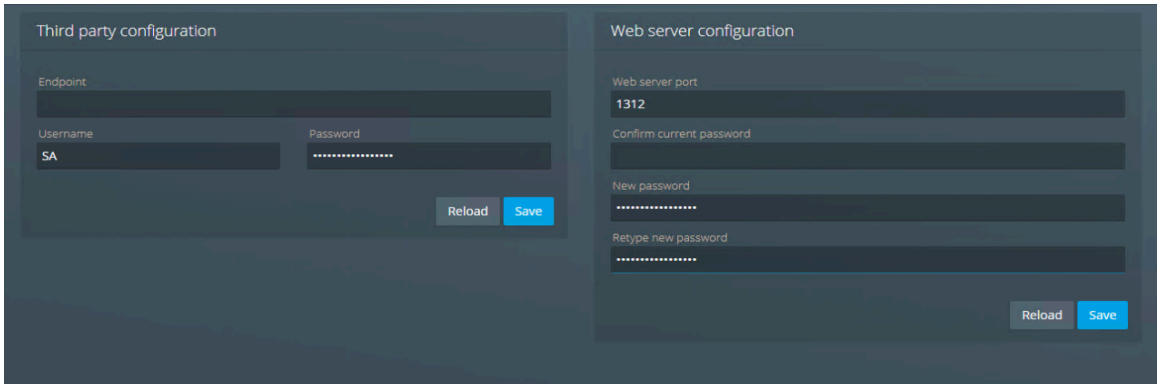
  NOTE: Do not include the domain name in the username. If you are using a Windows account, you must specify the directory this account belongs to in the *Proxy Settings* tab of the plugin role.
- **Password:** The password required to log into OpenAccess.

3 Click **Save**.

4 In the *Web server configuration* section, enter the following:

- **Web server port:** The port on which the proxy will host its web configuration server and its API. This API is used to communicate from the plugin to the proxy and request data from OpenAccess.
- **Password:** The password used to access the proxy. This is set during the installation process of the plugin.

IMPORTANT: The password configuration is stored in a *secret.key* file. The *secret.key* file is created automatically during the installation of the proxy. Deleting this file removes the password required to access the proxy and can cause security breach. To reset the password, uninstall and reinstall the proxy.



5 Click **Apply**.

NOTE: You may need to restart the proxy service in the Windows Services console for some changes to take effect.

After you finish

Connect the OnGuard plugin role to the OnGuard system.

Related Topics

Downloading and installing the plugin on page 26

Connecting to the OnGuard server

You must connect the OnGuard plugin role with the OnGuard system through the proxy to receive events and alarms in Security Desk.

Before you begin

- Configure the proxy.
- Unblock the web service port. This is 1312 be default, but may have been changed when configuring the proxy.

Procedure

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

2 In the *Plugins* task, select the OnGuard plugin from the entity browser, and click the **Properties** tab.

3 In the **Host** field, enter the IP address of the server that the proxy is hosted on.

4 In the **Port** field, enter the port that the proxy uses to communicate with OnGuard.

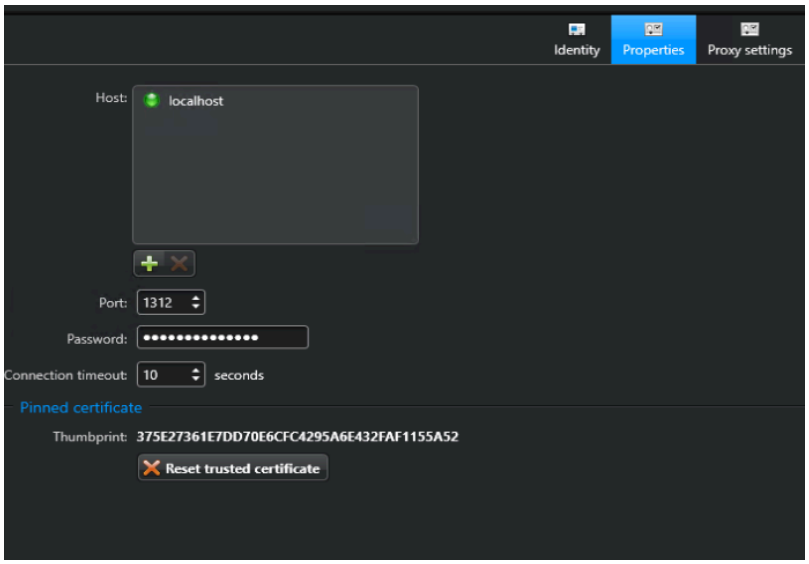
5 In the **Password** field, enter the password that you assigned to the web server.

NOTE: This password is initially set during the OnGuard plugin installation. To reset the password, uninstall and reinstall the proxy.

6 In the **Connection timeout** field, enter the amount of downtime, in seconds, before connecting to the next proxy on the list.

7 Click **Apply**.

After you connect to the proxy, the proxy automatically generates the certificate that is displayed in the *Pinned certificate* section. This certificate can be changed manually in the *OnGuardConfiguration.json* file, which is located in the *C:\ProgramData\Genetec\OnGuard* folder.



After you finish

Select the cardholder information that you want sent through the proxy.

Maintaining a connection between Security Center and OnGuard

To maintain communication with the OnGuard system, Security Center must regularly communicate with OpenAccess through the proxy.

Before you begin

Connect the OnGuard plugin role to the OnGuard system.

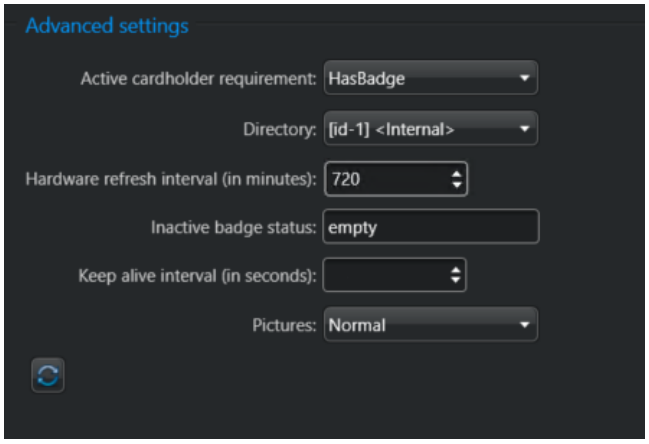
Procedure

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

2 Select the OnGuard plugin from the entity browser, and click the *Proxy settings* tab.

3 From the **Directory** list, select the directory that corresponds with the username and password that were entered in the proxy.

NOTE: If you are using OnGuard usernames (instead of usernames from a Windows or Active Directory account), select **[id]-1 <Internal>**.



4 In the **Keep alive interval (in seconds)** field, enter the time interval for the proxy to communicate with OpenAccess to maintain the connection between the two systems.

TIP: To avoid communication issues, it is recommended that you set this value to 840.

5 Click **Apply**.

After you finish

Select the cardholder information you want transferred between OnGuard and Security Center.

Selecting which cardholder information is sent through the proxy

After you connect the OnGuard plugin role to the OnGuard system, you must select which cardholder information is imported through the proxy.

Before you begin

Adjust settings to maintain a connection between Security Center and OnGuard.

What you should know

Redefining the predefined cardholder field types using the FormsDesigner app from OnGuard is not supported.

Procedure

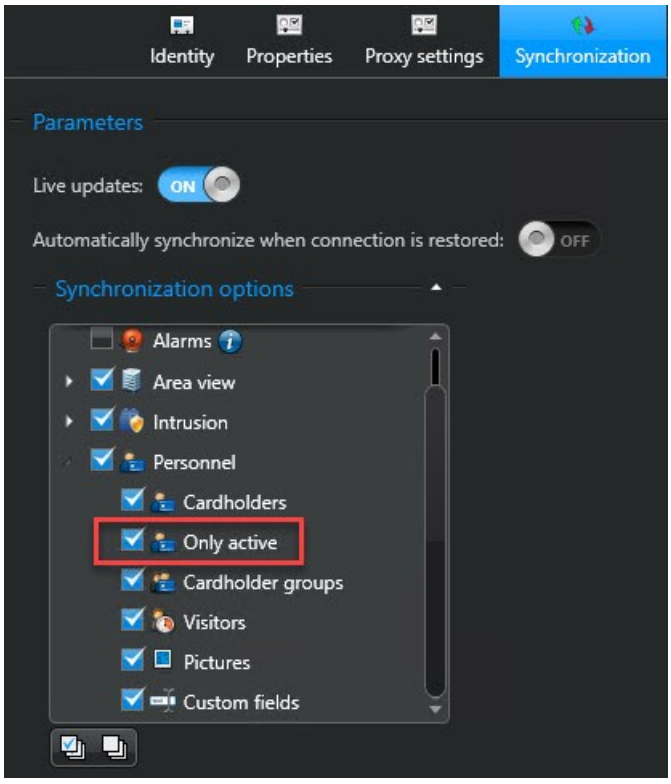
1 From the Config Tool homepage, open the *Plugins* task.

2 In the *Plugins* task, select the OnGuard plugin from the entity browser, and click the *Proxy settings* tab.

3 From the **Active cardholder requirement** list, select the type of cardholder that you want to import from OnGuard into Security Center. This can be one of the following:

- **HasActivatedBadge:** Synchronizes any cardholder that has an active badge.
- **HasBadge:** Synchronizes any cardholder that has a badge, regardless of whether it is active.

NOTE: For this feature to work, you must go to **Synchronization** > **Parameters** > **Synchronization options** and select the **Only active** option under **Personnel**.



4 In the **Inactive badge status** field, enter the term used to represent a deactivated badge in OnGuard.

This term is entered in the cardholder profile when it is deactivated in Security Center, so when a synchronization occurs, the OnGuard system can register the cardholder as inactive.

5 From the **Pictures** list, select whether you want to retrieve normal (full-sized) cardholder pictures or thumbnails through the proxy.

NOTE: To receive thumbnails, you must have the thumbnail option enabled in System Administration > Cardholder options > General Cardholder options > Multimedia > Create/save photo thumbnails.

IMPORTANT: Cardholder pictures imported from OnGuard are stored in the Security Center Directory database. Synchronizing large numbers of cardholder pictures can impair Security Center performance if the Directory database is not hosted on a SQL Standard server instance and the plugin server has insufficient resources. Before synchronizing cardholder pictures from OnGuard, the number of cardholders and average cardholder picture size and system resources must be taken into consideration.

6 Click **Apply**.

After you finish

Enable live synchronization of entities.

Enabling live synchronization of entities

For entities to be synchronized in real time between OnGuard and Security Center, you must enable live synchronization.

Before you begin

Connect to the OnGuard server.

What you should know

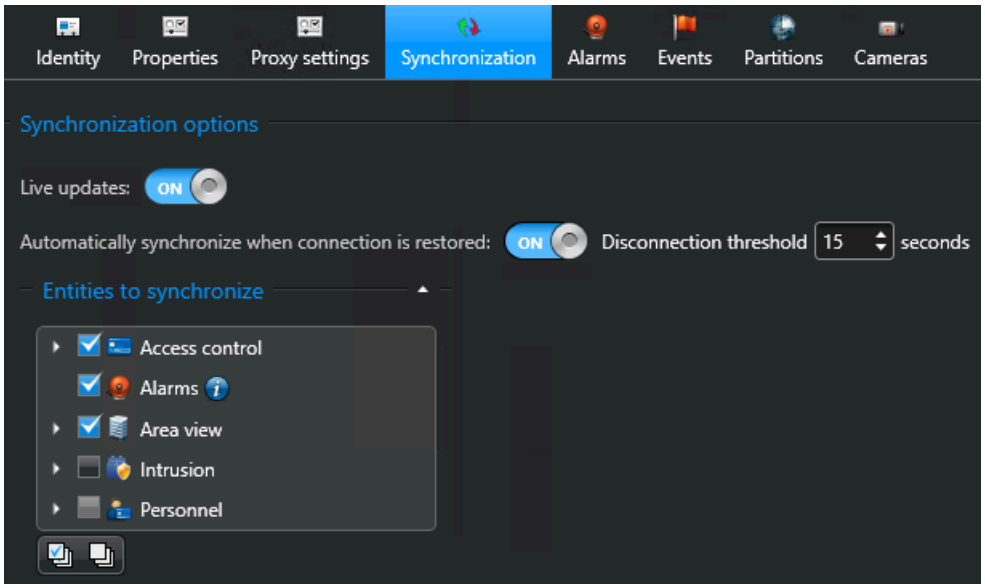
- When a panel or device is deleted in the OnGuard system, the changes are not automatically reflected in Security Center. To see the changes in Security Center, you must perform a manual synchronization.
- Disabling these options does not remove any of the entities that were previously added. Entities added by the plugin (except cardholders) can only be removed through the synchronization or on removal of the plugin role.
- To synchronize logged events, you must perform a manual synchronization.

Procedure

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

2 In the *Plugins* task, select the OnGuard plugin from the entity browser, and click the **Synchronization** tab.

3 In the *Synchronization options* section, move the **Live updates** slider to **ON**.



4 (Optional) To trigger a synchronization following a loss of connection between the OnGuard system in Security Center, in the *Parameters* section, move the **Automatically synchronize when connection is restored** slider to **ON**.

When this option is turned on:

- A full synchronization is done using the settings in the *Entities to synchronize* section when the plugin role first starts up and connects to the proxy.
- The **Disconnection threshold** option determines whether or not a full synchronization is triggered when the connection to the proxy is interrupted and restored. If the reconnection happens within the configured time-frame, it does not trigger a full synchronization. The default is 15 seconds.

5 In the *Entities to synchronize* section, select which types of entities that you want to synchronize in real time.

NOTE: Cardholder groups and partitions are not supported by the plugin.

6 Click **Apply**.

7 In the *Synchronized entities* section, click the refresh button () to view the number of entities from OnGuard that have been synchronized with Security Center.

The number of synchronized entities are displayed in the *Synchronized entities* section of the *Synchronization* screen.

After you finish

Configure the OnGuard plugin alarm settings.

Starting a manual synchronization

Cardholder and visitor changes made in OnGuard are automatically synchronized in Security Center. Changes to hardware devices are only reflected after a manual synchronization occurs.

Before you begin

Make sure that the plugin role is connected to the OnGuard server.

What you should know

- These settings only affect automatic synchronization and manual synchronization. Live updates done through real-time synchronization are unaffected by these options.
- When a manual synchronization is performed, the state of all inputs and outputs is displayed as **Unknown** in Security Center.
- Synchronizing the running state of alarm inputs and outputs from OnGuard to Security Center is not supported.
- For more information about which entities and properties are not automatically synchronized, see Synchronized entities and properties on page 17.

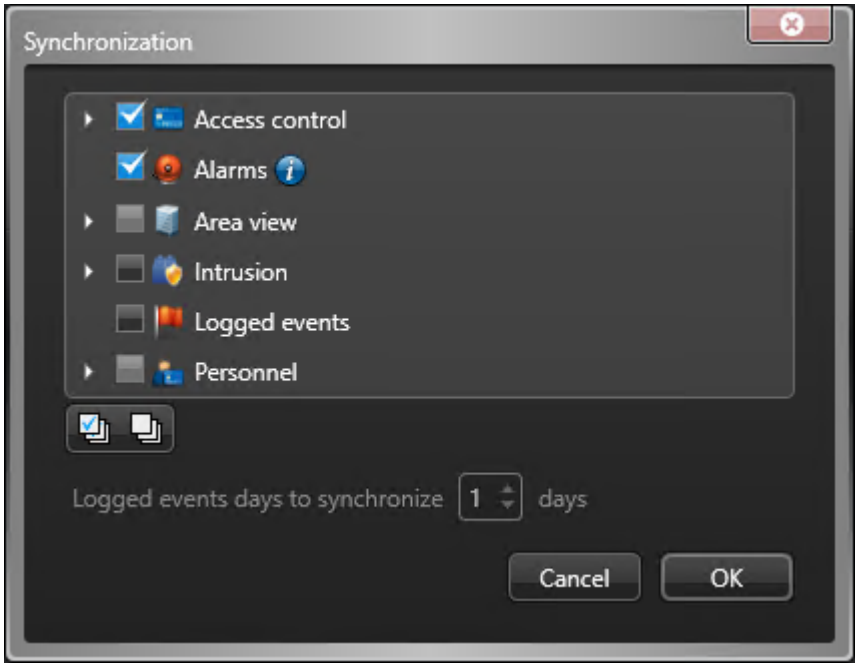
Procedure

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

2 In the *Plugins* task, select the OnGuard plugin from the entity browser, and click the *Synchronize* tab.

3 In the *Manual synchronization* section, click the **Synchronize** button.

4 In the **Synchronization** dialog box, select the entities and cardholders that you want to synchronize.



NOTE: The synchronization will take longer if you have a lot of cardholders.

5 Enter the number of days for which you want to synchronize logged events.

NOTE: Synchronizing the logged events will not recover the alarms that have been triggered and acknowledged in OnGuard while the proxy was offline. Only events are recovered.

6 Click **OK**.

The list of entities in the *Manual synchronization* section displays the entities that are synchronized.

After you finish

Configure your alarm settings.

Related Topics

Upgrading on page 23
Synchronized entities and properties on page 17

Configuring OnGuard plugin alarm settings

To receive alarms from the OnGuard access control system in Security Center, you must configure the alarm settings in the *Properties* tab.

What you should know

- The alarms listed on this page are imported from OnGuard.
- User-defined alarms are supported, but must have a text instruction applied in the OnGuard alarm definition in the OnGuard System Administration to be visible to the plugin. See the OnGuard OpenAccess documentation for more details.

Procedure

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

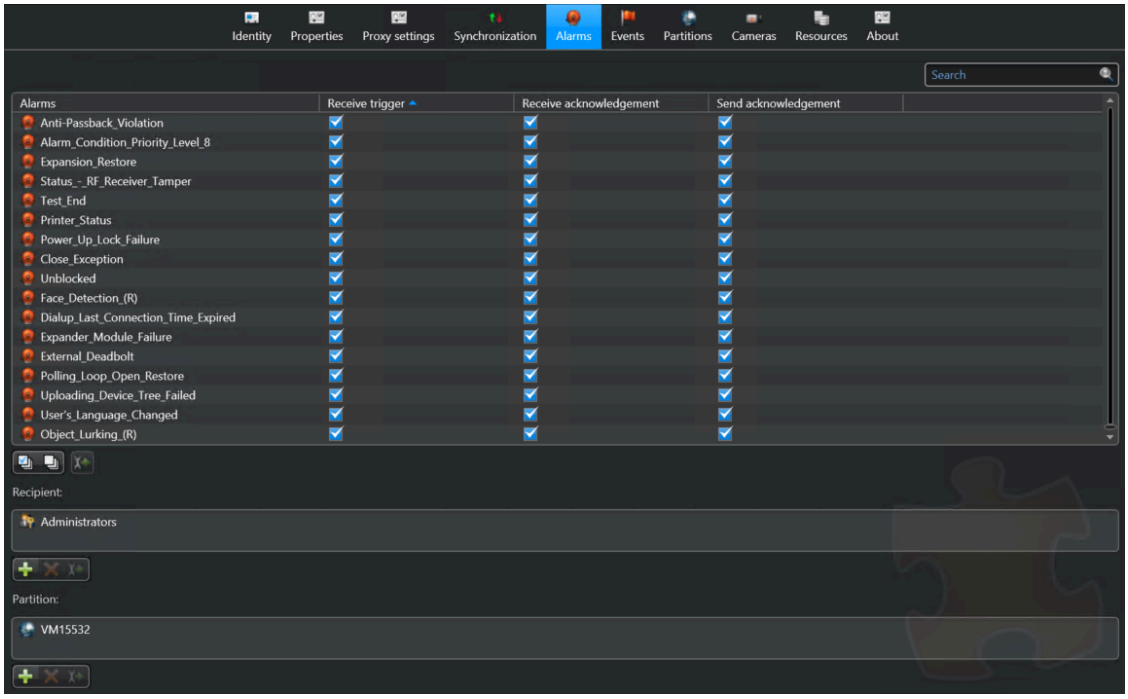
2 Select the OnGuard plugin from the entity browser, and click the **Alarms** tab.

3 In the list of **Alarms**, determine which action should take place for each alarm:

a) Check the **Receive triggered** box option to trigger an alarm in Security Center when the plugin receives a specific alarm from OnGuard.

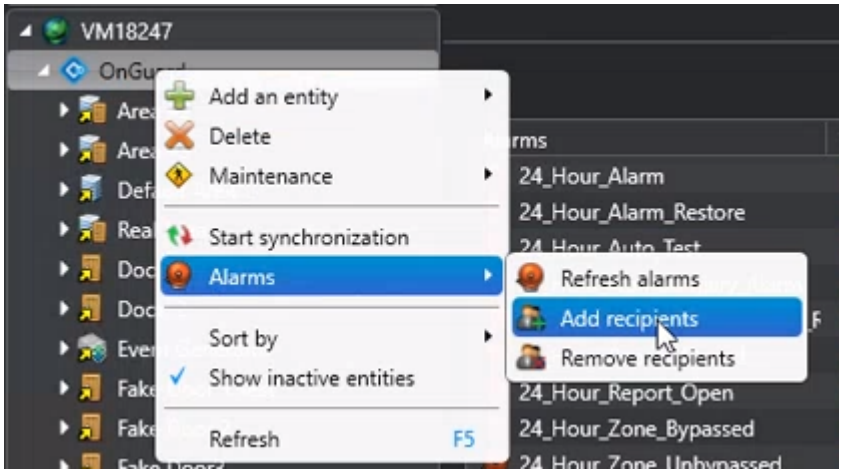
b) Check the **Receive acknowledge** box option to receive an acknowledgment in Security Center when an alarm is acknowledged in OnGuard.

c) Check the **Send acknowledge** box option to send an acknowledgment to OnGuard when an alarm is acknowledged in Security Center.



4 Beside **Recipients**, click ➕ to add which users or user groups are notified when alarms are triggered by the plugin.

NOTE: The recipients indicated in the **Recipients** list are only applied to alarms when the alarm entity is created by the plugin. To add recipients after the alarm was created, right-click on the plugin role and select **Alarms** > **Add recipients**.



5 Beside **Partitions** click ➕ to select which partitions you want the alarm entities to be added to when they are created by the plugin.

6 Click **Apply**.

After you finish

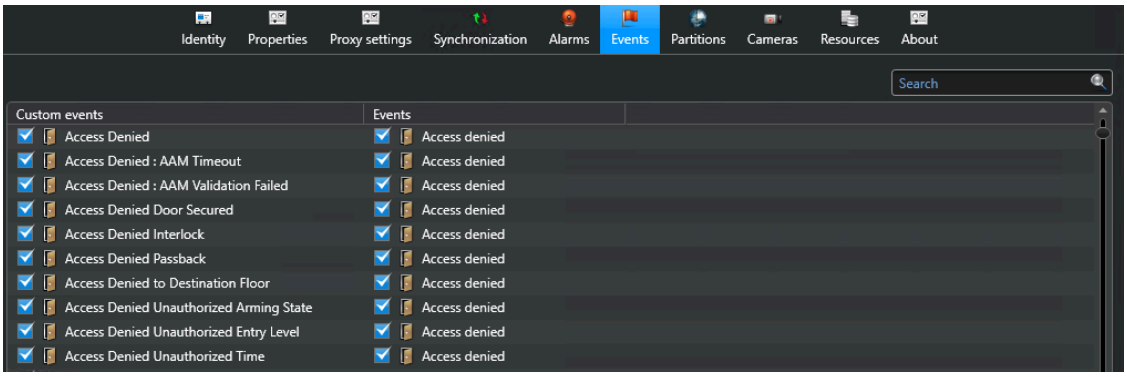
Disable the events that you do not want to see in Security Center.

Disabling OnGuard custom events in Security Center

If you do not want custom events to be triggered in Security Center when they are triggered in OnGuard, you can disable them in Config Tool.

What you should know

- All OnGuard hardware events creates custom events in Security Center. All the OnGuard custom events are enabled by default and will trigger events in Security Center when the corresponding events are triggered in OnGuard.
- The **Events** column in the *Events* tab indicates the Security Center event that is mapped to the custom event created by synchronizing with OnGuard. This provides the option to receive the custom event, Security Center event, or both when an event occurs in the OnGuard system.



- If you do not have a custom event or event checked, you will not receive a notification and the event that occurs will not be logged.

Procedure

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

2 In the *Plugins* task, select the OnGuard plugin from the entity browser, and click the **Events** tab.

3 Clear the checkboxes for the custom events that you do not want triggered in Security Center.

4 Click **Apply**.

The custom events you disabled from the list will not be triggered in Security Center when triggered in OnGuard, therefore they will not appear in the Monitoring task and in reports.

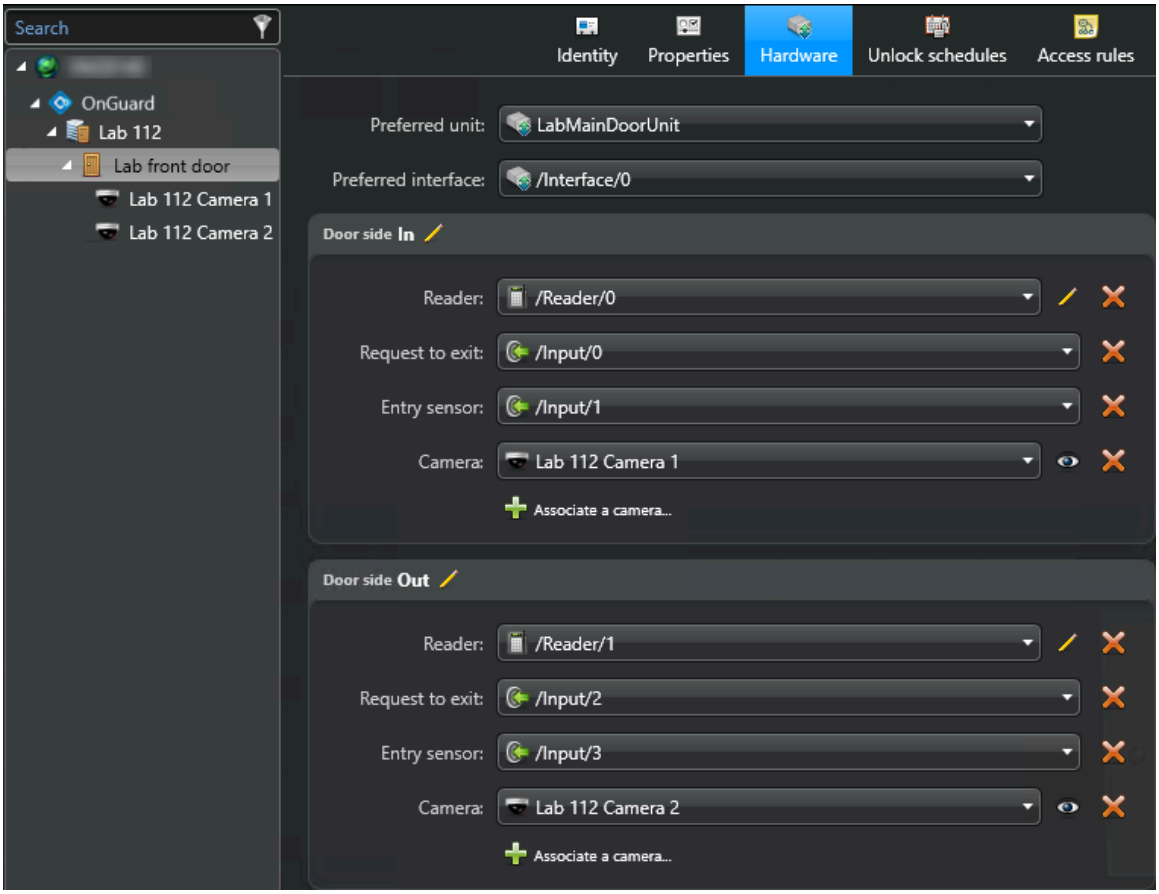
NOTE: For details about disabling native Security Center events in the *Monitoring task* see the *Security Center User Guide*.

About linking cameras to OnGuard entities

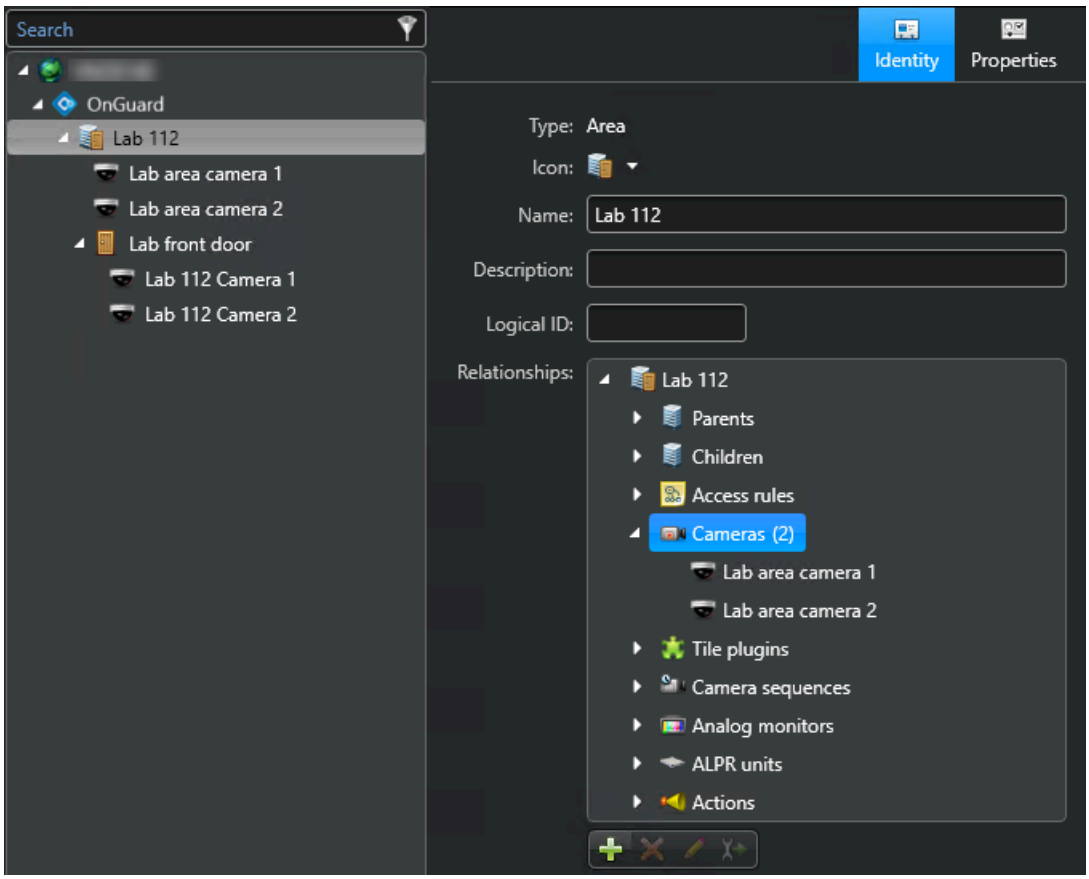
Linking Security Center cameras to entities makes it possible to view video feeds in the *Monitoring* task when an access control event occurs at an entity.

After you have added and configured cameras in Security Center, you can assign them to OnGuard entities such as elevators, floors, and areas in the *Area view* task.

- To assign a camera to a door, select a door and then associate a camera to it on the *Hardware* page.
  - For more information, see Assigning cameras to local doors. You can access this information by pressing F1 in Config Tool.



- To assign cameras to elevators, floors, areas, and intrusion detection areas, select an entity and access its configuration page.
  - For more information, see Common configuration tabs. You can access this information by pressing F1 in Config Tool.



- You can also link cameras to OnGuard inputs. The process is different for inputs than for native Security Center entities, like doors and elevators.
  - For instructions, see Linking Security Center cameras to OnGuard inputs on page 59.

Linking Security Center cameras to OnGuard inputs

You can link Security Center cameras to OnGuard inputs so that when an access control event occurs at the input, you can view the camera's video feed from the *Monitoring* task, *Alarm monitoring* task, and the *Alarm report* task in Security Desk.

Before you begin

Add and configure cameras in Security Center.

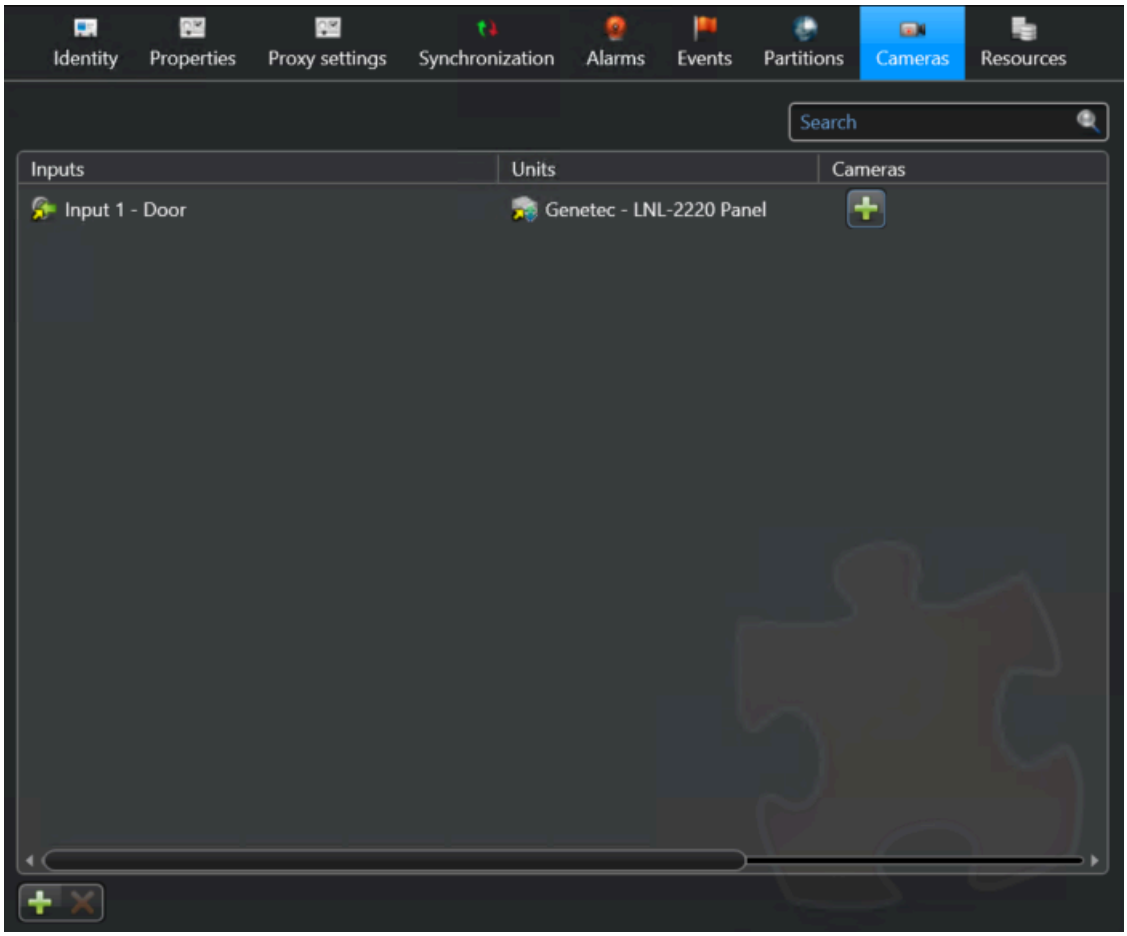
What you should know

- OnGuard inputs are imported by the plugin and are not native Security Center entities. For this reason, you must attach cameras to them from the OnGuard plugin role.
- You can view the states of inputs and outputs by selecting the OnGuard panel and then clicking on the *Peripherals* tab in Config Tool, or by using the *System status* task in Security Desk. The states are updated in real-time.
- You can assign a camera to an entity at any time, even after an event has occurred. When you double-click the event in the *Monitoring* task, you see the assigned camera's video.
- You can assign multiple cameras to the same input. Alarms include the video from **all** assigned cameras. However, events only include video from the **first** camera that was added to the input. So, when you double-click an event in the *Monitoring* task, you see the video of that first camera.

Procedure

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

2 In the *Plugins* task, select the OnGuard plugin from the entity browser, and then click the **Cameras** tab.
NOTE: You can search for cameras by camera name, input name, or unit name.



3 Click **Add** (), select one or more OnGuard inputs from the list, and then click **Select**.

4 Next to each input in the *Cameras* column, click **Add** (), select one or more cameras from the list, and then click **Select**.

5 Click **Apply**.

6 To view the camera's live video feed, click **Preview** ().

7 To configure the camera's settings, click **Open the camera's configuration page** ().

8 To remove a camera, click **Remove** ().

6

Monitoring OnGuard events

This section includes the following topics:

- "Contextual menu commands available for OnGuard entities" on page 62
- "How OnGuard alarms work with Security Center" on page 65
- "How OnGuard actions are triggered in Security Center" on page 66
- "Supported reports" on page 67

Contextual menu commands available for OnGuard entities

Entities related to the OnGuard plugin have contextual commands that can be executed when you right-click on the entity in Config Tool, or when you are monitoring the entity in a Security Desk tile.

The following table lists the contextual menu commands available.

IMPORTANT: Contextual menu commands are only available to users with the appropriate privileges. The **OnGuard contextual actions** privileges can be configured on the **Privileges** tab of the *User management* task in Config Tool.

Contextual menu command	Entity	Description
Alarms	Plugin role	• Refresh the state of alarms configured on OnGuard devices that are currently active. • Add or remove alarm recipients.
Set controller clock	Intrusion detection units and access control panels	Sends the current time to the unit or panel.
Download database	Intrusion detection units and access control panels	Sends a command to the unit or panel to download the cardholder database.
Download firmware	Intrusion detection units and access control panels	Sends a download firmware command to the unit or panel.
Reset use limit	Intrusion detection units and access control panels	Sends a command to reset the use limit of all cardholders on the unit or panel.
Connect (used for dial-up only)	Intrusion detection units and access control panels	This command instructs the host to connect to the panel using dial-up.
Disconnect (used for dial-up only)	Intrusion detection units and access control panels	Used for dial-up only. This command instructs the host to send a disconnect command to the unit or panel.
Open door[1]	Door/Reader	Sends a command to open the door for a specific door/reader.
Reader access modes	Door/Reader	Sends a command to set the current operating mode of a door/reader.
Reader biometric verify mode	Door/Reader	Sends a command to enable / disable the biometric mode of verification for a reader.

Contextual menu command	Entity	Description
Reader first card unlock mode	Door/Reader	Sends a command to enable/ disable first card unlock mode for the door/reader.
Download firmware	Door/Reader	Sends a download firmware command to the reader interface module.
Open door	Door (Intrusion door)	Sends a command to open the intrusion door.
Door mode	Door (Intrusion door)	Sends a command to change the door mode.
Arm	Intrusion Area	Sends a command to arm the area.
Disarm	Intrusion Area	Sends a command to disarm the area.
Silence Alarms	Intrusion Area	Sends a command to silence area alarms.
Mask	Input	Mask all inputs at the same time, alarm inputs, or the AUX1 or AUX2 inputs individually. Masking other individual inputs is not supported.
Unmask	Input	Unmask all inputs at the same time, alarm inputs, or the AUX1 or AUX2 inputs individually. Unmasking other individual inputs is not supported.
Bypass	Input	Sends a command to enable bypass for the alarm zone.
Unbypass	Input	Sends a command to disable bypass for the alarm zone.
Pulse	Output	Sends a command to activate inputs for a specific time.
Activate	Output	Sends a command to activate the relay outputs or reader auxiliary outputs. Reader auxiliary outputs can be activated individually or simultaneously.
Deactivate	Output	Sends a command to deactivate the relay outputs or reader auxiliary outputs. Reader auxiliary outputs can be activated individually or simultaneously.

Contextual menu command	Entity	Description
Pulse	Output	Sends a command to activate outputs for a specific time.
Acknowledge alarms	• Intrusion detection units and access control panel • Door/reader • Door (Intrusion door) • Intrusion area • Input • Output	Sends a command to acknowledge all active alarms for the selected entity.
Deactivate cardholder	Cardholders	Sends a command to deactivate the cardholder credential in the OnGuard system.

[1]Sending an OpenDoor command from Security Center to the OpenAccess API returns an *Open Door Command* event only after the door is relocked.

How OnGuard alarms work with Security Center

The plugin automatically synchronizes OnGuard alarms using alarm entities in Security Center. It automatically triggers alarms in Security Center when the corresponding events are received from OnGuard. You can also acknowledge alarms in Security Center.

Alarm monitoring

When you monitor OnGuard alarms in Security Center, you'll observe the following:

- OnGuard alarms can be monitored like any other Security Center alarms using the *Alarm monitoring* task in Security Desk.
- Alarms triggered in OnGuard are immediately triggered in Security Center.
- When Security Center initially connects to the proxy, the alarms that are currently active in OnGuard aren’t triggered in Security Center. After the initial connection, if the plugin disconnects and reconnects, the alarm triggers that were missed in OnGuard are recovered and triggered in Security Center.
- You can’t trigger alarms in OnGuard from Security Center.
- You can view the source input triggering an OnGuard alarm in the *Alarm monitoring* task. If the source input isn't synchronized with Security Center, its synchronized parent entity is reported as the source. The parent entity can be a reader, or the door associated with the reader. If neither the reader nor the door is synchronized, the plugin role is reported as the source.

Alarm acknowledgment

When you acknowledge OnGuard alarms in Security Center, consider the following:

- Alarms acknowledged in Security Center are immediately acknowledged in OnGuard.
- Alarms acknowledged in OnGuard are immediately acknowledged in Security Center.
- If you acknowledge an alarm in Security Center while the plugin is disconnected from OnGuard, the alarm is automatically acknowledged in OnGuard upon reconnection.

Alarm reports

If an alarm is activated and acknowledged while the plugin is disconnected from the server, the alarm is included in reports generated after the connection is restored.

For information about monitoring and acknowledging alarms, and generating alarm reports in Security Desk, see the Security Center User Guide. You can view the guide by pressing F1 in Security Desk.

How OnGuard actions are triggered in Security Center

There are several actions that you can trigger in OnGuard by using hot actions and event-to-actions in Security Center. You can also trigger actions on entities by adding the entity to a tile in the monitoring task and right-clicking on it.

The following table lists which actions are supported, and whether or not they are supported using a *Monitoring task* widget.

Security Center action	Event-to-action and Hot actions	Security Desk Monitoring task widget
Unlock door explicitly[1]	Supported	Supported
Arm intrusion detection area	Supported	Not supported[2]
Disarm intrusion detection area	Supported	Not supported[2]
Trigger output	Supported	Not available

[1]Not supported for intrusion detection panel doors.

[2]The status is always displayed as *Unknown* in the widget.

Supported reports

Discover the reports added to Security Center by the OnGuard plugin. You can investigate the events and alarms forwarded by the intrusion panels by using several of the reports available in Security Desk.

Supported Security Center reports

The following reports are available for use with the OnGuard plugin. These reports are available from the Security Desk *Tasks* page.

- Access control health history
- Access control unit events
- Cardholder access rights
- Cardholder activities
- Credential activities
- Credential configuration
- Door activities
- Visitor activities

NOTE: Due to a limitation in how OnGuard sends events to Security Center, it can take up to 30 seconds for the OnGuard system to detect network interruptions, which might cause events to be lost. To minimize the possibility of issues, it is a best practice to install the proxy on the OnGuard server.

7

Maintenance and troubleshooting

This section includes the following topics:

- "OnGuard plugin installed but missing from Security Desk and Config Tool" on page 69

OnGuard plugin installed but missing from Security Desk and Config Tool

If the plugin role is missing the *Properties*, *Events*, *Cameras*, and *Synchronization* pages, and if the OnGuard reports are missing, then the plugin is not installed on your local machine. The plugin must be installed on a Genetec™ Server (expansion) and on all client workstations that are used to monitor and control OnGuard entities.

Symptoms

- In Config Tool, you see the plugin in the *Plugins* task, and you can add a new plugin role, but the role is missing the **Properties** tab.
- OnGuard contextual menu items are missing when you right-click OnGuard doors and panels in Security Desk and Config Tool.
- In Security Desk, you do not see the Command activity and Synchronization activity reports for this plugin

Causes

The plugin is not installed on the local computer, the license (certificate) is invalid, or you are missing required user privileges.

Solutions

Solution 1: Install the plugin on your local computer.

Solution 2: Make sure that a Security Center server has the plugin installed, that the plugin role is hosted on it, and that it is configured correctly.

Solution 3: Confirm that the plugin is installed on your Security Center computer: from the homepage in Security Desk or Config Tool, click **About** > **Installed components** and look in the list for entries that begin with *Genetec.Plugins*.

Solution 4: Confirm that your system has a license (certificate) for the plugin: from the homepage in Security Desk or Config Tool, click **About** > **Certificates**, look in the list for the name of the plugin, and make sure that your access permissions are set to **Unlimited**.

Solution 5: Confirm that your user accounts have the required privileges granted.

Glossary

add-on

An add-on is a software package that adds tasks, tools, or specific configuration settings to Security Center systems.

alarm

An alarm entity informs users of a situation that requires immediate attention and provides details on how it can be handled in Security Center. For example, an alarm can indicate which entities (usually cameras and doors) best describe the situation, who must be notified, how it must be displayed to the user, and so on.

entity

An entity represents anything in your system that requires configuration. This can be a physical device, such as a camera or a door, or an abstract concept, such as an alarm, a schedule, a user, a role, a plugin, or an add-on.

event

An event is a record of an activity or incident that occurred in the system. Security personnel can monitor events in real time and investigate them later. Events can also trigger automations in the system.

event-to-action

An event-to-action links an action to an event. For example, you can configure an alarm to trigger when a door is forced open.

expansion server

An expansion server is any server machine in a Security Center system that does not host the Directory role. The purpose of the expansion server is to add to the processing power of the system.

Federation™

Federation™ joins multiple, independent Genetec™ security systems into a single virtual system. With this feature, users on a central system, called the Federation host, can view and control entities that belong to remote systems.

Maps

The *Maps* task is an operation task that heightens your situational awareness by providing the context of a map to your security monitoring and control activities.

plugin

A plugin (in lowercase) is a software component that adds a specific feature to an existing program. Depending on the context, plugin can refer either to the software component itself or to the software package used to install the software component.

Plugin

Plugin (with an uppercase, in singular) is the role template that serves to create specific plugin roles.

plugin role

A plugin role adds optional features to Security Center. A plugin role is created by using the *Plugin* role template. By default, it is represented by an orange puzzle piece in the *Roles* view of the *System* task. Before you can create a plugin role, the software package specific to that role must be installed on your system.

Plugins

The *Plugins* task is an administration task that you can use to configure plugin-specific roles and related entities.

role

A role is a software component that performs a specific job within Security Center or Security Center SaaS.

Service Release

A Service Release (SR) is a standalone release that includes minor functionality improvements, bug fixes, and the integration of new hardware, intrusion devices, and plugins.

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ TechDoc Hub:** The latest documentation is available on the TechDoc Hub.

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

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 Advantage Description.

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, contact GTAC at https://portal.genetec.com/support.
- For issues with license content or part numbers, or concerns about an order, 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, contact Genetec Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Hardware product issues and defects

Contact GTAC at https://portal.genetec.com/support to address any issue regarding Genetec appliances or any hardware purchased through Genetec Inc.