SecurityCenter

Open Platform Communications (OPC) Server Plugin

Guide

4.0

Genetec

Copyright notice

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. The use of this document is subject to the disclaimer of liability found in the end-user license agreement.

All specifications are subject to change without notice.

Document information

Document title: Open Platform Communications (OPC) Server Plugin Guide 4.0

Document number: EN.720.032-V4.0.B(1)

Document update date: October 24, 2016

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

About this guide

This guide describes how to integrate Open Platform Communications (OPC) Servers in Security Center.

This guide supplements OPC and Security Center documentation. It assumes you are familiar with the following:

- Security Center 5.5 systems
- Configuration and use of Open Platform Communications

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: Topics appearing in this guide that reference information found on third-party websites were accurate at the time of publication, however, this information is subject to change without prior notice to Genetec™.

Contents

1

Introduction to OPC Server plugin

This section includes the following topics:

What is the OPC Server plugin?

The Open Platform Communications (OPC) Server plugin integrates the OPC Server with Security Center for external systems that have an OPC Client interface. Clients and servers must use the same protocol to communicate with each other.

The OPC Server plugin is a communication protocol plugin that hosts an OPC compliant server. The plugin exports camera, area, and door entities as OPC objects, using the OPC Unified Architecture (UA) protocol. The plugin exposes the logical identifiers of camera, area, and door objects. It also indicates the state of the door objects (*open* or *closed*, and *locked* or *unlocked*) and camera objects (*online* or *offline*, and *recording started* or *recording stopped)*.

The plugin forwards video and access control events to OPC Clients, following the recommendations in "Part 9: Alarms and Conditions", *OPC Unified Architecture Specification*. Events are raised on the camera, area, and door objects to which the events relate. If an access control event is related to a cardholder, the cardholder's name and credential are also provided as event information. The event reporting hierarchy follows the logical hierarchy of the objects; if you monitor an area on a client workstation, you receive events from cameras, areas, and doors within that area.

2

Release notes

This section includes the following topics:

What's new in OPC Server plugin 4.0

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

The OPC Server plugin 4.0 is a new integration for Security Center 5.5 SR2.

Resolved issues in OPC Server plugin 4.0

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

There are no resolved issues in OPC Server plugin 4.0.

Known issues in OPC Server plugin 4.0

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

There are no known issues in OPC Server plugin 4.0.

Limitations in OPC Server plugin 4.0

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

There are no known limitations in OPC Server plugin 4.0.

OPC Server plugin 4.0 compatibility

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

OPC Server plugin 4.0 is compatible with the following systems:

- Security Center 5.5 SR2 and later
- OPC UA clients

Events supported by OPC Server plugin

Only specific Security Center events related to cameras, doors, and areas can be monitored on OPC Clients.

Event type	Event
Access events	
	Access denied
	Access denied: A second cardholder is required
	Access denied: A valid escort is required
	Access denied: Antipassback violation
	Access denied: Denied by access rule
	Access denied: Expired credential
	Access denied: First-person-in rule supervisor absent
	Access denied: Inactive cardholder
	Access denied: Inactive credential
	Access denied: Insufficient privileges
	Access denied: Invalid PIN
	Access denied: Lost credential
	Access denied: No access rule assigned
	Access denied: Out of schedule
	Access denied: Stolen credential
	Access denied: Unassigned credential
	Access denied: Unknown credential
	Access denied: Valid card, invalid PIN
	Access denied: Visitor escort not supported by this unit model
	Access granted
	Antipassback violation
Door events	

Event type	Event
	Door closed
	Door forced open
	Door locked
	Door maintenance completed
	Door maintenance started
	Door manually unlocked
	Door offline: Device is offline
	Door open too long
	Door opened
	Door unlocked
	Entry assumed
	Entry detected
	Hardware tamper
	Manual station activated
	Manual station reverted to normal state
	No entry detected
	Request to exit
	Request to exit normal
	Scheduled lock
	Scheduled unlock
Video events	
	Adaptive motion triggered
	Archiving queue full
	Audio alarm
	Blocked camera started
	Blocked camera stopped
	Camera not archiving

Event type	Event
	Camera tampering
	Direction alarm
	Edge storage medium failure
	Face detected
	License plate in sight
	License plate out of sight
	License plate reading
	Live bookmark added
	Loitering
	Motion on
	Motion off
	Object condition changed
	Object count reached
	Object crossed line
	Object detected
	Object entered
	Object exited
	Object following route
	Object left
	Object merged
	Object removed
	Object separated
	Object stopped
	Object state changed
	Person falling
	Person running
	Person sliding

Event type	Event
	Playback bookmark added
	PTZ activated
	PTZ locked
	PTZ stopped
	PTZ zoom started
	PTZ zoom stopped
	Receiving RTP packets from multiple sources
	Recording started (alarm)
	Recording started (continuous)
	Recording started (external)
	Recording started (motion)
	Recording started (user)
	Recording stopped (alarm)
	Recording stopped (continuous)
	Recording stopped (external)
	Recording stopped (motion)
	Recording stopped (user)
	RTP packets lost
	Signal lost
	Signal recovered
	Tailgating
	Transmission lost
	Transmission recovered
	Undefined video analytics event
	Unit failed to respond to edge video request
	Online state changed

3

Installing OPC Server plugin

This section includes the following topics:

Installing the OPC Server plugin

The OPC Server plugin is installed separately from the Security Center system.

Before you begin

- Read the release notes for any known issues, limitations, supported firmware, and other information about this release.
- Install Security Center 5.5 SR2 or later on the server. For more information about installing Security Center, see the *Security Center Installation and Upgrade Guide*.
- Check that your Security Center license has a valid certificate for the OPC Server plugin.

  NOTE: The license number is included in the product-release email from the Genetec product manager. This email also includes links to the plugin download package and other license information.
- Close Config Tool and Security Desk.

What you should know

You must install the plugin on the Security Center client and server computers.

- If your Security Center system consists of a single server, install the plugin on that server.
- If you have a multi-server Security Center system, install the plugin on an expansion server.

To install the OPC Server plugin:

1. Download the OPC Server installation package from the GTAP Product Downloads page.
2. Double-click the *setup.exe* file and follow the installation instructions in the wizard.
3. 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 right away. However, you must restart the Genetec Server to complete the plugin installation.
4. Optional: On the computer where you installed the OPC Server plugin, install the OPC Local Discovery Server (*LDS.exe*) from https://opcfoundation.org/developer-tools/developer-kits-unified-architecture/local-discovery-server-lds.

   A Local Discovery Server (LDS) is only required if you want OPC Clients to discover the existence of the OPC Server plugin, the OPC Server URL, and supported connection parameters through the LDS.

After you finish

Create the OPC Server plugin role.

4

Configuring OPC Server plugin

This section includes the following topics:

Creating the plugin role

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

Before you begin

Install the plugin.

To create the plugin role:

1 From the home page in Config Tool, open the **Plugins** task.

2 At the bottom of the **Plugins** task, click **Add an entity** (➕), and select **Plugin**.

3 On the *Specific info* page, select the plugin type, the server to run the plugin, and then click **Next**.

If you are not using an expansion server, the option to select a server is not displayed.

4 On the *Basic information* page, do the following:

a) Enter the name in the **Entity name** field.

b) Enter the description in the **Entity description** field.

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

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 is created, the following message appears: `The operation was successful`.

6 Click **Close**.

The OPC Server plugin role appears in the entity browser.

Configuring a user for the OPC Server plugin

To make sure that you can view Security Center entities on OPC Clients, you must configure the user whose credentials will be used to connect the OPC Server to Security Center.

Before you begin

Create a user in Security Center. For more information about creating users in Security Center, see the *Security Center Administrator Guide*.

What you should know

The user whose credentials are used to connect the OPC Server to Security Center determines which entities are exposed to OPC Clients. For a Security Center entity to be exposed, the user must have the user privilege to view that entity, and they must be an administrator of the partition that the entity is a member of.

To configure a user for the OPC Server plugin:

1. From the home page in Config Tool, open the *User management* task.
2. Select the user, and click the **Privileges** tab.
3. Set the following privileges to **Allow**:
   - Log on using the SDK
   - View area properties
   - View camera properties
   - View door properties
4. Click **Apply**.
5. Click the **Access rights** tab.
6. Select the checkbox beside the partitions you want to grant access rights for.

   This action automatically grants access rights for all its child partitions.
7. For each partition that you granted access rights for, select the checkbox in the **Administrator** column.
8. Click **Apply**.

Creating and configuring the OPC Server

To set up the OPC Server plugin and enable users to monitor Security Center entities on OPC Clients, you must create the OPC Server and configure its connection parameters.

Before you begin

- Create the OPC Server plugin role.
- Configure the user whose credentials will be used to connect the OPC Server to Security Center.

What you should know

Only specific configuration settings are described here. For more information about generic Config Tool settings, such as the *Identity* and *Resources* settings, see the *Security Center Administrator Guide*. You can access this guide by pressing `F1` in Config Tool.

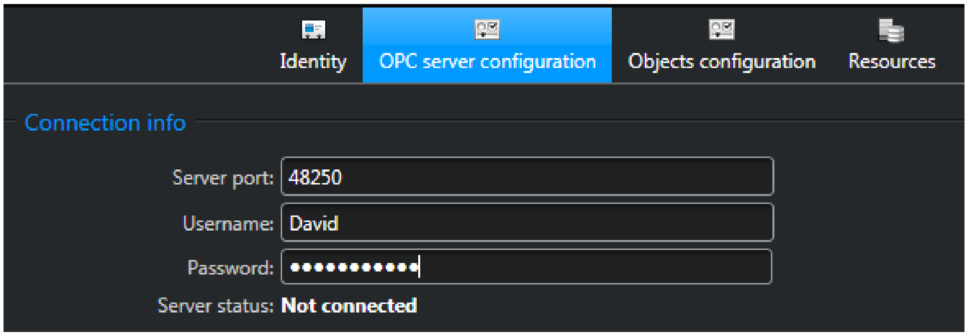
Setting up connection information for the OPC Server plugin:

1 From the home page in Config Tool, open the *Plugins* task.

2 Select the OPC Server plugin from the entity browser, and click the **OPC Server configuration** tab.

3 In the *Connection information* section, enter the following information:

- **Server port:** Port number on which the OPC Server is created.
- **Username:** Name of the user that the OPC Server uses to connect to Security Center with.
- **Password:** User password that the OPC Server uses to connect to Security Center with.

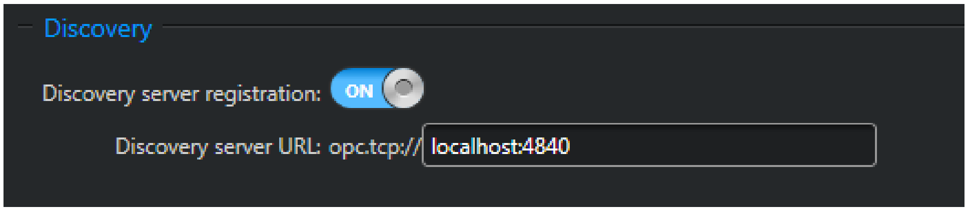


Server port: 48250
Username: David
Password: ●●●●●●●●●●●
Server status: Not connected

4 If you have a Local Discovery Server installed, register the OPC Server with the LDS as follows:

a) In the *Discovery* section, set the **Discovery Server registration** option to **ON**.

b) In the **Directory Server URL** option, enter the IP address and port of the LDS.



Discovery server registration: ON
Discovery server URL: opc.tcp:// localhost:4840

5 Click **Apply**.

The OPC Server is created, and is connected to Security Center. The **Server status** changes from **Not connected** to **Ready**.

Enabling authentication and trusting OPC Client certificates

To secure your system, you can enable authentication for connecting to the OPC Server, and select which OPC Client can connect to the OPC Server by trusting their certificates.

Before you begin

The OPC Client must have a valid certificate.

What you should know

When an OPC Client attempts to connect to the OPC Server, the client's certificate is initially rejected.

If you register the OPC Server with an LDS, the LDS certificate is trusted by default.

If you disable authentication, users can connect to the OPC Server without using a trusted certificate.

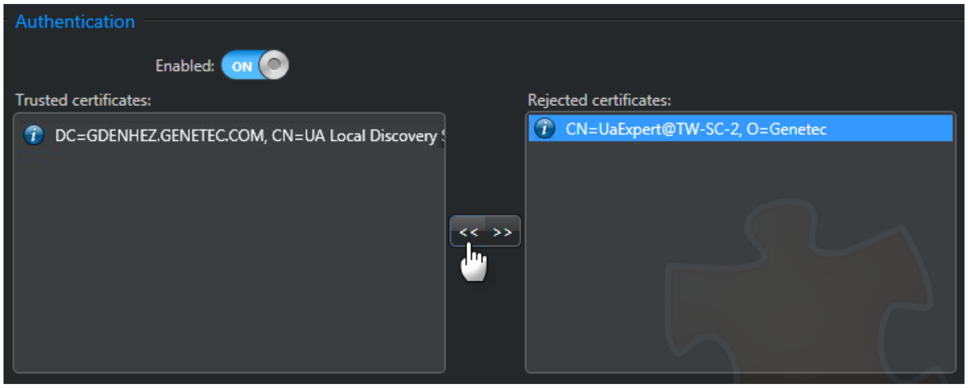
To enable authentication and trust an OPC Client certificate:

1 From the home page in Config Tool, open the *Plugins* task.

2 Select the OPC Server plugin from the entity browser, and click the **OPC Server configuration** tab.

3 In the *Authentication* section, set the **Enabled** option to **ON**.

4 In the *Rejected certificates* pane, select a certificate, and click the left arrow to move it to the *Trusted certificates* pane.



Authentication

Enabled: ON

Trusted certificates:

DC=GDENHEZ.GENETEC.COM, CN=UA Local Discovery S

Rejected certificates:

CN=UaExpert@TW-SC-2, O=Genetec

5 Click **Apply**.

Selecting which entities and events to monitor on OPC Clients

To send camera, door, and area entity information from Security Center to OPC Clients, you must select which entity types and events to expose.

To select which entities and events to monitor on an OPC Client:

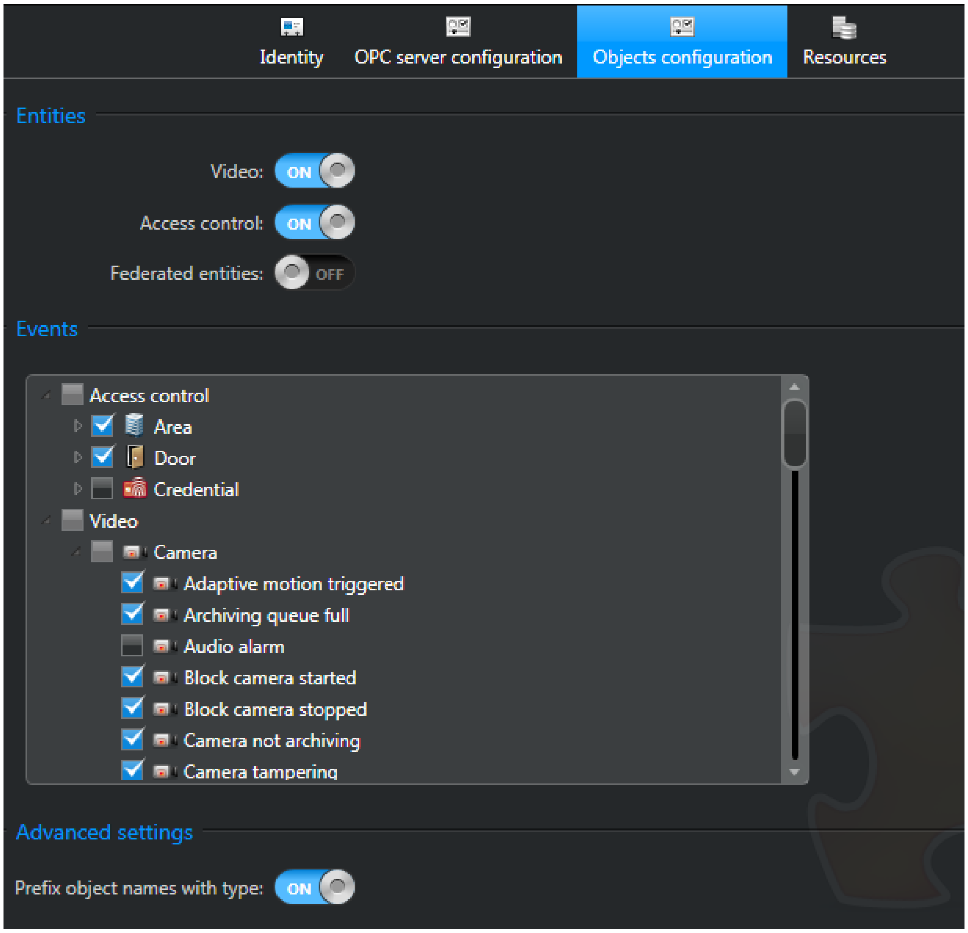
1 From the home page in Config Tool, open the *Plugins* task.

2 Select the OPC Server plugin from the entity browser, and click the **Object configuration** tab.

3 In the *Entities* section, select which entity types to monitor on OPC Clients:

- **Video:** Turn this option to **ON** to expose camera entities. The Archivers that manage the cameras are also exposed to show the camera hierarchy.
- **Access control:** Turn this option to **ON** to expose area and door entities.
- **Federated entities:** Turn this option to **ON** to expose federated cameras, areas, and doors. The Security Center Federation and Omnicast Federation roles are also exposed to show the entity hierarchy.

  NOTE: There might be a large number of federated entities.



Entities

Video: ON

Access control: ON

Federated entities: OFF

Events

- ■ Access control
  - ☑ Area
  - ☑ Door
  - ☐ Credential
- ■ Video
  - ■ Camera
    - ☑ Adaptive motion triggered
    - ☑ Archiving queue full
    - ☐ Audio alarm
    - ☑ Block camera started
    - ☑ Block camera stopped
    - ☑ Camera not archiving
    - ☑ Camera tampering

Advanced settings

Prefix object names with type: ON

4 In the *Events* section, select which event types to monitor on OPC Clients.

5 To prefix entity names with the entity type when cameras, doors, and areas are displayed on OPC Clients as OPC objects, set the **Prefix object names with type** option to **ON**.

Example: When the **Prefix object names with type** option is enabled, the *Front Entrance* camera entity is displayed as *Camera Front Entrance* on OPC Clients.

6 Click **Apply**.

In OPC Clients, you can now browse to the entities you exposed, and monitor events and states related to those entities.

Related Topics

Events supported by OPC Server plugin on page 8

Testing the OPC Server integration

After you configure the OPC Server plugin in Security Center, you can connect to an OPC Client and validate your OPC Server integration.

To test the OPC Server integration:

1. Connect to an OPC Client, and make sure that you have a valid client certificate.
2. Connect your OPC Client to the OPC Server, by doing one of the following:
   - If an LDS is installed on the computer where the OPC Server plugin is installed, connect using the LDS.

     NOTE: The OPC Server must be registered with the LDS in Config Tool.
   - Auto-discover the OPC Server if it is using the default port 4840.
   - Enter the specific IP address and port number of the OPC Server.
3. In the OPC Client, trust the OPC Server certificate.
4. In Config Tool, trust the OPC Client certificate.
5. In the OPC Client, make sure that you can see the Security Center entities you exposed as OPC objects.

You can now monitor events and states related to the Security Center entities.

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ Technical Information Site:** The latest documentation is available on the Technical Information Site. To access the Technical Information Site, log on to Genetec™ Portal and click Technical Information. Can't find what you're looking for? Contact documentation@genetec.com.
- **Installation package:** The Installation Guide and Release Notes are available in the Documentation folder of the installation package. These documents also have a direct download link to the latest version of the document.
- **Help:** Security Center client and web-based applications include help, which explain how the product works and provide instructions on how to use the product features. Patroller and the Sharp Portal also include context-sensitive help for each screen. 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 Genetec™ customer, you have access to the Genetec™ Technical Information Site, where you can find information and search for answers to your product questions.

- **Genetec™ Technical Information Site:** 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 the Technical Information Site for potential fixes, workarounds, or known issues.

  To access the Technical Information Site, log on to Genetec™ Portal and click Technical Information. Can't find what you're looking for? Contact documentation@genetec.com.
- **Genetec™ Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec™ Lifecycle Management (GLM) documents: EN_GLM_ASSURANCE and EN_GLM_ADVANTAGE.

Additional resources

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

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

Licensing

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

Hardware product issues and defects

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