Genetec™ Security Center.

OPC Client Plugin Guide 3.1

Click here for the most recent version of this document.

Document last updated: March 1, 2019

Genetec™

Legal notices

Document information

Document title: OPC Client Plugin Guide 3.1

Document number: EN.550.039-V3.1(2)

Document update date: March 1, 2019

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

About this guide

This guide describes how to use the OPC Client plugin to connect to OPC systems and devices so you can monitor them in Security Center.

This guide supplements OPC and Security Center documentation. 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
- Configuration and use of OPC systems

For a list of Security Center courses, visit https://www.genetec.com/support/training/certification-courses.

For specific information regarding your hardware, software, and systems, refer to their manufacturer's documentation and web site.

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 from Genetec Inc.

Contents

Preface

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

Chapter 1: Introduction to the OPC Client plugin

What is the OPC Client plugin? . . . 2
How the OPC Client plugin works with Security Center . . . 3
Integration overview for OPC Client . . . 4

Chapter 2: Release notes

What's new in the OPC Client plugin 3.1 . . . 7
Resolved issues in the OPC Client plugin 3.1 . . . 7
Known issues in the OPC Client plugin 3.1 . . . 8
Limitations in OPC Client plugin 3.1 . . . 9
Product compatibility for the OPC Client plugin 3.1 . . . 10
System requirements for the OPC Client plugin 3.1 . . . 11
License options for the OPC Client plugin . . . 12

Chapter 3: Installing the OPC Client plugin

Downloading and installing the OPC Client plugin . . . 14

Chapter 4: Configuring the OPC Client plugin

Creating the OPC Client plugin role . . . 16
Connecting the OPC Client plugin role to an OPC server . . . 17
OPC server failover mode and redundancy mode for the OPC Client plugin . . . 18
Creating an XML type definition file . . . 20
How entity types are defined in XML type definition files . . . 20
Importing an XML type definition file into Security Center . . . 22
Creating a CSV import file . . . 24
Rules for creating a valid CSV import file for the OPC Client plugin . . . 24
Headers in the CSV import file for OPC Client . . . 25
Importing OPC tags into Security Center . . . 27
Enrollment statuses of OPC devices . . . 28

Chapter 5: Configuring OPC entities

Creating rules for state changes of OPC entity properties . . . 32
Linking cameras to OPC entities . . . 35
Renaming OPC entities from Config Tool . . . 36
Editing properties of OPC entities from Config Tool . . . 37

Chapter 6: Monitoring OPC entities

About monitoring OPC entities . . . 39
OPC entities on maps . . . 39
Reviewing OPC Client rule engine events in Security Desk . . . 41

Technical support . . . 42

Where to find product information 43

1

Introduction to the OPC Client plugin

This section includes the following topics:

- "What is the OPC Client plugin?" on page 2
- "How the OPC Client plugin works with Security Center" on page 3
- "Integration overview for OPC Client" on page 4

What is the OPC Client plugin?

The Open Platform Communications (OPC) Client plugin connects to external OPC Unified Architecture (UA) servers, so you can access data from your existing OPC systems from Security Center.

The plugin can connect to OPC systems and devices including building automation or HVAC systems, as well as Internet of Things (IoT) devices that support OPC UA protocol, such as fire panels. These devices consist of multiple data points, which are represented as OPC tags on the OPC server.

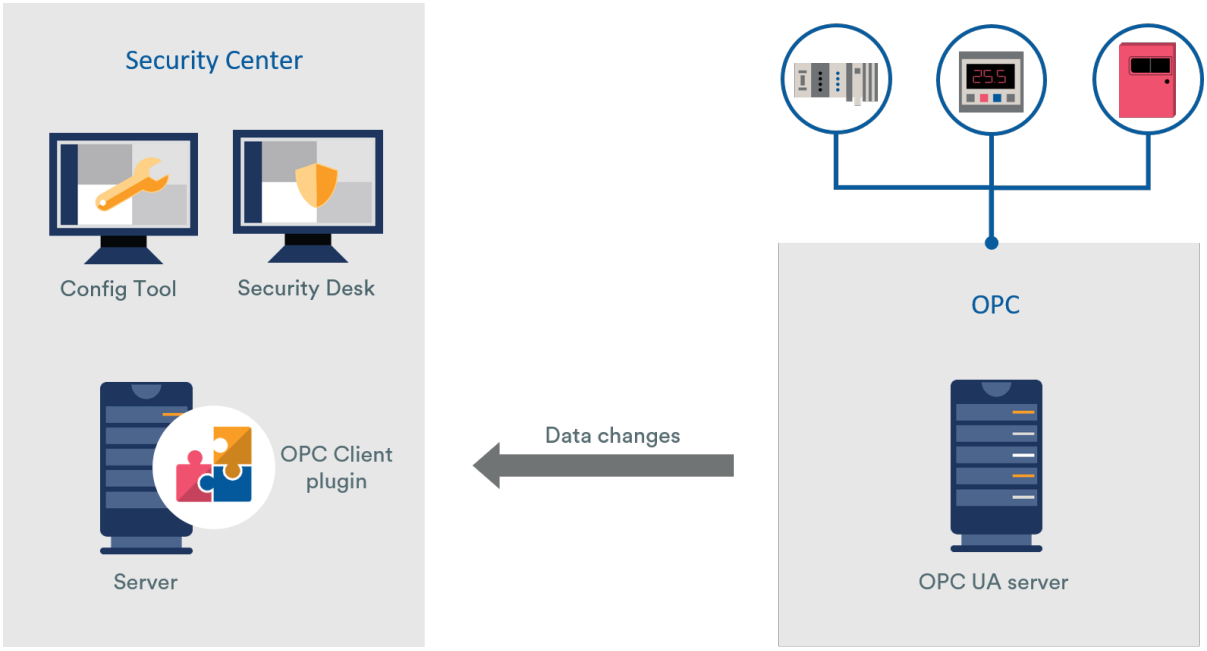
Through this integration, you can do the following:

- Integrate OPC tags or objects as OPC entities in Security Center.
- Monitor data changes of OPC entities.
- Display OPC entities and their statuses on a map.
- Link cameras to OPC entities to view video associated with alarms and events.
- Trigger events on OPC data changes.
- Trigger alarms on OPC data changes.
- Monitor the health statuses of OPC tags.
- Generate reports about events triggered by the OPC Client plugin.

How the OPC Client plugin works with Security Center

Using the OPC Client plugin, you can map OPC tags exposed by an OPC UA server to Security Center entities, and monitor data changes of the OPC tags associated with these entities in Security Center.

The OPC Client plugin hosts an OPC-compliant client, which means that Security Center becomes the OPC client application through the integration. When the OPC Client plugin role is connected to an OPC server, you can use a CSV file to import the OPC tags or objects from the external system into Security Center. These tags are mapped to OPC entities. Communication between Security Center and the OPC server is established through the OPC UA protocol.



NOTE: The OPC Client plugin 3.1 does not receive OPC UA events. It only receives data changes from items that are monitored by OPC.

Integration overview for OPC Client

You can integrate and OPC client in Security Center by following a sequence of steps.

The following table lists the tasks required for the integration.

Step	Description	Where to find more information
Learn about the release		
1	Read the release notes to learn about any known issues, limitations, supported software, and other information about this release of the plugin.	• What's new in the OPC Client plugin 3.1 on page 7. • Resolved issues in the OPC Client plugin 3.1 on page 7. • Known issues in the OPC Client plugin 3.1 on page 8. • Limitations in OPC Client plugin 3.1 on page 9.
Install the plugin		
2	Verify that the Security Center license has a valid certificate for the OPC Client plugin: go to the Config Tool home page, click **About** > **Certificates**, and confirm that OPC Client is on the list.	• The license number is included in the product-release email sent by Genetec Inc. This email also includes links to the plugin download package and other license information. • If you require a license, see License options for the OPC Client plugin on page 12.
3	Ensure that the servers on which you will install the plugin meet the recommended system requirements and are running a compatible version of Security Center.	• System requirements for the OPC Client plugin 3.1 on page 11. • Product compatibility for the OPC Client plugin 3.1 on page 10.
4	Download and install the OPC Client plugin on all Security Center servers and client workstations from which you want to monitor OPC entities.	• Downloading and installing the OPC Client plugin on page 14.
Connect the plugin to the OPC server		
5	Create the OPC Client plugin role on the server of your choice.	• Creating the OPC Client plugin role on page 16.

Step	Description	Where to find more information
6	From the *Plugins* task, connect to OPC servers.	• Connecting the OPC Client plugin role to an OPC server on page 17. • OPC server failover mode and redundancy mode for the OPC Client plugin on page 18.
Create OPC entities		
7	Create the XML file to define the entity types and properties that can be added to Security Center.	• Creating an XML type definition file on page 20. • How entity types are defined in XML type definition files on page 20.
8	Import the XML file into Security Center.	• Importing an XML type definition file into Security Center on page 22.
9	Create the CSV file from which OPC tags can be imported. This file is used to create OPC entities in Security Center.	• Creating a CSV import file on page 24. • Rules for creating a valid CSV import file for the OPC Client plugin on page 24. • Headers in the CSV import file for OPC Client on page 25.
10	Create OPC entities in Security Center by importing the OPC tags from the CSV file.	• Importing OPC tags into Security Center on page 27. • Enrollment statuses of OPC devices on page 28.
Configure the OPC entities		
11	Create rules based on state changes of OPC entity properties to trigger custom events or alarms in Security Center.	• Creating rules for state changes of OPC entity properties on page 32.
12	(Optional) Link cameras to OPC entities in Security Center, so you can monitor live video when custom events and alarms are triggered.	• Linking cameras to OPC entities on page 35.
13	(Optional) Create a map, and then add OPC entities to it.	• Refer to "Creating maps" in the *Security Center Administrator Guide*. • OPC entities on maps on page 39.

2

Release notes

This section includes the following topics:

- "What's new in the OPC Client plugin 3.1" on page 7
- "Known issues in the OPC Client plugin 3.1" on page 8
- "Limitations in OPC Client plugin 3.1" on page 9
- "Product compatibility for the OPC Client plugin 3.1" on page 10
- "System requirements for the OPC Client plugin 3.1" on page 11
- "License options for the OPC Client plugin" on page 12

What's new in the OPC Client plugin 3.1

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

The OPC Client plugin 3.1 includes the following new features and enhancements:

- **View OPC entity type information:** After defining entity types and their property information in the XML type description file, you can view this information on the *Extensions* page of the plugin. While you create the CSV import file, refer to this page to see which entity types can be added in Security Center through the OPC Client plugin.
- **Connect to OPC servers in failover or redundancy mode:** If the plugin is configured to connect to two OPC servers, you can choose to operate in failover mode or in redundancy mode.
- **View the progress and status of OPC entity enrollment:** When you import OPC tags from a CSV file to create OPC entities, you can view the progress of the import, and which entities were undiscovered, added, or already added in Security Center.
- **Trigger alarms using the OPC Client rule engine:** Create rules based on the state changes of OPC entity properties to trigger alarms in Security Center. You can configure these alarms to be automatically acknowledged when the property returns to its normal state.
- **Link cameras to OPC entities:** You can link a camera to an OPC entity from the *Plugins* task, so that the video feed can be displayed when an event or alarm is triggered on that entity.
- **Monitor OPC entities from maps:** Create a map and drag OPC entities onto it. Events and alarms associated with the OPC entities are displayed on the map.
- **Edit OPC entity information in Config Tool:** Rename an OPC entity or its properties from the *Plugins* task.

Resolved issues in the OPC Client plugin 3.1

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

The following issues were resolved in the OPC Client plugin 3.1.

Issue	Description
940459	Restoring the plugin database can result in rules triggering the wrong events, if the custom event IDs on the system the database comes from and the IDs on the restored system do not match.
940039	If the plugin is not restarted after a restore, the database is overwritten.

Known issues in the OPC Client plugin 3.1

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

The OPC Client plugin 3.1 includes the following known issues.

Issue	Description
1867639	When the OPC Client plugin is connected to an OPC UA server behind a DA Gateway, the OPC UA server is displayed as *Connected* in the plugin, even if the OPC DA server is offline.
1716766	The SNMP Manager plugin cannot be used with the OPC Client plugin.
1715564	Importing a large number of OPC tags (over 1000) might take a long time.
1715217	When two properties in the type description XML file have the same DisplayName, the plugin cannot be loaded. **Workaround:** Make sure every property has a unique DisplayName.
1700819	After backing up and restoring the plugin database, cameras that were linked to OPC entities in Security Center are no longer linked.
1662594	If you federate a Security Center system that is running the OPC Client plugin, you cannot see the OPC entities from the Federation™ host.
976415	The OPC Client plugin 3.1 does not receive OPC UA events.

Limitations in OPC Client plugin 3.1

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

The OPC Client plugin 3.1 includes the following known limitations.

Issue	Description
935586	Sharing a database is not supported and having more than one plugin on the same database could result in severe configuration issues. **Workaround:** Give all plugin instances unique database names when each role is created.

Product compatibility for the OPC Client plugin 3.1

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

To be eligible for technical support, you must install the Security Center and third-party software versions that are listed as certified or supported by design in the following table.

Plugin	Third-party version	Certified Security Center version
OPC Client 3.1	OPC UA servers **NOTE:** If your OPC server uses the Data Access (DA) specification, you must configure an OPC DA to UA Gateway on the server so that the OPC Client plugin role can communicate properly with the server.	5.6 SR4 and 5.7

Product compatibility indicates that the product supports and can run with specific versions of other products. A product is compatible when it meets one of the following certification levels:

- **Certified:** Genetec Inc. has tested and validated the product.
- **Supported by design:** The product has similar characteristics or is a newer version of a certified version, but Genetec Inc. has not tested or validated the product.

  NOTE: Service releases of a major release are supported by design. For example, if 5.6 SR2 is listed, then SR3 and subsequent service releases for 5.6 are supported. If a major release is not listed, then it is not supported.

System requirements for the OPC Client plugin 3.1

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

The OPC Client plugin 3.1 must be installed on an expansion server and client workstations that meet the recommended Security Center system requirements.

License options for the OPC Client plugin

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.

Part number	Description	Requirements
GSC-1PBAS-OPC-C	Base package for the OPC Client plugin supports 100 OPC entities.	• Professional or Enterprise packages (Synergis™ or Omnicast™) • Genetec™ Advantage
GSC-1PBAS-100D	This part supports an additional 100 OPC entities.	• Professional or Enterprise packages (Synergis™ or Omnicast™) • Genetec™ Advantage

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. For example, if you integrated a system that has visitors, you need the Visitors option 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 the *Security Center Administrator Guide*.

3

Installing the OPC Client plugin

This section includes the following topics:

- "Downloading and installing the OPC Client plugin" on page 14

Downloading and installing the OPC Client plugin

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

Before you begin

Make sure of the following:

- Your server meets the recommended system requirements.
- A compatible version of Security Center is installed.

What you should know

- Although it is possible to host the plugin role on any server, it is a best practice to host that role on a dedicated expansion server for best system performance.
- If you already have an Intrusion Manager role set up, install the extension on that server.
- For your operators to have access to the features added by this plugin, you must install this plugin on all Security Center client workstations.

To install the plugin:

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 the file.
By default, the file is unzipped to *C:\Genetec*.
5 Close Security Desk and Config Tool.
6 Open the extracted folder, right-click the *setup.exe* file, and click **Run as administrator**.
7 Follow the installation instructions.
8 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.

Example

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

NOTE: This video shows how to install the 3.0 version of the OPC Client plugin, but the same procedure is applicable to 3.1.

After you finish

Create the plugin role.

Related Topics
Product compatibility for the OPC Client plugin 3.1 on page 10
System requirements for the OPC Client plugin 3.1 on page 11

4

Configuring the OPC Client plugin

This section includes the following topics:

- "Creating the OPC Client plugin role" on page 16
- "Connecting the OPC Client plugin role to an OPC server" on page 17
- "Creating an XML type definition file" on page 20
- "Importing an XML type definition file into Security Center" on page 22
- "Creating a CSV import file" on page 24
- "Importing OPC tags into Security Center" on page 27

Creating the OPC Client plugin role

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

Before you begin

Download and install the plugin.

To create the plugin role:

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

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

The plugin creation wizard opens.

3 On the *Specific info* page, select the server on which the plugin role is hosted, 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.

To connect the OPC Client plugin role to a different OPC server, you must delete the role database and create a new database to ensure that the information from the old OPC server is removed.

CAUTION: If you are running multiple OPC Client plugin roles on the same server, ensure that each plugin role only connects to its own database. Make sure that a unique database name is designated to each role upon creation. Do not use the default database name.

Example: OPCClient_Plugin1, OPCClient_Plugin2, OPCClient_Plugin3, and so on.

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**.

The plugin role appears in the entity browser. The plugin role is red until it is connected to an OPC server.

Example

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

Connecting the OPC Client plugin role to an OPC server

To monitor entities from an OPC server in Security Center, you must connect the OPC Client plugin role to the OPC server.

Before you begin

Create the OPC Client plugin role.

What you should know

- One OPC Client plugin role can connect to a maximum of two OPC servers with the same node IDs.

  NOTE: To connect to OPC servers with different node IDs, you must create another instance of the OPC Client plugin role.

- When the plugin role is connected to a second OPC server, you can choose between two operation modes. For more information, refer to OPC server failover mode and redundancy mode for the OPC Client plugin on page 18.

To connect the OPC Client plugin role to an OPC server:

1. From the Config Tool home page, open the *Plugins* task.
2. Select the OPC Client plugin from the entity browser, and click the **Connection** tab.
3. Under the **Servers** list, click  .
4. In the *General* section, enter a name for the server.
5. In the *Connection* section, do one of the following:
   - Type the IP address and port number of the OPC server.
   - To automatically discover the available endpoints and security settings of the OPC server using a Discovery URL:
     1. Click **Discover**.
     2. In the *OPC server discovery* window, enter the IP address and port number of the OPC server, and then click **Start**.
     3. Select one of the available server endpoints, and then click **Select**.
6. If you did not automatically discover the available endpoints and security options of the OPC server, configure them in the *Security* section:
   - **Message security:** Select the security type for messages sent from the OPC server.
     - **None:** No security is applied.
     - **Sign:** All messages are signed but not encrypted.
     - **Sign and encrypt:** All messages are signed and encrypted.
   - **Security policy:** Select the algorithm for how messages from the OPC server are signed and encrypted.
7. In the *Authentication* section, configure the following:
   - **Scheme:** Select the authentication scheme that is required for OPC clients to connect to the OPC server.
     - **Anonymous:** No authentication required to connect.
     - **Username and password:** Connect to the OPC server using credentials. Enter your username and password.
     - **Certificate:** Connect to the OPC server using a valid certificate. Use the default certificate that is provided by Genetec Inc., or click **Browse** to select a .pfx file that was provided to you from a third-party certificate authority.

NOTE: If messages sent from the OPC server are signed, or signed and encrypted, you must trust the OPC server certificate by clicking **View certificate** > **Trust** > **Close**.

8 Click **Apply**.

Security Center is connected to the OPC server. The connection status changes from **Not connected** to **Connected**.

After you finish

- If Security Center requires a valid certificate to connect to the server, you must trust the client certificate from the OPC server.
- Connect the plugin role to a second OPC server.

OPC server failover mode and redundancy mode for the OPC Client plugin

When the OPC Client plugin role is connected to two OPC servers, you can configure the plugin to operate in failover mode or in redundancy mode.

The OPC server failover mode is configured on the *Connection* page of the OPC Client plugin.

NOTE:

- For failover to work properly, both OPC servers must have the same node IDs.
- If you change this operation mode, you must deactivate, and then reactivate, the plugin role for the change take effect.

Failover mode

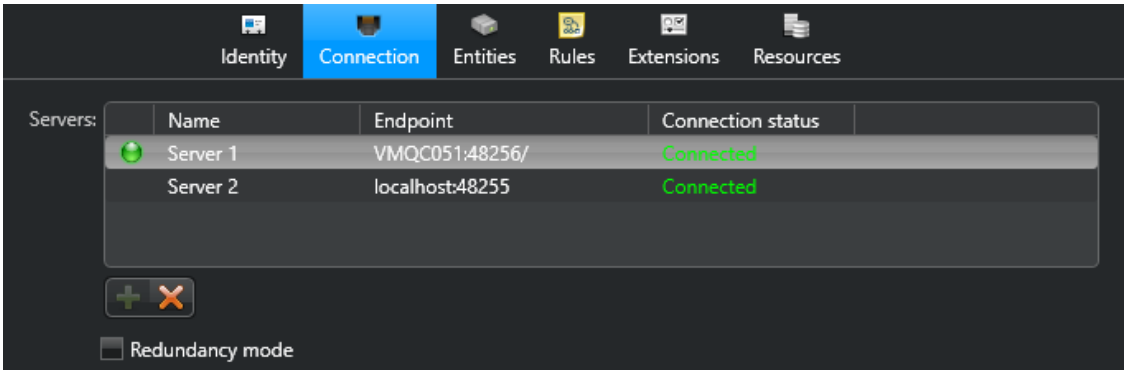
Failover mode is the default operation mode for the plugin when two connections are configured. In this mode, the OPC Client plugin connects to both configured OPC servers, but only listens for data change on the *active server*. On the *Connection* page of the plugin, the active server is indicated by a green icon ( ).

The active server is usually the first server with which the OPC Client plugin establishes a connection. The order in which the servers are listed does not affect which server is the active server.

When the connection between the plugin and the active server is lost, the connection will fail over to the next active server.

Example

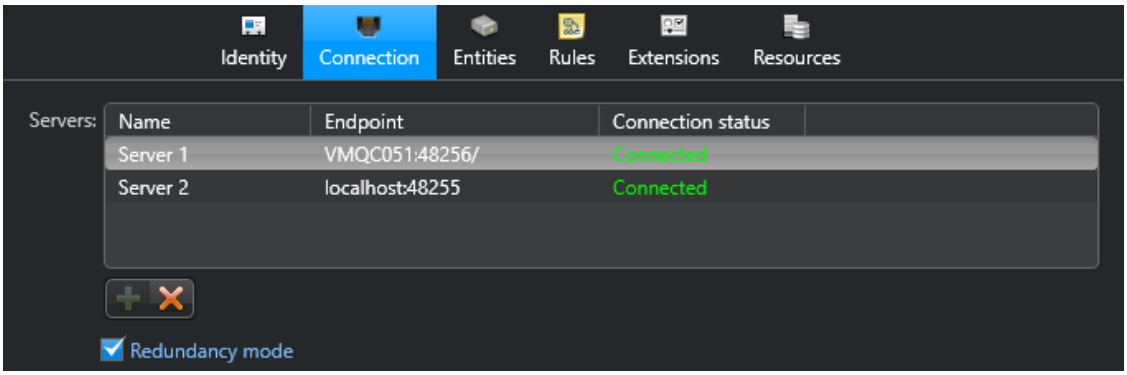
In the following image, the plugin is in failover mode because the **Redundancy mode** check box is not selected. *Server 1* is the active server.



- If *Server 1* goes offline, *Server 2* becomes the active server, and the plugin will start listening for data changes on *Server 2*.
- If *Server 1* comes back online, *Server 2* will remain the active server, as long as it is connected.

Redundancy mode

Redundancy mode is enabled by selecting **Redundancy mode** at the bottom of the **Servers** list. In this operation mode, the OPC Client plugin connects to both configured OPC servers, and listens for data change on both servers.



State changes of OPC tags are processed by the rule engine of the plugin. If both OPC servers are properly configured with the same node IDs, alarms and events used in rules are only triggered once because the plugin receives two data changes with identical values.

Related Topics

Creating rules for state changes of OPC entity properties on page 32

Creating an XML type definition file

Before you can import OPC tags from an OPC server into Security Center, you must define entity types for OPC entities to be imported. This is done through an XML file, which defines how OPC tags will be interpreted in Security Center.

What you should know

The type description file is an XML file that provides metadata from the external system that is imported into Security Center, so that entities can be created.

- The XML file name must end with the extension *.xml*.
- The XML format has been revised since version 3.0 of the OPC Client plugin. If you are using type definition files created for version 3.0, you must update them to be used with version 3.1.

To create the XML type definition file:

1 Using a text editor, open *Template.xml.template*, located in *$\Program Files (x86)\Security Center Plugins \OPCClient\Extensions*, and then save it under a new name.

Example: *OPCClientTypeDefinitions.xml*

2 In the XML file, define your entity types.

3 Save the XML file.

How entity types are defined in XML type definition files

The XML type definition file defines the entity types that the OPC Client plugin will be able to create in Security Center.

Each entity type in the XML file must include a name and property definitions.

The XML tags in the following table are listed as required or optional for each entity type:

XML tag	Include in file	Description
`Manufacturer`	Optional	Manufacturer of the device that will be mapped to the entity type.
`TypeName`	Required	Name for the custom entity type in Security Center. **NOTE:** This value must be unique.
`Description`	Optional	Description for the entity type.
`PropertyID`	Required	Identifier for this property. **NOTE:** This value must be unique for a given entity type.
`DisplayName`	Optional	Name for the property that is displayed in Security Center. **NOTE:** If this field is left empty, the `PropertyID` value is used instead. The `DisplayName` field can also be overridden by the `Display_Name` column in the CSV file.

XML tag	Include in file	Description
Type	Required	Data type of the property, which indicates how you can interact with the property value in Security Center. Use one of the following standard .NET data types: • System.Boolean • System.Double • System.Single • System.String • System.Int16 • System.UInt16 • System.Int32 • System.UInt32 • System.Int64 • System.UInt64 • System.Byte • System.SByte
Unit	Optional	The unit of measurement for the property. **NOTE:** If this field is left empty, the UNIT value in the CSV file is used.
UnitSymbol	Optional	The symbol for the unit of measurement for the property. **NOTE:** If this field is left empty, the UNITSYMBOL value in the CSV file is used.

Example

The following section of code defines an entity type called **FireDetector**. When an entity of this type is imported in Security Center, its **Property1** integer is displayed as **Temperature**.

```
<EntityTypes>
  <EntityType>
    <Manufacturer>Genetec</Manufacturer>
    <TypeName>FireDetector</TypeName>
    <Description>Example entity type</Description>
    <Properties>
      <Property>
        <PropertyId>Property1</PropertyId>
        <DisplayName>Temperature</DisplayName>
        <Type>System.Int32</Type>
        <Unit>Fahrenheit</Unit>
        <UnitSymbol>°F</UnitSymbol>
      </Property>
    </Properties>
  </EntityType>
</EntityTypes>
```

Importing an XML type definition file into Security Center

To import OPC tags from an OPC server into Security Center, you must import the type definition file into the OPC Client plugin.

Before you begin

Create the XML type definition file.

What you should know

The XML file is validated when the plugin starts.

IMPORTANT: The entity type definitions in the XML file are stored in the plugin database. After the XML file is imported, the entity types cannot be modified or deleted from Security Center by modifying or deleting them from the XML file.

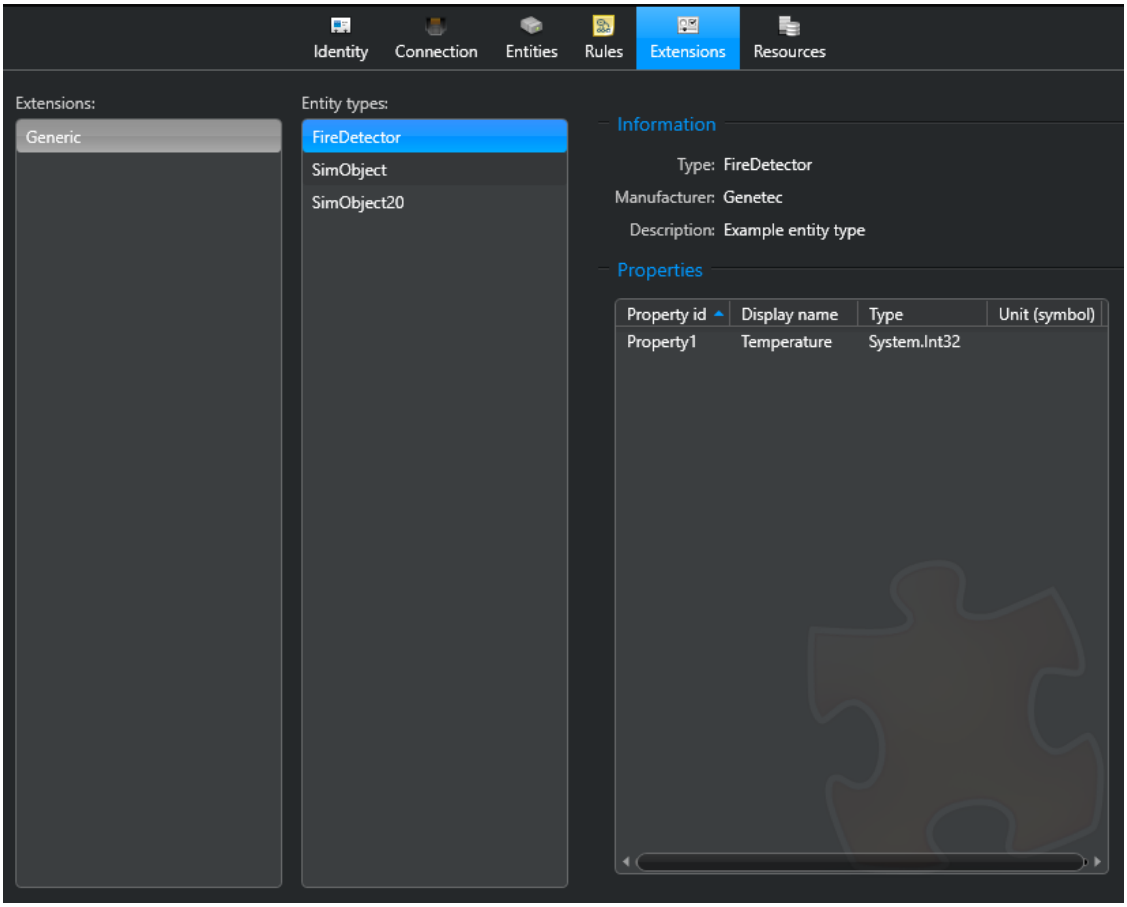
To delete or modify imported entity types, you must delete the plugin role and its database, create another instance of the plugin role, and create another XML file.

To add new entity types to Security Center, update the XML file to include the entity types under a unique name, and then reimport the file.

To import the XML type definition file into Security Center:

1. Copy your XML file to the OPC Client *Extensions* folder on the plugin server.
   The default location is *$\Program Files (x86)\Security Center Plugins\OPCClient\Extensions*.
2. If the OPC Client plugin role is already created, deactivate and then reactivate the role for the entity types to be loaded.
3. After the OPC Client role is created, verify that the **Generic** extension is loaded on the *Extensions* page of the OPC Client plugin.

Clicking the **Generic** extension displays the entity types and property information defined in the XML type definition file.



After you finish

Create a CSV import file.

Creating a CSV import file

Create a CSV file to map OPC tags to the properties defined in the XML type definition file, so that entities can be created in Security Center.

Before you begin

Create an XML type definition file.

What you should know

- Use a spreadsheet application, such as Microsoft Excel, to create and edit the CSV file. If you use Microsoft Word, the auto correct feature might remove commas that are required for the CSV to be valid.
- Read the rules for creating a valid CSV file.
- You can refer to *Template.csv.template*, which is located in *$\Program Files (x86)\Security Center Plugins \OPCClient\Extensions*.

To create the CSV import file:

1 Open a spreadsheet application like Microsoft Excel.

2 In the first row, enter the CSV headers listed in Headers in the CSV import file for OPC Client on page 25.

Most of the headers are mandatory and must be included. You can omit the optional headers, if they are not used by any of the entities listed in the file.

3 For each OPC entity, add a separate line for each property (*PROPERTY_ID*) that you want displayed in Security Center.

Example: In the following example, an OPC entity named `EntityA` has two properties, `Property1` and `Property2`. Notice that the `ENTITY_NAME` and `TYPE_NAME` are the same for both lines that define the properties of the same entity.

	A	B	C	D
1	ENTITY_NAME	TYPE_NAME	PROPERTY_ID	NODE_ID
2	EntityA	EntityTypeA	Property1	nsu=http://yourorganisation.org/TestOpcObjects/;s=Pin_A1
3	EntityA	EntityTypeA	Property2	nsu=http://yourorganisation.org/TestOpcObjects/;s=Pin_A2

4 Save the file as a CSV (comma separated values).

Example: *OPCEntities.csv*

You can save the file to any location on your network that the plugin server can access.

After you finish

Import the entities.

Rules for creating a valid CSV import file for the OPC Client plugin

If the CSV file you import from is set up correctly, entities and their corresponding properties are created in Security Center. When you try to import from an invalid CSV file, you see an error message that describes the problem.

For the CSV file to be set up correctly, make sure of the following:

- The file name ends with *.csv*.
- The headers are listed as required in Headers in the CSV import file for OPC Client on page 25.
- There are no duplicate headers.

- There is at least one line of content under the headers.
- In each line of content, there is a field for each header.

  For example, if there are 12 headers, each line must have 12 fields, even if the fields are blank.
- Each field is separated by a comma.
- Each property of an entity is defined on one line, meaning that each entity is represented by multiple lines.
- ENTITY_NAME and TYPE_NAME must be repeated for each property of an entity.
- Each line with the same ENTITY_NAME has the same TYPE_NAME.
- Each PROPERTY_ID exists in the XML for the given TYPE_NAME.
- Each PROPERTY_ID is defined only once for each TYPE_NAME.

Headers in the CSV import file for OPC Client

The CSV file contains the information used to create entities and their properties in Security Center.

In the CSV file, you specify the location of an OPC tag on the OPC server, choose which entity properties to import, and map those properties to an entity type that is defined in the XML type definition file.

The CSV headers listed as required in the following table must be included in the first line of the CSV file. Headers listed as optional can be omitted if they are not used by entities in the file.

CSV header	Include in file	Description
ENTITY_NAME	Required	Name for the new custom entity in Security Center. **NOTE:** Properties imported for the same entity must share the same entity name.
TYPE_NAME	Required	Name of an entity type that is defined in TypeName field of the XML file.
PROPERTY_ID	Required	ID of the property in the external system that is defined in the PropertyID field of the XML file.
DISPLAY_NAME	Optional	Name for the property that is displayed in Security Center. **NOTE:** If you do not include this parameter in the CSV file, the DisplayName defined in the XML file is used.
NODE_ID	Required	ID of the node for the OPC tag to read on the OPC server. **NOTE:** Use the following format: nsu=<namespaceUri>;<identifier_type_flag>=<identifier>
UNIT	Optional	The unit of measurement for the property. **NOTE:** If you do not include this parameter, the Unit that is defined in the XML file is used.
UNITSYMBOL	Optional	The symbol for the unit of measurement for the property. **NOTE:** If you do not include this parameter, the UnitSymbol that is defined in the XML file is used.

Example

In the following example, the entity type *FireDetector* is defined in the XML type definition file.

```
<EntityTypes>
  <EntityType>
    <Manufacturer>Genetec</Manufacturer>
    <TypeName>FireDetector3</TypeName>
    <Description>Example entity type</Description>
    <Properties>
     <Property>
       <PropertyId>Property1</PropertyId>
       <DisplayName>Temperature</DisplayName>
       <Type>System.Int32</Type>
       <Unit>Fahrenheit</Unit>
       <UnitSymbol>°F</UnitSymbol>
      </Property>
      <Property>
        <PropertyId>Property2</PropertyId>
        <DisplayName>Temperature</DisplayName>
        <Type>System.Int32</Type>
        <Unit>Celsius</Unit>
        <UnitSymbol>°C</UnitSymbol>
      </Property>
    </Properties>
  </EntityType>
</EntityTypes>
```

The following image shows the corresponding CSV file, which imports three Security Center entities of the type *FireDetector*: **EntityA**, **EntityB**, and **EntityC**, each with two properties.

	A	B	C	D	E	F	G
1	ENTITY_NAME	TYPE_NAME	PROPERTY_ID	DISPLAY_NAME	NODE_ID	UNIT	UNITSYMBOL
2	EntityA	FireDetector	Property1		nsu=http://yourorganisation.org/TestOp		
3	EntityA	FireDetector	Property2		nsu=http://yourorganisation.org/TestOp		
4	EntityB	FireDetector	Property1		nsu=http://yourorganisation.org/TestOp		
5	EntityB	FireDetector	Property2		nsu=http://yourorganisation.org/TestOp		
6	EntityC	FireDetector	Property1	Temperature 1	nsu=http://yourorganisation.org/TestOp		
7	EntityC	FireDetector	Property2	Temperature 2	nsu=http://yourorganisation.org/TestOp		

- Entities **EntityA**, **EntityB**, and **EntityC** are mapped to the entity type *FireDetector*.
- The properties of **EntityA** and **EntityB** will be displayed in Security Center as *Temperature*, as defined in the XML type definition file.
- The properties of **EntityC** will be displayed in Security Center as *Temperature 1* and *Temperature 2*, even though *Temperature* is configured as the **DisplayName** in the XML file. The **DISPLAY_NAME** value in the CSV file overrides the **DisplayName** value in the XML file.
- No **UNIT** or **UNITSYMBOL** values are included in the CSV file, so they are taken from the XML file.

Importing OPC tags into Security Center

To monitor OPC tags from an OPC server in Security Center, you must create OPC entities using the OPC Client plugin.

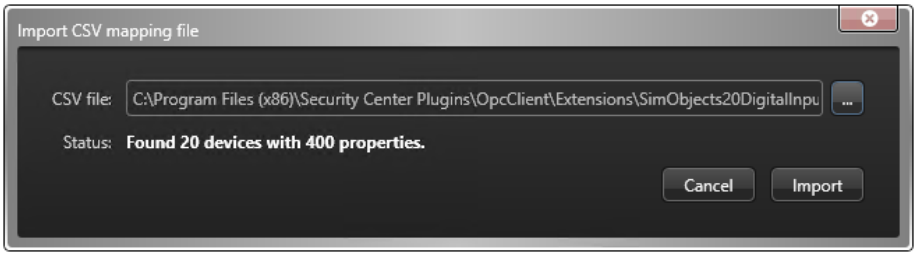
Before you begin

- Create and import the XML type definition file.
- Create the CSV file.

To import OPC tags into Security Center:

1 From the Config Tool home page, open the *Plugins* task.
2 Select the OPC Client plugin from the entity browser, and click the **Entities** tab.
3 At the bottom of the list of entities, click **Import from CSV**.
4 In the *Import CSV mapping file* dialog box, select the CSV file.

In the **Status** field, if the CSV file is configured properly, the number of devices and properties found is displayed. If the CSV file is not configured properly, an error message is displayed indicating the first line in which an error is found.

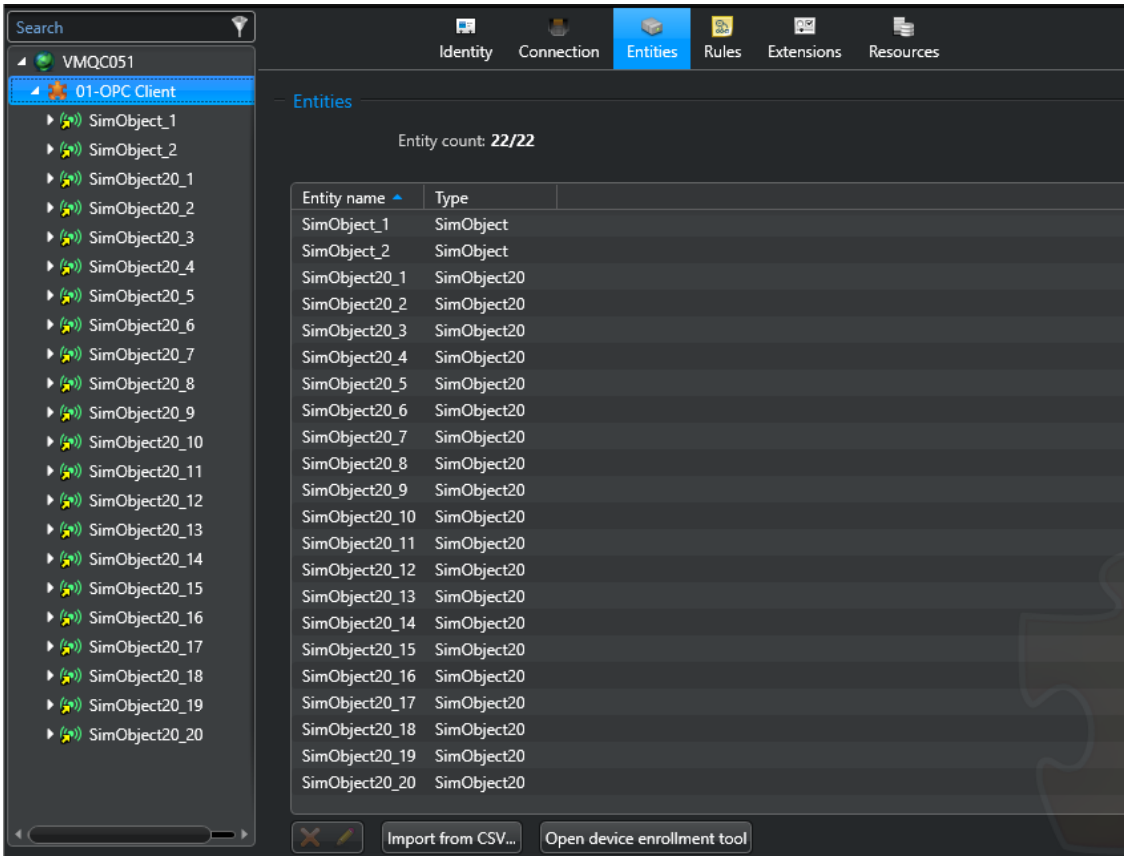


5 Click **Import**.

NOTE: You can view the status of the import from the notification tray.

The number of Security Center entities that were created is displayed in the **Entity count** field.

The entities are displayed in the entity browser, and listed in the *Entities* section of the plugin. You can view entity properties on the *Properties* page of each entity. The entity states are synchronized with the OPC server.



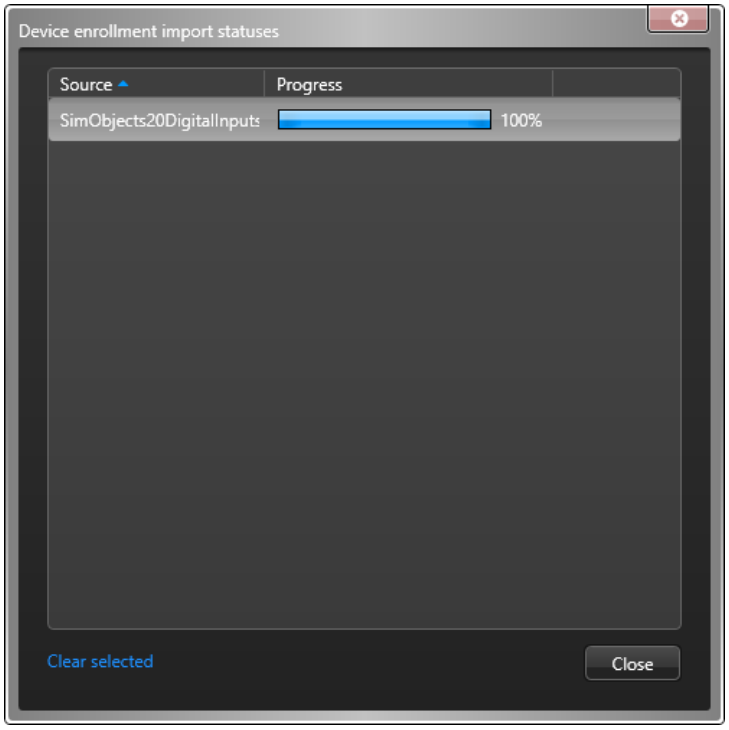
Enrollment statuses of OPC devices

When importing OPC tags from a CSV file to enroll OPC devices in Security Center as OPC entities, you can view the progress of the import in Config Tool. After the import, you can view which devices were added, already added, or undiscovered.

Notification tray icons

The status of the import is displayed in the Config Tool notification tray.

- The **Open device enrollment import statuses** icon is blue when the import is in progress, and then turns green when the import is complete (>).
- Clicking the icon opens the *Device enrollment import statuses* window, which displays the progress of the import.



Enrollment statuses of OPC devices

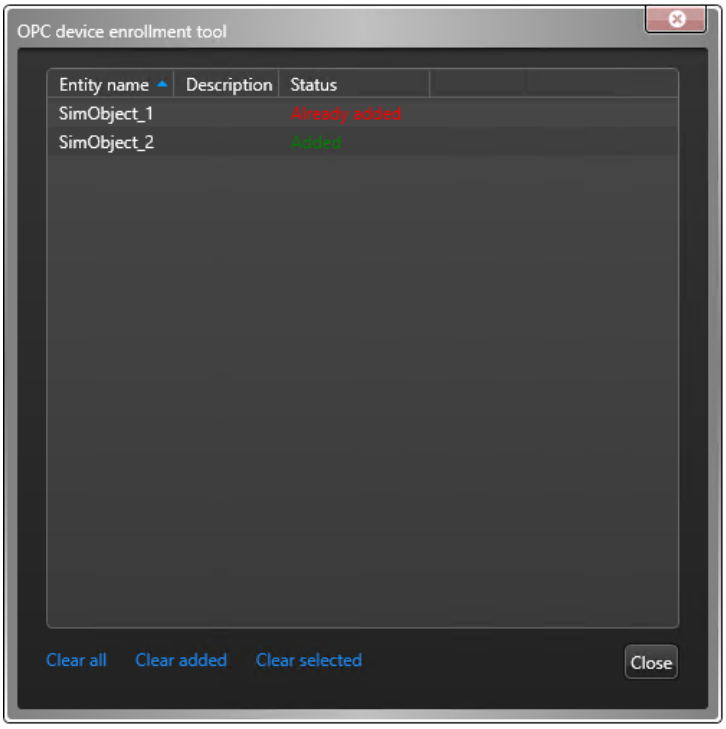
In the *OPC device enrollment tool* window, all the entities that were created for OPC devices are listed. One of the following statuses is displayed beside each entity:

- **Added:** The device was discovered on the OPC server and an entity was successfully created in Security Center.
- **Already added:** An entity was already created in Security Center for the device. No duplicate entity is created.
- **Undiscovered:** The device was not found on the OPC server. No entity was created in Security Center for this device.

You can access the *OPC device enrollment tool* window by clicking **Open device enrollment tool** from the *Entities* page of the OPC Client plugin.

Example

The following image shows the *OPC device enrollment tool* window.


OPC device enrollment tool
Entity name
Description
Status
SimObject_1
Already added
SimObject_2
Added
Clear all
Clear added
Clear selected
Close

5

Configuring OPC entities

This section includes the following topics:

- "Creating rules for state changes of OPC entity properties" on page 32
- "Linking cameras to OPC entities" on page 35
- "Renaming OPC entities from Config Tool" on page 36
- "Editing properties of OPC entities from Config Tool" on page 37

Creating rules for state changes of OPC entity properties

To receive events and alarms in Security Center when the states of OPC tags change on the OPC server, you can set up rules for the associated OPC entity properties using the rule engine of the OPC Client plugin.

Before you begin

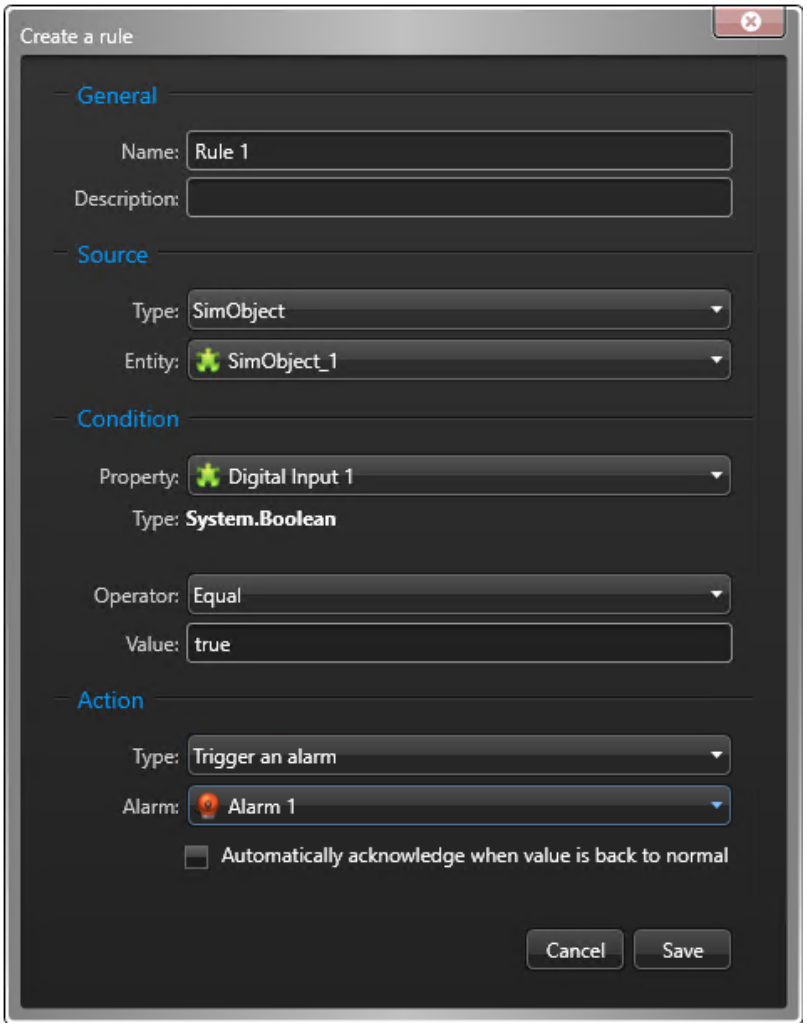
Create custom events in Config Tool. For information about creating custom events, see the *Security Center Administrator Guide*.

What you should know

When a rule is created for OPC entity properties, the plugin subscribes to data changes for the properties selected in the rule configuration. When data changes are received by the plugin, the rule is evaluated. If the value received matches the conditions in the rule, then either an event or an alarm is triggered, according to the configured action.

To create a rule for the state change of an OPC entity property:

1 From the Config Tool home page, open the *Plugins* task.
2 Select the OPC Client plugin from the entity browser, and click the **Rules** tab.
3 At the bottom of the *Rules* page, click  .
4 In the *Create a rule* dialog box, enter the following parameters for the rule:



- **General:**
  - **Name:** Enter a name for the rule.
  - **Description:** Enter a description for the rule.
- **Source:**
  - **Type:** Select the type of OPC entity to monitor.
  - **Entity:** Select a specific OPC entity to monitor, or select **All** to monitor all OPC entities of the same type.
- **Condition:**
  - **Property:** Select which OPC entity property to monitor. When you select a property, its data type is displayed (boolean, string, and so on).
  - **Operator:** Select what the property value must be in relation to the **Value** option (equal to, not equal to, lesser than, greater than, and so on) in order to trigger the event.
  - **Value:** Enter a value that the **Operator** is tested against.
- **Action:**
  - **Type:** Select either **Raise a custom event** or **Trigger an alarm**.
  - **Event:** This option is displayed when you select **Raise a custom event** as the action type. Select which custom event to trigger.

- **Alarm:** This option is displayed when you select **Trigger an alarm** as the action type. Select which alarm to trigger.
  NOTE: You can select the option **Automatically acknowledge when value is back to normal**, so that you do not have to manually acknowledge the alarm after if it is triggered.

5 Click **Save**.

Events and alarms are triggered in Security Desk based on the rules you created. For more information about monitoring events in Security Desk, see the *Security Desk User Guide*.

Linking cameras to OPC entities

Link cameras to OPC entities in Security Center, so that when an event or an alarm is triggered from a rule created for those entities, you can see the cameras' video feed in Security Desk. If configured, video is recorded automatically, so you can investigate an event at any time.

Before you begin

Add and configure cameras in Security Center. For more information, see the *Security Center Administrator Guide*.

To link a camera to an OPC entity:

1 From the Config Tool home page, open the *Plugins* task.
2 In the *Plugins* task, expand the OPC Client plugin role from the entity browser.
3 Select an entity, and then click the **Attached cameras** tab.
4 In the *Attached cameras* section, click **Attach camera** ( ).
5 In the dialog box that opens, select a camera, and then click **OK**.

The camera is listed in the *Attached cameras* section. When an event or alarm is triggered from a rule for an entity with a linked camera, the video feed is displayed in Security Desk.

After you finish

Configure the camera settings of the cameras you linked to OPC entities. For more information, see "Configuring camera settings" in the *Security Center Administrator Guide*.

Renaming OPC entities from Config Tool

After creating OPC entities in Security Center, you can rename them in Config Tool.

To rename an OPC entity from Config Tool:

1 From the Config Tool home page, open the *Plugins* task.
2 Select the OPC Client plugin from the entity browser, and click the **Entities** tab.
3 From the list of entities, select the entity you want to rename, and then click  at the bottom of the list.
4 In the *Rename entity* dialog box, enter a new name.
5 Click **OK**.

The entity name is updated.

Editing properties of OPC entities from Config Tool

After adding OPC entities in Security Center, you can rename their properties, and add the unit of measurement and symbol of their properties in Config Tool.

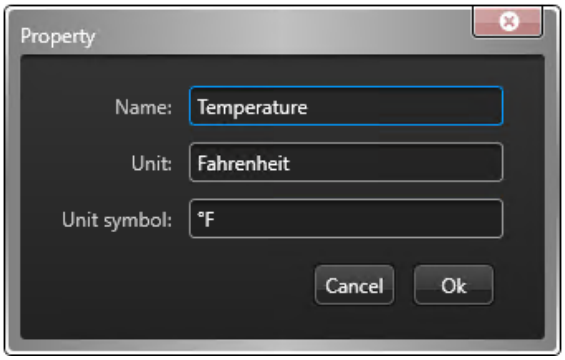
To edit a property of an OPC entity from Config Tool:

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

2 Select expand the OPC Client plugin from the entity browser, and then select an OPC entity.

3 From *Properties* page of the entity, select the property you want to edit, and then click at the bottom of the list.

4 In the *Property* dialog box, edit the following fields:



- **Name:** Enter a new name for the property.
- **Unit:** Enter a unit of measurement for the property.
- **Unit symbol:** Enter the symbol of the unit that will be displayed where available space is limited.

5 Click **OK**.

The property information is updated.

6

Monitoring OPC entities

This section includes the following topics:

- "About monitoring OPC entities" on page 39
- "Reviewing OPC Client rule engine events in Security Desk" on page 41

About monitoring OPC entities

You can monitor state changes of OPC entity properties by receiving custom events and alarms generated by the OPC Client rule engine, or by viewing the changes from Security Desk and Config Tool.

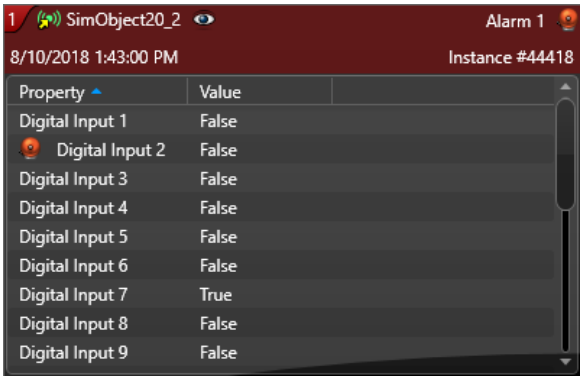
State change monitoring in Config Tool

From the *Properties* page of an OPC entity, you can view real-time state changes of the associated properties by enabling **Live monitoring** ( ) at the bottom of the list of properties.

State change monitoring in Security Desk

In addition to native Security Center functionality in the *Monitoring*, *Alarm monitoring*, and *Maps* tasks, when monitoring an OPC entity in a canvas tile or from a map, you can also view data changes of all the properties of that entity in real time.

This view is available by clicking , and then selecting the option named after the OPC entity.



OPC entities on maps

You can monitor custom events and alarms generated by the OPC Client rule engine from the Security Desk *Maps* task.

OPC entities are displayed on maps as custom map objects. The color of the corresponding map object reflects the status of the entity.

- The icon is green when the entity is online ( ).
- The icon is yellow when the entity is in warning ( )

  NOTE: The entity is yellow if there is an error in one of its properties, for example, an invalid node ID.
- The icon is red when the entity is offline ( ).

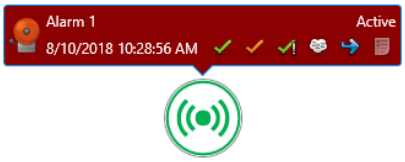
For more information on creating maps, refer to the *Security Center Administrator Guide*.

Custom events and alarms

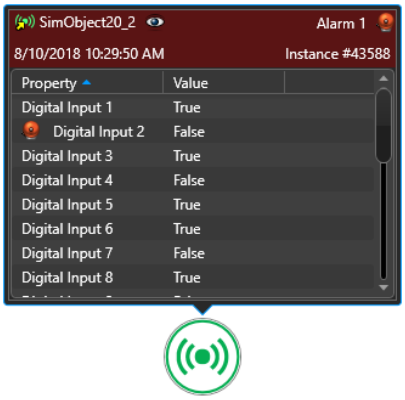
When custom events and alarms generated by the OPC Client rule engine are triggered, you can view them on the map.

- When an event is triggered, the event information is displayed above the OPC map object. Clicking the event information displays the video feed of the linked camera. If no camera is linked to that entity, real-time property information is displayed.

- When an alarm is triggered, an alarm icon is displayed above the OPC map object. Hovering over the alarm icon displays the alarm acknowledgment commands.



- Clicking the alarm icon displays the video feed of the linked camera. If no camera is linked to that entity, real-time property information is displayed. An alarm icon is displayed next to the property that the alarm was triggered by.



Reviewing OPC Client rule engine events in Security Desk

Using the *OPC event report* task in Security Desk, you can generate a report on custom events triggered by state changes of OPC entity properties.

To review past OPC Client events in Security Desk:

1 From the Security Desk home page, open the *OPC event report* task.

2 Set up the query filters for your report. Select one or more of the following filters:

- **Entities:** Select which OPC entities to investigate.
- **Events:** Select the Security Center custom events that were triggered based on the rules you created for the imported OPC tags using the rule engine of the OPC Client plugin.
- **Time range:** Define the time range for the query. The range can be defined for a specific period or for global units of time, such as the last day or the last week.

3 Click **Generate report**.

The events are listed in the report pane.

After you finish

You can print or export the report.

Technical support

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

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

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

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

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

Additional resources

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

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

Licensing

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

Hardware product issues and defects

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

Where to find product information

You can find our product documentation in the following locations:

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