OPC Client Plugin Guide 3.0

Copyright notice

Document information

Document title: OPC Client Plugin Guide 3.0

Document number: EN.720.039-V3.0.B(1)

Document update date: June 21, 2017

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) Clients in Security Center.

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

- Security Center 5.6 systems
- Configuration and use of OPC systems.

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 Inc.

Contents

Preface: Preface

Chapter 1: Introduction to OPC Client plugin

Chapter 2: Release notes

Chapter 3: Installing OPC Client plugin

Chapter 4: Configuring OPC Client plugin

Chapter 5: Using the OPC Client plugin

1

Introduction to OPC Client plugin

This section includes the following topics:

What is the OPC Client plugin?

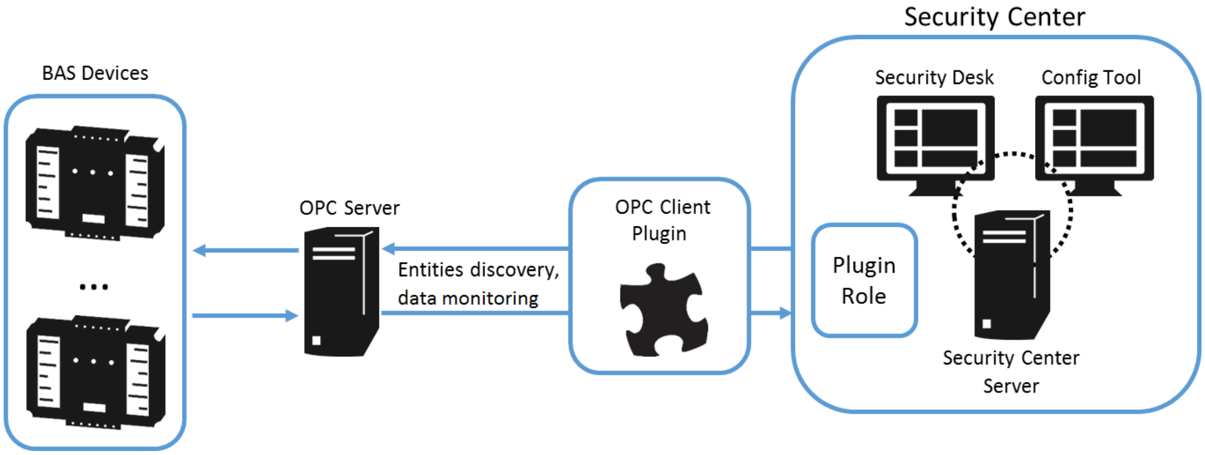
The Open Platform Communications (OPC) Client plugin is a communication protocol plugin that integrates an OPC Client to Security Center. The plugin will support and monitor any OPC device in Security Center.

You can use the plugin to:

- Import OPC tags from an OPC Server and monitor in Security Center.
- Integrate and monitor OPC devices in Security Center.
- Generate events based on sensor information and create events-to-action in Security Center.

How it works

The OPC Client plugin hosts an OPC compliant client, which means that through the integration Security Center becomes the OPC Client application. The OPC Client plugin role can connect to an OPC Server, and OPC tags or objects from the external system will be imported in Security Center as custom tile plugin entities using a mapping file. Communication between Security Center and the OPC Server uses the OPC protocol.



2

Release notes

This section includes the following topics:

What's new in OPC Client plugin 3.0

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

The OPC Client plugin 3.0 is a new integration for Security Center 5.6 SR1.

Known issues in OPC Client plugin 3.0

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 3.0 includes the following known issues.

Issue	Description
940039	If the plugin is not restarted after a restore, the database is overwritten. **Workaround:** Restart the plugin immediately after the database restore.
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. **Workaround:** Make sure that the custom event IDs, used in the rules, are created on the system before restoring a database. Otherwise, make sure that all rules in the restored database are properly re-configured with the new custom events.
949351	You do not have the option to change the OPC Client XML mapping file after it is selected. **Workaround:** Delete and recreate the plugin to change the XML file.

Limitations in OPC Client plugin 3.0

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

The OPC Client plugin 3.0 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.
976415	OPC Client 3.0 does not support events from the external system.

Compatibility for OPC Client plugin 3.0

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

OPC Client plugin 3.0 is compatible with the following systems:

- Security Center 5.6 SR1 and later
- OPC UA servers

  NOTE: If your OPC Server uses the DA (Data Access) or AE (Alarms and Events) specification, you must configure an OPC DA or AE to UA Gateway on the server so that the OPC Client plugin role can communicate properly with the server.

3

Installing OPC Client plugin

This section includes the following topics:

Installing the OPC Client plugin

The OPC Client 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 5.6 SR1 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 Client plugin, and has the valid part number for the plugin (GSC-1PBAS-OPC-C). This part number supports 100 devices. For additional devices, you can use a different part number (GSC-1PBAS-100D).

  NOTE: The license number is included in the product-release email sent by the product manager of Genetec Inc. 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, according to the configuration of your system:

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

To install the OPC Client plugin:

1. Download the OPC Client 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 immediately. However, you must restart the Genetec™ Server to complete the plugin installation.

After you finish

Create the OPC Server plugin role.

4

Configuring OPC Client plugin

This section includes the following topics:

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

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, the database for the plugin role, and then click **Next**.

   If you are not using an expansion server, the option to select a server 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. We recommend that a unique database name be designated to each role upon creation. Example: OPCClient_Plugin1, OPCClient_Plugin2, OPCClient_Plugin3, etc. Do not use the default database name.

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 Client plugin role appears in the entity browser. The plugin role is red, because it is not yet connected to an OPC Server.

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

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.

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

1. From the home page in Config Tool, open the *Plugins* task.
2. Select the OPC Client plugin from the entity browser, and click the **Connection** tab.
3. In the **Server** option, 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, type the IP address and port number of the OPC Server, and then click **Start**.
        3. Select one of the available server endpoints and click **Select**.
4. If you did not automatically discover the available endpoints and security options of the OPC server, configure them as follows:
    a) From the **Security policy** drop-down list, select the algorithm for how messages from the OPC Server are signed and encrypted.

    b) From the **Message security** drop-down list, 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.

    c) From the **Scheme** drop-down list, 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. Type 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.
5. 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**.
6. Click **Apply**.

Security Center is connected to the OPC Server. The **Server status** changes from **Disconnected** to **Connected**.

After you finish

If Security Center requires a valid certificate to connect to the server, you must trust the client certificate on the OPC Server.

Creating a mapping file for the OPC Client plugin

Before you can import OPC tags from an OPC Server in Security Center, you must create a mapping file for the OPC Client plugin that defines how OPC tags should be interpreted in Security Center.

What you should know

The mapping file is an XML file that provides metadata about the external system entities (OPC tags or objects) you want to import. The file defines the structure and properties of the external system entities, and how to interact with those entities and their properties in Security Center.

Using the XML mapping file, you can explicitly define which entities to import using a CSV file, which works in conjunction with the XML mapping file.

To create a mapping file:

1. In the XML file, define entity types.
2. Select the following mapping scheme to specify which external system entities to import in Security Center:
   - In a CSV file, map entities explicitly.

How entity types are defined in mapping files

The first thing you must define in an XML mapping file for the OPC Client plugin are the entity types.

An entity type defines how the external system entities (OPC tags and objects) of that type are interpreted in Security Center. Each entity type in the mapping file must include a name and property definitions.

The following XML tags must be included in the mapping file for each entity type:

XML tag	Description
BaseEntityType	Root XML tag to create a custom entity type.
TypeName	Name for the custom entity type in Security Center. This value must be unique.
CustomPropertyDefinitions	Section that defines a property for the entity type, which is nested in a <PropertyDefinitions> tag. You must add one <CustomPropertyDefinitions> section per property.
ESPropertyName	Name of the property on the external system.
SCPropertyName	Name for the property that is displayed in Security Center.

XML tag	Description
`Type`	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`	This column is used to set a default unit of measurement for this property.
`UnitSymbol`	This column is used to set a default unit of measurement for this property.

Example

The following section of code defines an entity type that is called **FireDetector** when it is imported in Security Center. The **Property1** integer property of the entity type is renamed to **Temperature** in Security Center.

```
<EntityTypes>
  <BaseEntityType xsi:type="CustomEntityType">
    <TypeName>FireDetector</TypeName>
    <PropertyDefinitions>
      <CustomPropertyDefinition>
        <ESPropertyName>Property1</ESPropertyName>
        <SCPropertyName>Temperature</SCPropertyName>
        <Type>System.Int32</Type>
        <Unit>Fahrenheit</Unit>
        <UnitSymbol>°F</UnitSymbol>
      </CustomPropertyDefinition>
    </PropertyDefinitions>
  </BaseEntityType>
</EntityTypes>
```

How to map external system entities using a CSV file

After you define entity types in the XML mapping file for the OPC Client plugin, you can explicitly select which external system entities (OPC tags or objects) to import in Security Center using a CSV file.

To import entities using a CSV file, you specify a location on the OPC Server and which entity properties to import, and map those properties to an entity type that is defined in the XML mapping file.

The CSV file must include the following information:

CSV header	Description
`ENTITY_NAME`	A name for the new custom entity in Security Center.
`ENTITY_PATH`	Location on the OPC Server from which to map the external system entities. The path should use the following format: */0:Objects/NamespaceIndex:Subfolder/NamespaceIndex:Subfolder*
`TYPENAME`	Name of an entity type that is defined in the mapping file. This value must match the `TypeName` value of that entity type.
`ESPROPERTYNAME`	Name of the property on the external system, that is defined in the `ESPropertyName` value in the mapping file.
`SCPROPERTYNAME`	(Optional) Name for the property that is displayed in Security Center. If you do not include this parameter, the `SCPropertyName` that is defined in the mapping file is used.
`PROPERTY_PATH`	The exact path to the property on the external system that you want to map. This value must be unique on each line of the CSV.
`UNIT`	This column is used to set a default unit of measurement for this property.
`UNITSYMBOL`	This column is used to set a default unit of measurement for this property.

Example

In the following example, the entity type *AirConditioner* is defined in the XML mapping file.

```
<EntityTypes>
  <BaseEntityType xsi:type="CustomEntityType">
    <TypeName>EntityTypeA</TypeName>
    <PropertyDefinitions>
      <CustomPropertyDefinition>
        <ESPropertyName>Property1</ESPropertyName>
        <SCPropertyName>Count</SCPropertyName>
        <Type>System.Int32</Type>
        <Unit>Fahrenheit</Unit>
        <UnitSymbol>°F</UnitSymbol>
      </CustomPropertyDefinition>
      <CustomPropertyDefinition>
        <ESPropertyName>Property2</ESPropertyName>
        <SCPropertyName>IsOpen</SCPropertyName>
        <Type>System.Boolean</Type>
      </CustomPropertyDefinition>
    </PropertyDefinitions>
  </BaseEntityType>
```

```
</EntityTypes>
```

The corresponding CSV file imports three Security Center entities of type *AirConditioner*: **EntityA**, **EntityB**, and **EntityC**. The properties of **EntityA** and **EntityB** use the property names that are defined in the XML mapping file. PropA_1 and PropA_2 map to the `Property1` property of entity type *AirConditioner*, which is mapped to the `Count` property in Security Center. PropB_1 and PropB_2 are mapped to the `Property2` property of entity type *AirConditioner*, which is mapped to the `IsOpen` property in Security Center.

EntityC is also mapped to the entity type *AirConditioner*, but its property `PropA_3` is renamed in Security Center to `Temperature`, and its property `PropB_3` is renamed to `IsActive`.

```
ENTITY_NAME,ENTITY_PATH,TYPENAME,ESPROPERTYNAME,SCPROPERTYNAME,PROPERTY_PATH,UNIT,
UNITSYMBOL
EntityA,/0:Objects/2:FolderName,EntityTypeA,Property1,,/Objects/FolderName/PropA_1
EntityA,/0:Objects/2:FolderName,EntityTypeA,Property2,,/Objects/FolderName/PropB_1
EntityB,/0:Objects/2:FolderName,EntityTypeA,Property1,,/Objects/FolderName/PropA_2
EntityB,/0:Objects/2:FolderName,EntityTypeA,Property2,,/Objects/FolderName/PropB_2
EntityC,/0:Objects/2:FolderName,EntityTypeA,Property1,Temperature,/Objects/
FolderName/PropA_3,Celcius,°C
EntityC,/0:Objects/2:FolderName,EntityTypeA,Property2,IsActive,/Objects/FolderName/
PropB_3
```

Importing OPC tags and events in Security Center

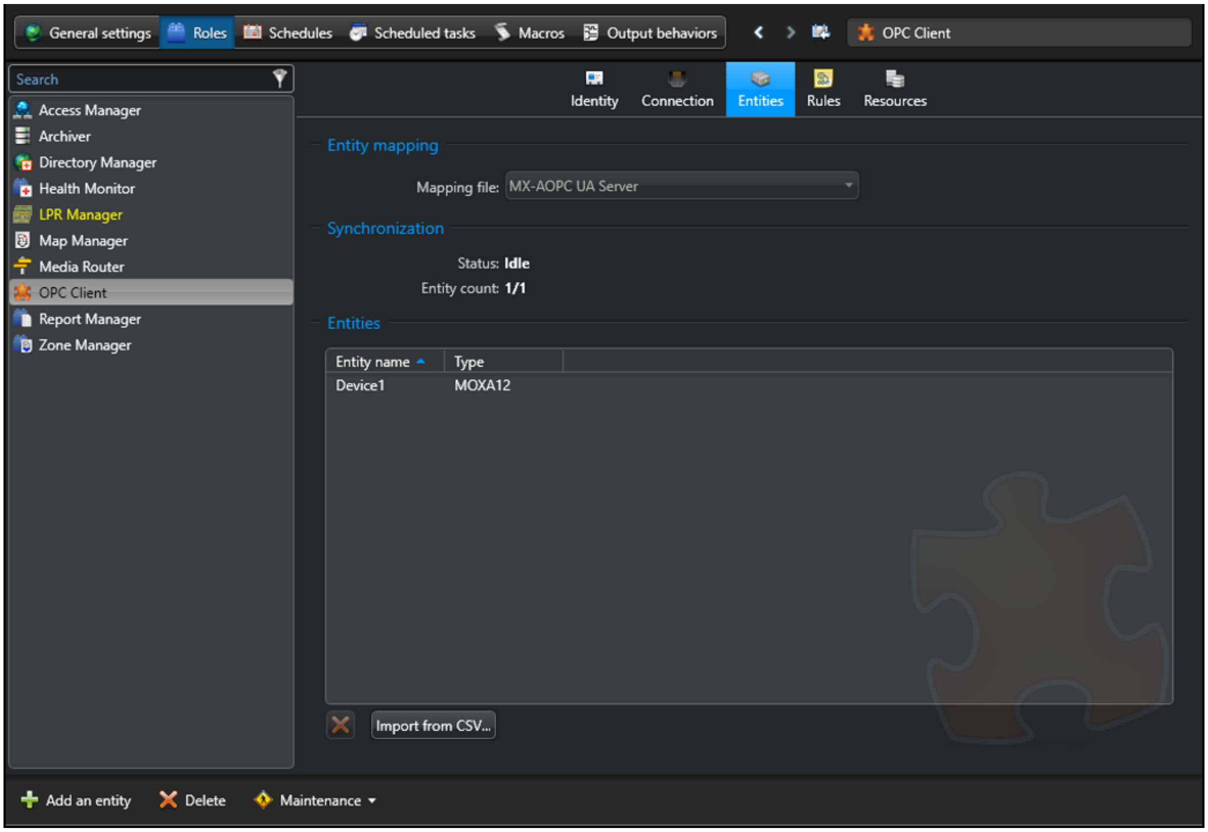
To monitor OPC tags from an OPC Server in Security Center using the OPC Client plugin, you must import the OPC tags by selecting a mapping file.

Before you begin

Create the mapping file.

To import OPC tags and events in Security Center:

1 From the home page in Config Tool, open the *Plugins* task.
2 Select the OPC Client plugin from the entity browser, and click the **Entities** tab.
3 In the **Mapping file** field, select the mapping file.
4 Click **Import from CSV** in the *Synchronization* section, browse to and select the CSV file, and then click **Import**.
5 To delete an entity, select the entity and click (✖).



Mapping file: MX-AOPC UA Server

Status: Idle
Entity count: 1/1

Entity name	Type
Device1	MOXA12

The number of Security Center entities that were mapped or created displays next to the **Entity count** field. If there is an error in the mapping file, an `XML validation error` message displays next to the **Status field**.

The imported Security Center entities that were mapped or created display under the OPC Client plugin role in the entity browser and in the Plugin’s Entities page. You can view the properties of the imported entities in the *Entity information* tab of each tile plugin entity. The entity states are synchronized from the OPC Server.

Creating rules for state changes of OPC tags

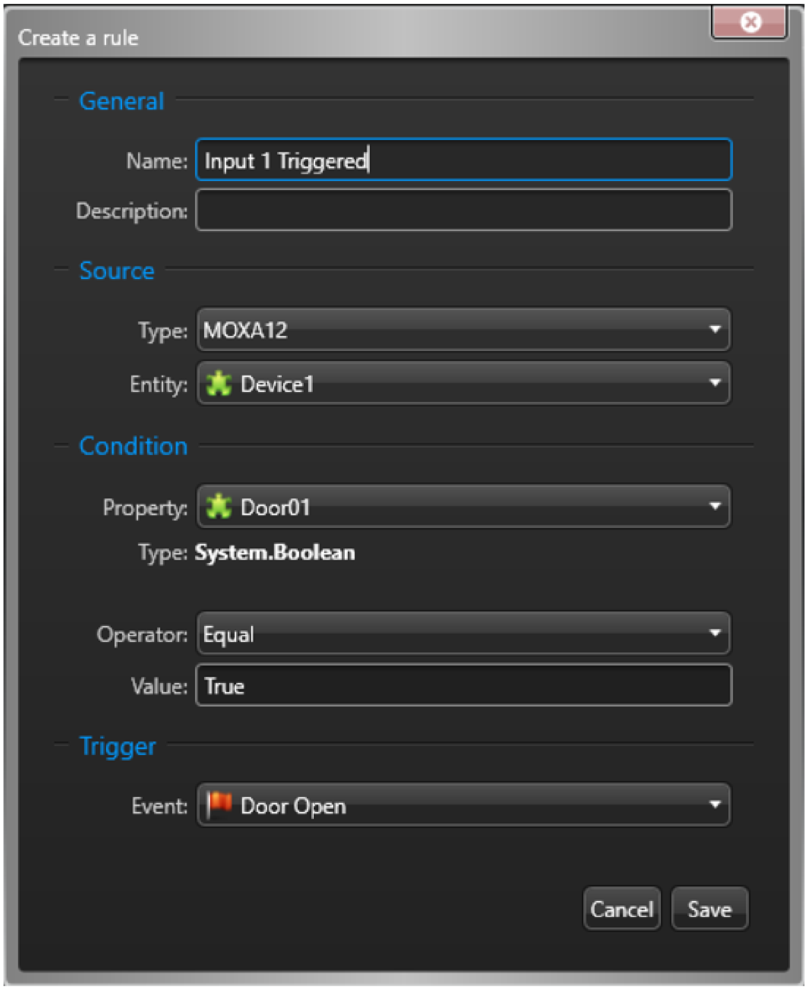
To receive events in Security Center when the states of OPC tags change on the OPC Server, you can set up rules for the imported entities from the OPC Client plugin role.

Before you begin

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

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

1. From the home page in Config Tool, 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* tab, click +.
4. In the *Create a rule* dialog box, enter the following parameters for the rule:



Name: Input 1 Triggered
Description:
Type: MOXA12
Entity: Device1
Property: Door01
Type: System.Boolean
Operator: Equal
Value: True
Event: Door Open

- **Name:** Type a name for the rule.
- **Description:** Type a description for the rule.
- **Type:** Select the type of OPC tag to monitor.
- **Entity:** Select a specific OPC tag to monitor, or select **All** to monitor all OPC tags of the same type.

- **Property:** Select which OPC tag 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:** Type a value that the **Operator** is tested against.
- **Trigger:** Select which custom Security Center event to trigger.

5 Click **Save**.

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

5

Using the OPC Client plugin

This section includes the following topics:

Reviewing past OPC events in Security Desk

To review and investigate events from the OPC Server, as well as events that were triggered in Security Center based on state changes of OPC tags, you can use the *OPC events* report in Security Desk.

To review past OPC Server events in Security Desk:

1. From the home page in Security Desk, open the *OPC events* report.
2. Set up the query filters for your report. Choose one or more of the following filters:
   - **Entities:** Select which OPC tags to investigate.
   - **Events:** Select the Security Center custom events that were triggered based on the rules you created for the imported OPC tags in the *Rules* tab of the OPC Client plugin role.
   - **Time range:** Define the time range for the query. The range can be defined for a specific period of time 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. The following report pane columns are available for this report:
   - **Event:** Event name.
   - **Timestamp:** Date and time that the event occurred.
   - **Entity:** OPC tag (tile plugin entity) that triggered the event.
   - **Message:** Message related to the OPC Server event. This report column does not apply to events that were triggered based on rules you created for the OPC Client plugin.

After you finish

Using the OPC Client you can also view, in real-time, data changes in the Config Tool and incoming events using the monitoring task inSecurity Desk.

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 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 employees of Genetec Inc. to communicate with each other and discuss many 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.

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. Genetec 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.