Genetec™ Security Center.

# Tag Tracker Plugin Guide 3.0

Genetec™

# Copyright notice



### Document information

Document title: Tag Tracker Plugin Guide 3.0

Document number: EN.550.XYZ.VX.Y(1)

Document update date: January 14, 2019

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

# About this guide

This guide describes how to integrate barcode scanner in Security Center using the Tag Tracker plugin, so that you can use Security Center to manage and monitor the scanners.

This guide supplements the documentation provided with Security Center and your other systems and devices. 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
- Datalogic scanners and/or usb barcode scanners

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 website.

### 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:

1

# Introduction to the Tag Tracker plugin

This section includes the following topics:

# What is the Tag Tracker plugin?

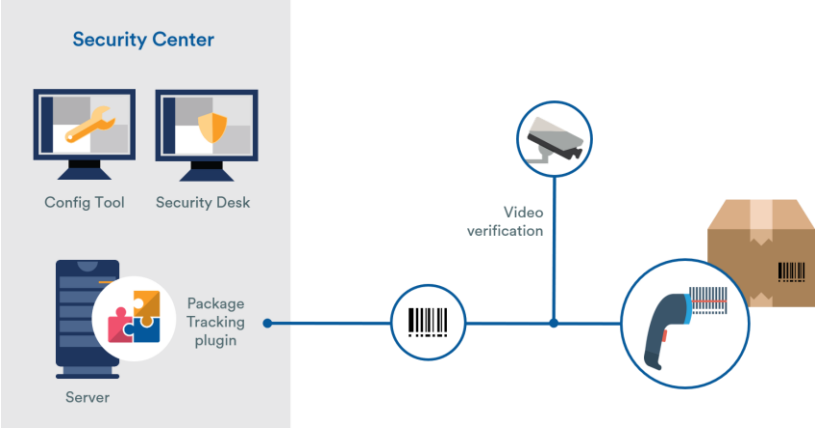
The Tag Tracker integration allows you to configure barcode scanner and track scans history in security center.

The integration allows you to do the following:

- Integrate Datalogic or USB based scanner devices in Security Center
- Add scanners to Area
- Associate multiple cameras to scanners
- Generate reports of scans filtered by barcode (full or partial), scanner, date, …
- See video feed associated to every scan in the report
- Live monitoring of scanners with associated video feed

# How the Tag Tracker plugin works with Security Center

The Tag Tracker plugin allows to receive reads from third party scanners and display them, either using live monitoring of reporting, along associated video feed.  It also embeds read code in the video, as overlay and bookmark, to easily investigate barcode history.




## Components

The following components comprise a Tag Tracker integration in Security Center.

- A connected scanner.  Tag Tracker can be configured so that when a barcode is scanned, it persists it for future investigation and trigger a live event.
- An optional Tag Tracker bridge (for generic USB scanner only), represented by a scanner unit, that will receive the scans from the scanner and propagate them to Security Center.
- The Genetec™ Tag Tracker plugin defines the connection information for the different scanners and provides the barcode reports in Security Center. The plugin must be installed on every Security Center computer that will be used to generate Tag Tracker reports.

2

# Release notes

This section includes the following topics:

# Supported devices

When you have deployed the Tag Tracker plugin 3.0 in Security Center, you can integrate Datalogic devices.

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

**Certified**

The device has been tested and validated by Genetec Inc.

**Supported by design**

The device shares the same design characteristics as a certified device but has not been validated or tested by Genetec Inc.

| Model | Device type | Firmware ver. | Supported protocol | Certification |
|---|---|---|---|---|
| DS2400N | Laser bar code scanner | N/A | Telnet | Certified |
| DX8210 | Laser bar code scanner | N/A | Telnet | Supported by design |

- System requirements for the Tag Tracker plugin 3.0 on page 14
- License options for the Tag Tracker plugin on page 16

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

In addition to a certificate for your plugin, make sure that your Security Center license includes all of the options you expect to use in Security Center. For example, if you integrated a system that has visitors, you need the Visitor Management option in Security Center. If an option is missing, a failure message is displayed when the server tries to create or modify the entity related to that option.

- For a list of available license options, see License options in Security Center. on page 16

# What's new in the Tag Tracker plugin 3.0

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

The Tag Tracker plugin 3.0 is a new integration for Security Center 5.7SR3.

# Known issues in the Tag Tracker 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.

There are no known issues in the Tag Tracker plugin 3.0.

# Limitations in the Tag Tracker plugin 3.0

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

The Tag Tracker plugin 3.0 includes the following known limitations.

| Issue | Description |
|---|---|
| 1745717 | When enrolling the same unit multiple times, the events will not always be linked to the good scanner. |
| 1748690 | We don't validate existing configuration when adding a new bridge, so we could enroll the same bridget twice (related to previous issue). |
| 1756242 | We don't read the Datalogic scanner's configuration, hence we only support comas |
| 1757070 | Changing the name of a scanner in CT is not reflected in the bridge and vice versa. |
| 1758629 | Unable to validate if we are communicating with a supported unit. Establishing a connection to something else than a Datalogic scanner unit will be displayed as a valid connection. |
| 1761947 | There is no visual difference between a scanner offline and deleted. |
| 1769152 | Report shows data from scanners in partition not available to the user. |
| 1817865 | The plugin accept connection to a Datalogic scanner in client mode.<br>**Workaround:** The datalogic scanner must be in server mode. |
| 1860087 | The overlay is created only after a first scan. |

# Product compatibility for the Tag Tracker plugin 3.0

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

The Tag Tracker plugin 3.0 is compatible with the following systems.

| Plugin name | Third-party name and version | Certified Security Center version |
|---|---|---|
| Tag Tracker 3.0 | N/A | 5.7 GA |

**IMPORTANT**:

- Datalogic didn't provide a protocol version to base our compatibility upon. It is a basic telnet connection with every scan as a single line of data terminated with a new line character. We had to assume that this will not change.

# Supported devices

When you have deployed the Tag Tracker plugin 3.0 in Security Center, you can integrate Datalogic devices.

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

**Certified**

The device has been tested and validated by Genetec Inc.

**Supported by design**

The device shares the same design characteristics as a certified device but has not been validated or tested by Genetec Inc.

| Model | Device type | Firmware ver. | Supported protocol | Certification |
|---|---|---|---|---|
| DS2400N | Laser bar code scanner | N/A | Telnet | Certified |
| DX8210 | Laser bar code scanner | N/A | Telnet | Supported by design |

# System requirements for the Tag Tracker plugin 3.0

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

### Plugin server

The Tag Tracker plugin 3.0 must be installed on a server that meets the recommended server specifications as described in the Security Center system requirements.

### Client workstation

The Tag Tracker plugin 3.0 must be installed on a workstation that meets the recommended computer specifications as described in the Security Center system requirements.

### GIS Maps

Maps must contain GIS coordinates, like in ArcGIS, Bing Maps and Google Maps. System requirements are the recommended hardware and software components that are required for your product and system to run optimally.

# License options for the Tag Tracker 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.

Use the following part numbers to get the license certificate for the plugin.

| Part number | Description | Requirements |
|---|---|---|
| GSC-1PBCODETRACKING | • Barcode tracking Plugin. 1 part required per barcode reader connected on plugin. | • Synergis™ Enterprise<br>• Omnicast™ Enterprise |

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

In addition to a certificate for your plugin, make sure that your Security Center license includes all of the options you expect to use in Security Center. For example, if you integrated a system that has visitors, you need the Visitor Management option in Security Center. If an option is missing, a failure message is displayed when the server tries to create or modify the entity related to that option.

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

3

# Installing the Tag Tracker plugin

This section includes the following topics:

- **Error! Reference source not found.** on page **Error! Bookmark not defined.**
-

| Step# | Description | Where to find more information |
|---|---|---|
| **Understand prerequisites and key issues before deploying** | | |
| 1. | Before installing the plugin, read the release notes to learn about new features, and to understand the requirements and known issues. | • What's new in the SDS Guardian plugin 3.0 on page 6<br>• Known issues in the SDS Guardian plugin 3.0 on page 7<br>• Limitations in the SDS Guardian plugin 3.0 on page 8 |
| 2. | Understand how the <third-party system> devices and components connect to Security Center | • How the SDS Guardian plugin 3.0 works with Security Center on page 3 |
| 3. | Learn which features are included with the extension. | • **Error! Reference source not found.** |
| **Deploy and configure your SDS Guardian system** | | |
| 4. | Make sure that your SDS Guardian system is operating as required by your organization, and that all its devices are operating as expected and available in Guardian Gateway. | • For instructions, refer to the SDS Guardian documentation. |
| **Install the plugin** | | |
| 5. | Verify that your Security Center license has a valid certificate for the SDS Guardian plugin. From the Config Tool home page, click **About** > **Certificates** to confirm that *Guardian Gunshot* 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.<br>• If you need to acquire a new license, refer to License options for the SDS |

| Step# | Description | Where to find more information |
|---|---|---|
| | | Guardian plugin on page 10. |
| 6. | Make sure the server where the plugin will be installed meets the recommended system requirements and is running a compatible version of Security Center. | • System requirements for the SDS Guardian plugin 3.0 on page 9<br>• Product compatibility for the SDS Guardian plugin 3.0 on page 8 |
| 7. | On the Security Center server, download the plugin and install it. | Downloading and installing the SDS Guardian plugin on page 14 |
| **Configure the plugin** | | |
| 8. | In Config Tool, create the Tag Tracker plugin role. | Creating the Plugin role on page 16 |
| 9. | Connect Security Center to the Guardian Gateway server. | Connecting to Guardian Gateway from Security Center on page 17 |
| **Test that the integration works as expected** | | |
| 10. | Arm an intrusion area. | In the Security Desk User Guide:<br>Arming intrusion detection areas |
| 11. | Verify that you can trigger an alarm from an intrusion area. | In the Security Desk User Guide:<br>Triggering alarms for an intrusion detection area |
| 12. | Verify that you can view video of the intrusion event. | In the Security Desk User Guide:<br>Investigating intrusion detection area events |
| 13. | Verify that you see events and alarms in the related Security Center reports. | In Security Desk, generate an **Alarm** report, **Incidents** report, and **Intrusion detection area activities** report. |
| **Set up your operators' client workstations** | | |
| 14. | On each Security Center client workstation from which you want to configure RPM II devices and perimeters (intrusion detection areas), install the plugin.<br>**Note:** When the plugin is installed on a Security Center server but not your Security Center client workstation, the client receives events and alarms, which you can view in the Monitoring task and the Event window. If you want to configure and view the RPM II entities in | Downloading and installing the Tag Tracker plugin |

| Step# | Description | Where to find more information |
|---|---|---|
| | Config Tool, you must install the extension on that client workstation. | |
| 15. | In the Monitoring task of Security Desk, add the RPM II intrusion detection role to the Event monitoring list and enable alarm monitoring. | |
| 16. | Test that your workstation works as expected. If it does, you have successfully completed the integration. | Do steps 22 to 25. |

- Downloading and installing the Tag Tracker plugin on page 18
- Upgrading the Tag Tracker plugin on page 22

# Process overview for the Tag Tracker plugin

Conveying the scans into Security Center as events consists of a series of steps that need to be followed in sequence.

| Step# | Description | Where to find more information |
|---|---|---|
| **Understand prerequisites and key issues before deploying** | | |
| 1. | Before installing the plugin, read the release notes to learn about new features, and to understand the requirements and known issues. | • What's new in the SDS Guardian plugin 3.0 on page 6<br>• Known issues in the SDS Guardian plugin 3.0 on page 7<br>• Limitations in the SDS Guardian plugin 3.0 on page 8 |
| 2. | Understand how the <third-party system> devices and components connect to Security Center | • How the SDS Guardian plugin 3.0 works with Security Center on page 3 |
| 3. | Learn which features are included with the extension. | • **Error! Reference source not found.** |
| **Deploy and configure your SDS Guardian system** | | |
| 4. | Make sure that your SDS Guardian system is operating as required by your organization, and that all its devices are operating as expected and available in Guardian Gateway. | • For instructions, refer to the SDS Guardian documentation. |
| **Install the plugin** | | |
| 5. | Verify that your Security Center license has a valid certificate for the SDS Guardian plugin. From the Config Tool home page, click **About** > **Certificates** to confirm that *Guardian Gunshot* 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.<br>• If you need to acquire a new license, refer to License options for the SDS Guardian plugin on page 10. |
| 6. | Make sure the server where the plugin will be installed meets the recommended system requirements and is running a compatible version of Security Center. | • System requirements for the SDS Guardian plugin 3.0 on page 9<br>• Product compatibility for the SDS Guardian plugin 3.0 on page 8 |
| 7. | On the Security Center server, download | Downloading and installing the SDS |

| Step# | Description | Where to find more information |
|---|---|---|
| | the plugin and install it. | Guardian plugin on page 14 |
| **Configure the plugin** | | |
| 8. | In Config Tool, create the Tag Tracker plugin role. | Creating the Plugin role on page 16 |
| 9. | Connect Security Center to the Guardian Gateway server. | Connecting to Guardian Gateway from Security Center on page 17 |
| **Test that the integration works as expected** | | |
| 10. | Arm an intrusion area. | In the Security Desk User Guide:<br>Arming intrusion detection areas |
| 11. | Verify that you can trigger an alarm from an intrusion area. | In the Security Desk User Guide:<br>Triggering alarms for an intrusion detection area |
| 12. | Verify that you can view video of the intrusion event. | In the Security Desk User Guide:<br>Investigating intrusion detection area events |
| 13. | Verify that you see events and alarms in the related Security Center reports. | In Security Desk, generate an **Alarm** report, **Incidents** report, and **Intrusion detection area activities** report. |
| **Set up your operators' client workstations** | | |
| 14. | On each Security Center client workstation from which you want to configure RPM II devices and perimeters (intrusion detection areas), install the plugin.<br>**Note:** When the plugin is installed on a Security Center server but not your Security Center client workstation, the client receives events and alarms, which you can view in the Monitoring task and the Event window. If you want to configure and view the RPM II entities in Config Tool, you must install the extension on that client workstation. | Downloading and installing the Tag Tracker plugin |
| 15. | In the Monitoring task of Security Desk, add the RPM II intrusion detection role to the Event monitoring list and enable alarm monitoring. | |

| Step# | Description | Where to find more information |
|---|---|---|
| 16. | Test that your workstation works as expected. If it does, you have successfully completed the integration. | Do steps 22 to 25. |

# Downloading and installing the Tag Tracker plugin

*[Step by step instructions for installing the plugin on your Security Center system. Example below.]*

To integrate SALTO in Security Center, you must install the SALTO plugin on all Security Center servers and client computers from which you want to manage SALTO entities.

## Before you begin

Make sure that your server meets the system requirements.

**To install the SALTO plugin:**

1. Download the SALTO installation package from the GTAP Product Download page.
2. In the package, browse to the *SALTO* folder.
3. Double-click the `setup.exe` file and follow the installation instructions in the wizard.
4. 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.
5. Close, and then open, any instances of Config Tool and Security Desk to load the plugin.

## After you finish

Create the Card Synchronization plugin role.

# Upgrading the Tag Tracker plugin

*[Step by step instructions for upgrading the plugin in your Security Center system. Example below.]*

If you already have Security Center access control integrated with CCURE, and you want to upgrade your CCURE system to version 2.30, 2.40, or 2.50, you also need to upgrade Security Center and the plugin.

### Before you begin

Perform the pre-installation tasks.

### What you should know

The plugin needs to be upgraded on Security Center client and server computers. It is not required to uninstall the plugin prior to upgrading to the new version.

**To upgrade the plugin:**

1. Close all instances of Config Tool and Security Desk.
2. Download the CCURE Access Control Plugin installation package from the GTAP Product Download page.
3. Double-click the *Genetec Security Center - CCure Access Control Plugin.exe* file, and follow the installation instructions.
4. After the plugin is upgraded, log on to Config Tool.
5. From the Config Tool home page, open the *Plugins* task.
6. In the *Plugins* task, select the CCURE access control plugin from the entity browser, and click the **Resources** tab.
7. In the database actions, click **Database update**.
8. When the database update is completed, restart the plugin role.

# 4

# Granting user privileges for the Tag Tracker plugin

*[Standard plugin configuration task. Example follow.]*

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

**NOTE:** You might require more, depending on the tasks you want to perform in Config Tool and Security Desk.

**To grant user privileges:**

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

2 Select the user that will monitor Tag Tracker, and click the **Privileges** tab.

3 Set the following privileges to **Allow**:

- View tile plugin properties
- Modify tile plugin properties
- Action privileges
- Radar Detection Zones
- Arm/Disarm radar detection zones
- Dismiss target
- Alert on target

| Privilege | Description |
|---|---|
| BuyTime activities | Allows the user to view and use the *BuyTime user activity report* task. |
| Postpone arming schedule | Allows the user to postpone arming schedules from the *Monitoring* task. |

- Set the following privileges to **Allow**:

  *[The following table is for intrusion detection panels and devices.]*

| Privilege | Task |
|---|---|
| Config Tool | To use Config Tool. |
| Security Desk | To use Security Desk. |
| Monitoring | To use the Monitoring task in Security Desk. |
| Intrusion detection | To use the Intrusion detection task in Security Desk. |
| Intrusion detection area activities | To use the Intrusion detection area activities task in Security Desk. |

| | |
|---|---|
| Intrusion detection unit events | To use the Intrusion detection unit events task in Security Desk. |
| View intrusion detection area properties | To view the intrusion detection area configuration pages in Config Tool. |
| Modify intrusion detection area properties | To modify the intrusion detection area configurations in Config Tool. |
| Add/delete intrusion detection areas | To add or delete intrusion detection areas in Config Tool. |
| View intrusion detection unit properties | To view the intrusion detection unit configuration pages in Config Tool. |
| Modify intrusion detection unit properties | To modify the intrusion detection unit configurations in Config Tool. |
| Add/delete intrusion detection units | To add or delete intrusion detection units in Config Tool. |
| Acknowledge intrusion alarm | To akcnowledge alarms in intrusion detection areas in Security Desk. |
| Arm/disarm intrusion detection areas | To arm or disarm intrusion detection areas from Security Desk. |
| Silence intrusion alarm | To silence alarms in intrusion detection areas in Security Desk. |
| Trigger intrusion alarm | To trigger alarms in intrusion detection areas in Security Desk. |
| Alarm monitoring | To use the Alarm monitoring task in Security Desk. |
| Alarm report | To use the Alarm report task in Security Desk. |
| Acknowledge alarms | To acknowledge active alarms in Security Desk. |
| Forward alarms | To forward alarms in Security Desk. |
| Snooze alarms | To snooze active alarms in Security Desk. |
| Trigger alarms | To trigger alarms in Security Desk. |
| View alarm properties | To view alarm configuration pages in Config Tool. |
| Modify alarm properties | To modify alarm configuration settings in Config Tool. |
| Add/delete alarms | To add or delete alarms in Config Tool. |

4 Click **Apply**.

# Configuring the Tag Tracker plugin

*[This chapter includes all the things you need to know and do to configure the plugin]*

This section includes the following topics:

- Creating the plugin role on page 27
- Connecting the Tag Tracker role to the Tag Tracker server on page 28
- Adding Tag Tracker entities to Security Center on page 29
- Enabling failover on the plugin role on page 30
- Granting user privileges for the Tag Tracker plugin on page 24
- <Configuring thing> on page 31

# Creating the plugin role

*[This topic explains how to create a plugin role, the first step in the configuration process. Most plugins follow a standard process. Example follows.]*

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 Config Tool home page, 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.

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.

5 Click **Next**.

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

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

8 Click **Close**.

The plugin role appears in the entity browser.

# Connecting the Tag Tracker role to the Tag Tracker server

*[Optional. Sometimes there is no need to connect to a server. This topic explains how to connect a plugin role to the plugin server so that events can be monitored and reported on in Security Center. Most plugins follow a standard process. Example follows.]*

To monitor entities and events from an RSA system in Security Center, you must connect the Restricted Security Area Surveillance plugin role to the RSA server.

**To configure the plugin role:**

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

2 Select the Restricted Security Area Surveillance role, and then click the **Properties** tab.

3 In the **Server** box, enter the inbound TCP/IP address of the third-party RSA server.

4 In the **Port** box, enter the inbound TCP/IP network port used by the RSA server and plugin to communicate.

5 Specify the user name and password of an administrator-level account for the RSA system.

6 Click **Apply**.

When the plugin connects to the RSA server, the **Server status** changes from **Disconnected** to **Connected**.

# Adding Tag Tracker entities to Security Center

*[This topic explains how to add or import Tag Tracker entities to Security Center. Example follows.]*

When you add your RSA zones to Security Center, the zones are displayed as colored areas on the Security Center map. For some RSA systems, like SpotterRF, you must add zones to the Restricted Security Area Surveillance plugin role.

### Before you begin

- Your RSA system must contain at least one zone.
- Security Center must have a Geo-referenced map.
- The Restricted Security Area Surveillance plugin role must have at least one radar.

### What you should know

- This task applies to SpotterRF.
- A zone represents the perimeter of a restricted area.
- Zones are defined in your Restricted Security Area Surveillance system, and then are added to the plugin role.
- Zones are displayed as a colored area on the default Security Center map.
- After adding your radar and zones to Security Center, you will be able to see targets detected by the radar on Security Center maps.

**To add a zone to Security Center:**

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

2 Select the Restricted Security Area Surveillance role, and then click the **Zones** tab.

3 Click (Add) button.

4 Select a radar from the list.

5 Select the zones you want to add.

6 Select a map.

7 Click **Save**, and then click **Apply**.

8 Optional: Add event-to-actions for events detected within this zone.

# Enabling failover on the plugin role

*[This topic explains how to setup failover so that in the event of server failure the plugin role switches to the failover sever. The process follows a standard set of steps. Example follows.]*

### Before you begin

To learn how to configure failover servers for your plugin role and the Directory, refer to the *Security Center Administrator Guide*. You can access this guide by pressing F1 in Config Tool. If the server of the supported component fails and a failover server is configured, Security Center will automatically switch the component to its failover server and have the plugin to communicate with it. No user action is required when a failover occurs. Expansion servers must be available in your system to use as failover servers.

### What you should know

You can deploy a failover server for the following servers:

- Plugin role
- Security Center Directory

To add failover servers to the Directory, refer to the *Security Center Administrator Guide*. You can access this guide by pressing F1 in Config Tool.

**To add failover servers for the plugin role:**

1 In the *Plugins* task, select the plugin from the entity browser, and click the **Resources** tab.

2 In Servers, click **Add an item** (+), and select a server.

3 Click **Add** > **Apply**.

If the server of the plugin role fails, Security Center will automatically switch the role to the failover server.

# <Configuring thing>

*[Add any additional configuration tasks required to get the plugin up and running and ready to use. Sample structure below.]*

*Write a short description. The short description should describe the purpose or main point of the topic. An effective short description typically answers two questions: What is the topic about? Why do users care about or need the information in the topic?*

### Before you begin

- This section lists the things the reader needs to do before performing the steps below.

**To configure X:**

1 Step. Try to include screen shots of the steps results so the user can check if they performed correctly.

5

# Using the Tag Tracker plugin

*[This section includes all the tasks a user can perform in using this plugin to do their job.]*

This section includes the following topics:

# Granting access to Tag Tracker entities in Security Center

*[Sample task.]*

So that cardholders can open SALTO doors and lockers, you must add the cardholders to access rules, and then add the rules to your SALTO doors and lockers.

**To grant cardholder access to SALTO doors, lockers, and areas (zones):**

1 In Config Tool, create an access rule.

2 Add cardholders and cardholder groups to the rule.

3 Define a schedule that contains eight or fewer time periods, and then apply your changes. In SALTO, a cardholder schedule (timetable) can only contain eight periods, where a period is a unique block of time, regardless of the day of the week. The following image shows a schedule that contains three time periods:

- Period 1) 8:00 to 5:30
- Period 2) 8:00 to 10:45
- Period 3) 12:45 to 3:45 4


4 Add the access rule to the door or doors and apply your changes.

5 Security Center immediately exports the rules to the SALTO system.

6 Update the cardholder's credentials: from the *Cardholder Management* task, select a cardholder, open the *Modify cardholder* window, click the **Salto credential management** button, and then click **Update**.

Within seconds, authorized cardholders can unlock the doors and lockers for the specified schedules.

# Reporting an incident

*[Add any additional tasks operators can perform, for example monitoring plugin entities, reporting on entity activity. Example structure below.]*

*Write a short description. The short description should describe the purpose or main point of the topic. An effective short description typically answers two questions: What is the topic about? Why do users care about or need the information in the topic?*

### Before you begin

- This section lists the things the reader needs to do before performing the steps below.

**To configure X:**

1 Step. Try to include screen shots of the steps results so the user can check if they performed correctly.

6

# Troubleshooting the Tag Tracker plugin

*[Most users will turn to the user guide when they have an issue with the plugin installation, configuration, or while using the plugin to do their job. Try to anticipate these issues and provide solutions.]*

This section includes the following topics:

# Plugin installed, but missing from Security Desk and Config Tool

*[This is a standard issue. Symptoms differ across plugins. Update this topic to reflect the symptoms specific for your plugin.]*

If the plugin role's *Properties* page, reports, events, and alarms are missing, then the plugin is not installed on your local machine. The plugin must be installed on a Genetec™ Server (main or expansion) and on all client workstations that are used to monitor incidents.

To help you troubleshoot this issue, refer to the possible causes and their respective solutions below.

**Symptoms:**

- In Config Tool, you see the plugin in the *Plugins* task, and you can add a new plugin role, but the role is missing the **Properties** tab.
- In Security Desk, you do not see the reports for this plugin.
- In Security Desk, you are not receiving events or alerts for this plugin.
- In Security Desk, the plugin does not appear on the *Options* page.

**Cause:**

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

**Solutions:**

- **Solution 1:** Install the plugin on your local computer.
- **Solution 2:** Make sure that a Genetec™ Server has the plugin installed, the role created, and is configured correctly.
- **Solution 3:** Confirm that the plugin is installed on your Security Center computer: from the home page in Security Desk or Config Tool, click **About** > **Installed components** and look in the list for entries that begin with *Genetec.Plugins*.
- **Solution 4:** Confirm that your system has a license (certificate) for the plugin: from the home page in Security Desk or Config Tool, click **About** > **Certificates**, look in the list for the name of the plugin, and make sure that your access permissions are set to **Unlimited**.

**Commented [JL1]:** Change this word to whatever it is that you are monitoring in your specific system.
Areas? Perimeters? Devices? Intruders?

**Commented [JL2]:** This only applies if your plugin installs specific reports.

**Commented [JL3]:** This only applies if your plugin adds settings or information to the Options page in Security Desk.

# Error messages

*[List error messages that are coming from the plugin and include description of problem and solution. Effective error messages are a key usability feature of the product. Effective error messages help the users solve issues themselves. Sample below.]*

Some of the error messages and warnings displayed in Security Center come from the SALTO system. Our messages include the SALTO error number, a description of the problem, and when we can, we tell you what you can do to solve the problem. You might also want to refer to your SALTO user documentation to find out more about each message.

The following error messages originate in the SALTO system and are displayed in Security Center.

- SALTO Error 1: The SALTO database is unavailable or unreachable.
- SALTO Error 4: An unknown error occurred on the SALTO system.
- SALTO Error 5: The requested operation has been canceled or aborted.
- SALTO Error 6: The specified process ID is not correct or unknown. Contact Genetec Inc. technical support.
- SALTO Error 7: SALTO is unable to accept your changes probably because the parameters violate one of their business rules.
- SALTO Error 10: Unable to add the entity because an entity with the same ID already exists in SALTO. You need to import entities into Security Center.

*[If the error messages for the plugin do not have error numbers that link to the other-party's documentation, and the errors do not include a solution, then you should list the error message, indicate where the message appears in Security Center, and provide solutions.*

*If an error message has multiple causes and solutions, it needs to have its own topic, which you can link to from the table below.]*

The following error messages might appear in the plugin's Diagnostic window, which you open by right-clicking the plugin, selecting **Maintenance > Diagnostic**.

| Error | Solution |
|---|---|
| *Error message* | *Solution.* |
| *Error message x.* | *See Xref to troubleshooting topic on page x.* |

# Cannot receive Tag Tracker alarms

If alarms triggered in Tag Tracker are not triggered in Security Center, they may be configured without recipients in Security Center.

### Cause

This issue typically occurs when an alarm does not have recipients associated with it.

**Solution**

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

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

3 In **Alarm recipients**, make sure that the user who should be notified when the alarm is triggered is added to the list.

**NOTE:** The users or user groups selected here are the default alarm recipients configured when alarm entities are created by the plugin. If this list is empty, alarms will still be triggered in Security Center, but no user will be notified. You can also add alarm recipients later in the alarm entity **Properties** tab.

4 Open the **Alarms** task, select the alarm entity in the entity browser, and then click **Properties**.

5 Make sure that the user is added to the alarm **Recipients**.

6 If the problem persists, restart the plugin role.

7 Try restarting the server on which the plugin role is running.

8 Try restarting the SiPass proxy server.

**NOTE:** Restarting the proxy server will trigger a full synchronization with the SiPass server, which may take a long time to complete depending on the number of entities that must be synchronized.

# Cannot receive Tag Tracker events

*[Standard troubleshooting topic.]*

If events triggered in Tag Tracker are not triggered in Security Center, you may want to verify that they are not ignored in Security Center.

## Cause

This issue typically occurs when the events are set to be ignored in the plugin configuration.

**Solution**

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

2 In the *Plugins* task, select the Tag Tracker plugin from the entity browser, and click the **Ignored events** tab.

3 Under **Processed events**, make sure that the events you want triggered in Security Center are listed.

4 In Security Desk, open the *Monitoring* task, and then make sure that the entities for which you should receive the events are monitored.

5 In Security Desk, click **Options** > **Events**.

6 Make sure that the event and its Display in tile option are selected, and then click **Save**.

**NOTE:** For all custom events you must select **Custom event** in the list.

7 If the problem persists, restart the plugin role.

8 Try restarting the server on which the plugin role is running.

9 Try restarting the SiPass proxy server.

**NOTE:** Restarting the proxy server will trigger a full synchronization with the SiPass server, which may take a long time to complete depending on the number of entities that must be synchronized.

# Cannot synchronize events from the Tag Tracker plugin

*[Standard troubleshooting topic. Depending on plugin, details may differ. Sample follows.]*

If you see that some SiPass entities or events are missing in Security Center, or that the synchronization does not occur at all, you may want to start a synchronization manually.

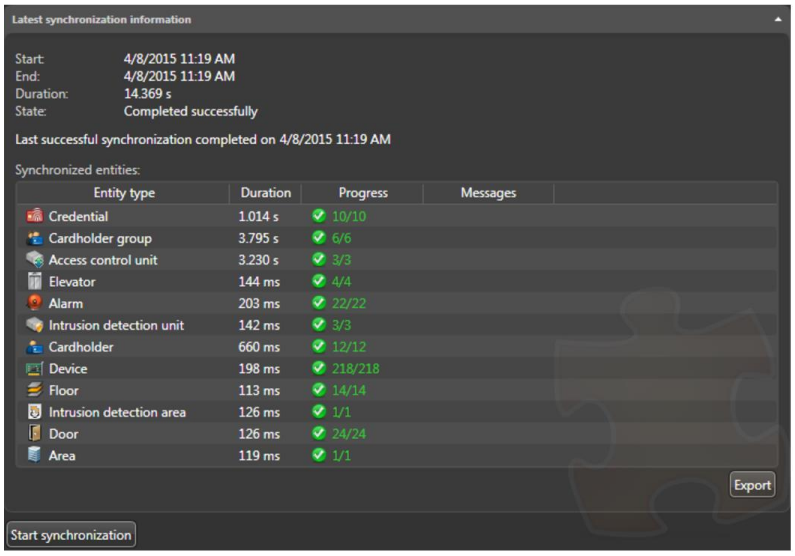
## Cause

Synchronization issues typically occur when the SiPass plugin and the SiPass server run incompatible versions, or when a disconnection occurs while a synchronization is in progress.

**Solution**

1. Make sure that a connection is established between Security Center and the SiPass server; that is, the plugin role does not show a warning by turning yellow.
2. Make sure that the plugin and the <Plugin> server are compatible.
3. From the Config Tool home page, open the *Plugins* task.
4. In the *Plugins* task, select the Tag Tracker from the entity browser, and click the **Synchronization** tab.
5. Click the **Refresh** () button under **Currently synchronized entities**, and verify that the number of entities currently synchronized matches the number of entities (objects) in SiPass that are eligible for synchronization.
6. If the number of entities does not match, or if there is no entity at all being synchronized, click **Start synchronization** to start a manual synchronization.

   The synchronization progress and the number of entities being synchronized for each type of entity is displayed under Latest synchronization information.




7 Under **Latest synchronization** information, make sure that the synchronization completed successfully.

8 If the problem persists, restart the plugin role.

9 Try restarting the server on which the plugin role is running.

10 Try restarting the Tag Tracker proxy server.

**NOTE:** Restarting the proxy server will trigger a full synchronization with the Tag Tracker server, which may take a long time to complete depending on the number of entities that must be synchronized.

7

# Additional resources

This section includes the following topics:

# Events added by the Tag Tracker plugin

*[List the custom events and privileges added by the plugin. Example follows.]*

Custom events and privileges are added in Security Center when you install the BuyTime plugin.

### Custom events

The BuyTime plugin adds the following custom events in Security Center. They can be used as query filters in activity reports or to create event-to-actions.

| Event | Source entity | Description |
|---|---|---|
| Arming postponed (User) | User | The arming of an intrusion detection area has been postponed by a user. |
| Arming postponed (Credential) | Credential | The arming of an intrusion detection area has been postponed using the specified credential. |
| Arming postponed (Cardholder) | Cardholder | The arming of an intrusion detection area has been postponed by a cardholder. |
| Arming postponed (Intrusion detection area) | Intrusion detection area | The arming of an intrusion detection area has been postponed. |
| Schedule deactivated (Intrusion detection area) | Intrusion detection area | The arming schedule has become inactive. |
| Schedule activated (Intrusion detection area) | Intrusion detection area | The arming schedule has become active. |
| BuyTime period activated (Intrusion detection area) | Intrusion detection area | The time you have to request an extension has started. |
| Late arming (Intrusion detection area) | Intrusion detection area | An intrusion detection area was armed after the arming was postponed. |
| Intrusion area disarmed during active schedule (Intrusion detection area) | Intrusion detection area | An intrusion detection area was manually disarmed, while the arming schedule was in effect. |
| Intrusion area armed during active schedule (Intrusion detection area) | Intrusion detection area | An intrusion detection area was manually armed during the BuyTime period or the extension. |
| Arming (Intrusion detection area) | Intrusion detection area | An intrusion detection area was armed on schedule, after the BuyTime ended and nobody postponed the arming schedule. |

# 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.

# 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.