
# CCURE Access Control Plugin and Video Integration Guide

3.2

Genetec

# Copyright notice



### Document information

Document title: CCURE Access Control Plugin and Video Integration Guide 3.2

Document number: EN.550.008-V3.2(4)

Document update date: May 26, 2015

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

# About this guide

This guide describes how to integrate Software House CCURE 9000 access control systems with Security Center.

This guide supplements Security Center and CCURE documentation. For more information about CCURE applications, see your CCURE documentation.

This guide assumes you are familiar with the following:

- Security Center 5.2 systems.
- Configuration and use of CCURE 9000 access control software.
- Configuration and use of EMC AutoStart software.
- Configuration and use of everRun MX software (High Availability and Extend).

## Notes and notices

The following notes and notices might appear in this guide:

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

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

# Contents

1

# Release Notes

This section includes the following topics:

# What's new in CCURE Access Control Plugin and Video Integration?

The CCURE access control plugin 3.2 and video integration include the following new features and enhancements.

- **CCURE system version:** Security Center now supports CCURE 9000 system version 2.30 and 2.40.
- **CCURE data in Security Center reports:** CCURE events are now shown in Security Center access control reports, such as Cardholder activities and Door activities.
- **Alarms and custom events:** CCURE events are now automatically mapped to alarms and custom events in Security Center. These alarms and custom events are triggered when the corresponding events are received from CCURE and can be used to configure event-to-actions to provide automatic system response.
- **Offline CCURE events:** Events that occurred in CCURE when Security Center was disconnected are automatically retrieved upon reconnection. All Offline CCURE events are stored in the Security Center database, however only those that occurred within the grace period will be shown in the Monitoring task.
- **Failover:** Failover of the Security Center Directory, Plugin role, Archiver, and Media Router is now supported. Failover of the CCURE server is also supported.
- **Camera mappings:** Security Center cameras can now be mapped to CCURE doors, elevators, areas, and intrusion detection areas, using the existing configuration pages provided in Config Tool.
- **Multiple server support:** Multiple independent Security Center systems can connect simultaneously to the same CCURE server. CCURE events are received by all Security Center systems, and video coming from multiple Security Center systems can be viewed on a single CCURE client.
- **Synchronization status:** The plugin now provides detailed synchronization status to help troubleshooting synchronization issues.
- **Cardholder details:** Detailed cardholder information available in CCURE can now be viewed in Config Tool and in Security Desk. Cardholder details are also displayed in the Monitoring task when access control events are received.

# Known issues

The CCURE access control plugin and video integration 3.2 includes the following known issues.

| Issue | Description |
|---|---|
| 104125 | When you are viewing a CCURE door in a Security Desk tile, the **Unlock/Lock** button is available, but it does not work. |
| 114152 | If you are using a multi-tile view in CCURE, the playback button is disabled.<br>**Workaround:** Refresh the camera tile. |
| 133108 | In the CCURE Monitoring workstation, a video recording that was initiated from Security Center cannot be played back by double-clicking the video icon. |
| 172147 | CCURE 2.20: Security Center cannot receive the following access control events: *Request to exit*, *Door opened Door closed* , on *Access granted/Request to exit*.This issue was caused by a default System variable change between CCURE 2.10 and 2.20.<br>**Workaround:** Open the Administration Workstation application, click **Options & Tools** > **System Variables** > **iStar Driver**, and then set **Non Alarm Input Report Flag** to **False**. |
| 222047 | CCURE card readers are not associated with elevators in Security Center. |
| 256462 | It is not possible to view video in CCURE client applications when using the SDK 5.3. This issue was observed with some cameras.<br>**Workaround:** Update configuration of the CCURE client applications following these steps:<br>1 On the workstation where the CCURE client applications are installed, close them if they are running.<br>2 Browse to the installation folder, by default *C:\Program Files (x86)\Tyco\CCURE Client*.<br>3 Open file *SoftwareHouse.NextGen.Client.AdminWorkstation.exe.config*.<br>4 At the bottom of the file, in the *startup* attribute, make sure you have the following:<br>`<startup useLegacyV2RuntimeActivationPolicy="true">`<br>`<supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5"/>`<br>`</startup></configuration>`<br>5 Save and close the file.<br>6 Repeat previous steps with file *SoftwareHouse.NextGen.Client.MonitoringStation.exe.config*.<br>7 Start your client applications. |

# Limitations

The CCURE access control plugin and video integration 3.2 includes the following known limitations.

| Issue | Description |
|---|---|
| 104008 | When you unlock a door from the CCURE system using an *access granted* event, the lock status of the door in the door widget is not updated in Security Desk. |
| 113452 | You cannot view video in CCURE from a Security Center camera that is federated from an Omnicast system. |
| 113453 | You cannot receive CCURE access control data coming from a federated Omnicast system that has the CCURE plugin installed. |
| 113454 | CCURE data is not included in the *People counting*, *Time and attendance*, *Cardholder activities*, *Door activities*, or *System status* reports. |
| 113455 | The following actions are not supported with CCURE entities:<br>• *Unlock door explicitly*<br>• *Temporary override unlock schedules*<br>• *Unlock for maintenance*<br>• *Sound/silence buzzer*<br>• *Reset area people count*<br>• *Forgive antipassback violation*<br>• *Arming/Disarming Intrusion Detection Area*<br>• *Trigger Intrusion Alarm*<br>• *Trigger output* |
| 113458 | Access control units imported from CCURE are not included in *Health statistics*. |
| 128133 | The **Pre-Alarm Time** option in the CCURE Administration Station is not supported in Security Center.<br>**Workaround:** In Security Center Config Tool, set the length of time in the **Time to record before an event** option in the Archiver's *Camera recording* tab, or in the *Recording* tab of specific camera entities. |
| 133237 | No message is displayed for the Security Center video server status in the CCURE Monitoring station with an EMC redundancy setup.<br>**Workaround:** Use the CCURE Administration station to create an alarm for a custom event. |
| 220027 | Installation of the Security Center video component on the CCURE server fails with error `InsertLicenseOption command failed with exit code -1003. The setup will abort.` |

| Issue | Description |
|---|---|
| | **Workaround:** See Installation of the Security Center video component fails in the CCURE video integration troubleshooting section. |
| 223751 | Tamper status and events are not displayed in reports for intrusion detection units. |
| 225526 | CCURE server: The Security Center CCURE access control service does not start automatically when the server is restarted.<br>**Workaround:** Open a *Server Configuration Application* window and start the service manually. |
| 253960 | The Security Center CCURE video component service does not start automatically when the plugin is installed for the first time.<br>**Workaround:** Open a *Server Configuration Application* window, select the **Enabled** box for the vido component service, and start the service manually. |

# Compatibility

The CCURE access control plugin and video integration 3.2 is compatible with the following systems.

- Security Center 5.2 SR9 and later
- CCURE 9000 systems versions 2.30 and 2.40
- CCURE 9000 Enterprise systems versions 2.30 and 2.40
- CCURE 9000 systems that are configured using EMC AutoStart redundancy
- CCURE 9000 systems that are configured using everRun MX High Availability (pair of servers that work together as a single host and share the same host name)
- CCURE 9000 systems that are configured using everRun MX Extend redundancy (pair of servers sharing the same host name along with an external physical host)

**IMPORTANT:**

- The CCURE plugin 3.2 is not compatible with previous versions of CCURE 9000 systems.
- The CCURE plugin 3.1 can be upgraded to version 3.2 in Security Center 5.2 SR9. Existing camera mappings will be preserved, however an upgrade of the plugin database will be required.
- Upgrades from the Omnicast CCURE plugin to the Security Center CCURE plugin are not supported. If you have migrated from an Omnicast system to a Security Center system, you will have to uninstall the Omnicast CCURE plugin, and then install the Security Center CCURE plugin. Your event database information will be lost, and you will have to re-create your configuration in the Administration Station.

# Part I

# CCURE access control plugin

This part includes the following chapters:

2

# Introduction to CCURE access control plugin

This section includes the following topics:

# What is the CCURE access control plugin?

The CCURE access control plugin integrates CCURE 9000 access control systems with Security Center, so that Security Center can receive and monitor access control entities and events from CCURE systems.

The plugin allows you to do the following:

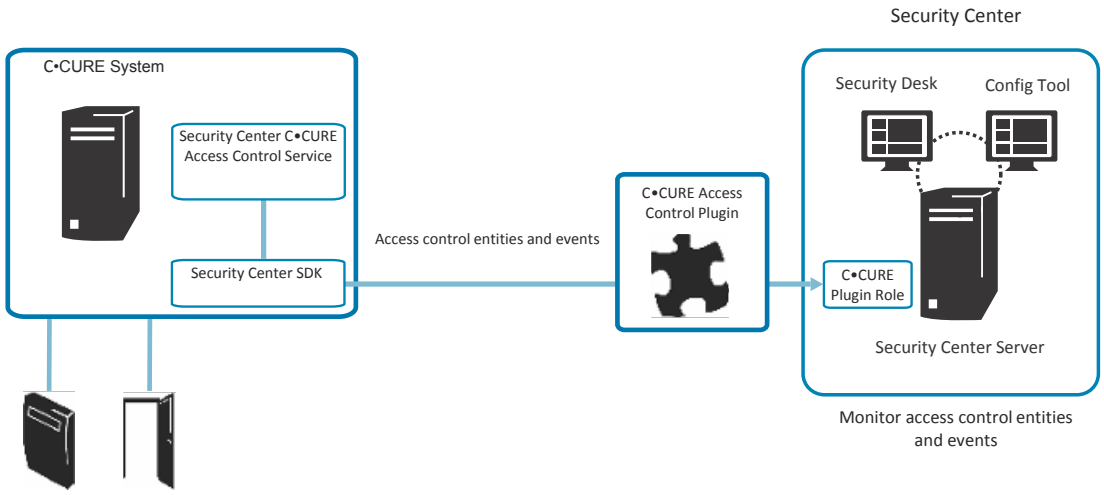
- Synchronize Security Center entities with entities, devices, and events configured in CCURE.
- Map the CCURE access control devices (controllers, doors, door sides, areas, intrusion areas, and elevators) along with intrusion detection units to Security Center cameras.
- Display live access control events from CCURE in Security Desk with detailed cardholder information.
- Monitor live and playback video related to the access control events coming from CCURE in Security Desk *Monitoring* task.
- View the current state of CCURE doors (open, closed, locked, unlocked).
- Configure event to actions using CCURE events.
- Generate Security Center reports to search for past CCURE events.
- View the synchronization status of CCURE entities and events in Security Center.
- Support Security Center Federations: that is, monitor at the federation host, entities and events of a CCURE system connected to a federated Security Center system.

For information about monitoring entities in Security Desk, see the *Security Desk User Guide*. You can access this guide by pressing `F1` in Security Desk.

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

## How the CCURE access control plugin works with Security Center

The CCURE access control plugin integrates CCURE 9000 access control systems in Security Center using three components installed on Security Center and CCURE servers.




- **CCURE access control plugin:** The CCURE access control plugin is a software package installed on Security Center servers and client workstations. It allows creation of the CCURE access control

plugin role in Security Center, and provides all the features to receive and manage access control entities and events from CCURE 9000 systems.

- **Security Center CCURE access control service:** The service, which is included in the CCURE video integration installation package, is installed on CCURE servers that will be connected to Security Center. Working together with the plugin, it allows CCURE systems to send access control entities and events to Security Center.
- **CCURE plugin role:** The CCURE plugin role is used to activate the CCURE access control plugin features in Security Center. It allows Security Center to get access control data from CCURE systems.
- **Security Center Software Development Kit (SDK):** The SDK is a software package installed on CCURE servers to provide the communication interface between the CCURE access control service and the CCURE access control plugin.

**NOTE:** The CCURE access control plugin only works in one direction, from CCURE to Security Center. No data or commands are sent to CCURE, except for data queries sent to get access control entities and events from CCURE. Because of this, it is not possible for example to unlock doors, even if the widget is available in Security Desk, change configuration of entities or rename custom events from Security Center.

## Differences between Omnicast and Security Center CCURE access control plugins

The Security Center CCURE access control plugin increases the functionality that is available with the Omnicast 4.x CCURE access control plugin.

Although both plugins allow you to receive and monitor access control entities and events from the CCURE system, there are additional features in Security Center. For example, with the Security Center CCURE access control plugin you can synchronize access control entities from the CCURE system, and view the current state of those entities in Security Center; these features are not supported with the Omnicast 4.x CCURE access control plugin.

With the Omnicast 4.x CCURE access control plugin, you must create an event mapping XML file to convert the CCURE events into Omnicast events. However, with the Security Center CCURE access control plugin, the CCURE system is seamlessly integrated into Security Center.

# How CCURE events are mapped in Security Center

CCURE events are mapped to events, custom events, and alarm entities in Security Center.

CCURE events are automatically mapped to Security Center events. Security Center custom events are used to map CCURE events that do not require acknowledgement and that cannot be mapped to Security Center events. The plugin automatically creates the custom events, and if new events are added in CCURE, it will automatically create corresponding custom events in Security Center.

Security Center alarm entities are used to map CCURE events that require acknowledgement. The plugin automatically creates the alarm entities, and if new events that require acknowledgement are added in CCURE, it will automatically create corresponding alarm entities in Security Center. An event acknowledged in CCURE will also have its corresponding alarm acknowledged in Security Center.

**IMPORTANT:** Due to the one-way communication with CCURE, alarms acknowledged in Security Center are not acknowledged in CCURE.

The plugin maps CCURE events to the equivalent Security Center events as shown below.

**NOTE:** The mapping cannot be modified.

| CCURE 9000 | | | Security Center | |
|---|---|---|---|---|
| **Message type** | **Source** | **State code** | **Event** | **Source entity** |
| Area activity | Area | One occupant | Area first man in | Area |
| | | Area empty | Area last man out | |
| | | Area clear counts | People count reset | |
| Card admitted | Door, Elevator | Admit | Access granted | Cardholder, Door, Elevator, Area |
| | | Admit no personnel | | |
| | | Admit unknown | | |
| | | Complex CHUID | | |
| | | Deleted | | |
| | | Direction in | | |
| | | Direction out | | |
| | | Door unused | | |
| | | Duress | | |
| | | Ext reader status msg | | |
| | | Group access | | |
| | | Host | | |

| CCURE 9000 | | | Security Center | |
|---|---|---|---|---|
| | | Manual | | |
| | | Noticed | | |
| | | PIN only access | | |
| Card rejected | Personnel, Door, Elevator | Card disabled | Access denied - Inactive credential | Cardholder, Door, Elevator, Area |
| | | Card status | | |
| | | Disabled | | |
| | | Not activated | | |
| | | Expired | Access denied - Expired credential | |
| | | No PIN | Access denied - Valid card, inactive PIN | |
| | | PIN | | |
| | | WAS unknown PIN | Access denied - Invalid PIN | |
| | | Unknown PIN | | |
| | | Passback | Access denied - Antipassback violation | |
| | | Timed anti-passback | | |
| | | Lost | Access denied - Lost credential | |
| | | Stolen | Access denied - Stolen credential | |
| | | Unkown card | Access denied - Unknown credential | |
| Intrusion zone activity | Intrusion zone | Intrusion zone armed | Intrusion detection area master armed | Intrusion detection area |
| | | Intrusion zone force armed | | |
| | | Intrusion zone disarmed | Intrusion detection area disarmed | |
| | | Intrusion zone violated | Intrusion detection area alarm activated | |

| CCURE 9000 | | | Security Center | |
|---|---|---|---|---|
| | | Intrusion zone violated clear | Intrusion detection area cancelled alarm | |
| Intrusion zone error | Intrusion zone | Intrusion zone violated | Intrusion detection area alarm activated | Intrusion detection area |
| Object state changed | XFEvent | Active | Alarm triggered | Alarm |
| | | Inactive | Alarm acknowledged | |
| | Controller | Communication restored | Unit connected | Unit, Intrusion unit |
| | | Communication failure | Unit lost | |
| | | IStar battery low | Unit battery fail | |
| | | IStar onboard battery low | | |
| | | Low battery | | |
| | | Power failure | Unit AC fail | |
| | | AC power failure | | |
| | | Tamper | Intrusion detection unit tamper | |
| | | Tamper abnormal | | |
| | Door | Door closed | Door closed | Door |
| | | Door open | Door opened | |
| | | Locked | Door locked | |
| | | Door lock by link | | |
| | | Door lock by operator | | |
| | | Door unlock by operator | Door unlocked | |
| | | Momentary unlock | | |
| | | Door unlock | | |

| CCURE 9000 | Security Center |
|---|---|
| Door lock unsecure | |
| Door lock open | |
| Door left open | Door open too long |
| Door held | |
| Door switch shorted | Door tamper |
| Door switch cut | |
| Door forced | Door opened while lock secure |
| Door lock tamper | Door tamper |
| Request to exit | Door Rex on |

# CCURE events in Security Center reports

The plugin displays two types of CCURE events.

- **Real time events:** The events are received and stored in a database as soon as they occur. This requires an active connection with the CCURE server.
- **Offline events:** The events occur while Security Center is disconnected from the CCURE server. All offline events are retrieved and stored in the database as soon as a connection is established. Events that occurred within the grace period are also displayed in the *Monitoring* task when the associated entities are monitored. You can configure the grace period in the *Properties* tab of the Plugin role.

CCURE events are displayed in Security Center reports with the following information.

**NOTE:** The *Hardware inventory* report shows CCURE units, but without additional information being provided in the report columns.

| Security Center report | Supported columns |
|---|---|
| Cardholder activities | • Event / Event timestamp<br>• First name / Last name / Email address / Picture<br>• Location / Access point<br>• Unit / Unit type<br>• Device<br>• Time zone<br>• Occurence period<br>• Custom fields of cardholder entities |
| Door activities | • Event / Event timestamp<br>• Door / Side<br>• Cardholder<br>• First name / Last name / Email address / Picture<br>• Unit / Unit type<br>• Device<br>• Time zone<br>• Occurence period<br>• Custom fields of cardholder entities |
| Elevator activities | • Event / Event timestamp<br>• Elevator / Floor<br>• Cardholder<br>• First name / Last name / Email address / Picture<br>• Time zone<br>• Occurence period |

| Security Center report | Supported columns |
|---|---|
| | • Custom fields of cardholder entities |
| Area activities | • Event / Event timestamp<br>• Area<br>• Cardholder<br>• First name / Last name / Email address / Picture<br>• Time zone<br>• Occurence period<br>• Custom fields of cardholder entities |
| Intrusion detection area activities | • Event / Event timestamp<br>• Intrusion detection area<br>• Intrusion detection unit<br>• Occurence period |
| Access control unit events | • Event / Event timestamp<br>• Unit / Unit type<br>• Occurence period |
| Intrusion detection unit events | • Event / Event timestamp<br>• Intrusion detection unit<br>• Occurence period |
| System status > Access control units | • Entity<br>• Health<br>• AC fail<br>• Battery fail<br>• Tampered |
| System status > Areas | • Entity<br>• Logical path<br>• Health |
| System status > Doors | • Entity<br>• Logical path<br>• Health<br>• Open<br>• Lock |

| Security Center report | Supported columns |
|---|---|
| System status > Elevators | • Entity<br>• Logical path<br>• Health |
| System status > Intrusion detection area | • Entity<br>• Logical path<br>• Health<br>• Arming state<br>• Alarm active |
| System status > Intrusion detection units | • Entity<br>• Health<br>• AC fail<br>• Battery fail<br>• Tampered |

# How synchronization works with CCURE

Synchronization of CCURE entities and events in Security Center is done automatically when connection is established, in real time when changes are detected, or manually from Config Tool.

The plugin performs two types of synchronization:

- **Full synchronization:**
  - Re-imports all CCURE entities and events in Security Center, even though they were not modified.
  - Automatically starts when a connection is established with the CCURE server.
  - Can be started manually via Config Tool.
  - Typically takes more time because all entities are synchronized.
- **Partial synchronization:**
  - Changes are received in real time for specific CCURE entities and events.
  - Automatically maintains the two systems synchronized after the connection is established.
  - Cannot be started manually.
  - Takes less time because only the changes are synchronized.

# Synchronized entities and properties

The plugin synchronizes the following CCURE entities in Security Center with their associated properties.

**NOTE:**

- Inputs and outputs are not synchronized from CCURE.
- A controller in CCURE is always synchronized with an access control unit and an intrusion detection unit in Security Center.

| CCURE entity | Security Center entity | Properties |
|---|---|---|
| Personnel | Cardholder | • Description<br>• First Name<br>• Last Name<br>• Email address<br>• Picture<br>• Status<br>• Bypass antipassback rules<br>• Other cardholder properties (custom fields) |
| Door | Door | • Name<br>• Description<br>• Side A reader<br>• Side B reader |
| Elevator | Elevator | • Name<br>• Description<br>• Floors |
| Area | Area | • Name<br>• Description |
| Intrusion zone | Intrusion detection area | • Name<br>• Description |
| iSTAR controller | Access control unit | • Name<br>• Description |
| iSTAR controller | Intrusion detection unit | • Name |

| CCURE entity | Security Center entity | Properties |
| --- | --- | --- |
| | | • Description |

# Synchronized cardholder properties

The plugin uses native properties of cardholder entities, such as **First name**, **Last name**, **Email address**, and **Picture**, and also custom fields to synchronize personnel record attributes from CCURE.

The plugin automatically creates the custom fields with the names defined in CCURE. Those names can be modified in Security Center. They can also be modified in CCURE, in which case they will automatically be renamed in Security Center. If the value of a custom field is modified in Security Center, it will be overwritten with the value received from CCURE when a synchronization occurs.

The plugin automatically synchronizes the following personnel record attributes with cardholder entities.

| CCURE personnel record configuration tab | Attributes |
|---|---|
| General | • First Name<br>• Middle Name<br>• Last Name<br>• Object ID<br>• Personnel Type<br>• Operator Name<br>• Email address<br>• Escort Option<br>• Options<br>  • Alternate shunt (ADA)<br>  • Noticed<br>  • Activate Antipassback Event<br>  • Keypad Command Administrator<br>  • Intrusion Zone Administrator<br>  • Inactivity Exempt<br>  • Can Perform Guard Tour<br>• Modification History<br>  • Last edited on<br>  • Last edited by |
| Customer | Customer Fields:<br>• Text1 - Text12<br>• Int1 - Int6<br>• Logical1 - Logical2<br>• Date1 - Date2 |
| Customer Extended | Customer Extended:<br>• Text13 - Text25 |

| CCURE personnel record configuration tab | Attributes |
|---|---|
| | • Int7 - Int9<br>• Logical3 - Logical4<br>• Date3 - Date4 |
| Images | Primary Image |

# How failover works with the CCURE access control plugin

The CCURE access control plugin supports the failover of several components in Security Center and in CCURE.

- Plugin role
- Security Center Directory
- CCURE server

Failover of the CCURE server requires the CCURE system to be deployed in a high availability configuration, EverRunMX for example.

To configure backup servers for the 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 backup server is configured, Security Center will automatically switch the component to its backup server and have the CCURE access control plugin to communicate with it. No user action is required when a failover occurs.

# 3

# CCURE access control plugin installation

This section includes the following topics:

# Preparing to install the CCURE access control plugin

Before you install the CCURE access control plugin, you must perform some pre-installation steps.

**Before installing the plugin:**

1 Read the release notes.
2 Install CCURE Server and Client version 2.30 or 2.40.
3 Install the Security Center SDK on the CCURE server and client workstations.

**IMPORTANT:** The SDK must be of the same version as Security Center.

4 Install the Security Center video component on the CCURE server.

**IMPORTANT:** The CCURE access control plugin requires installation of the video component.

5 Install Security Center 5.2 SR9 or later.

For more information about installing Security Center, see the *Security Center Installation and Upgrade Guide*.

6 Make sure you have the *CCURE Access Control* and *CCURE Video* certificates supported in your Security Center license. You can verify this in the Config Tool home page by clicking **About** > **Certificates**.
7 Make sure your license includes the CCURE video integration part number (GSC-1PVSHCC). You can verify this in the Config Tool home page by clicking **About** > **Purchase order**.

The license number is included in the product-release email from the Genetec product manager. This email also includes links to the plugin download package and other license information.

8 Make sure that the license of your CCURE system supports access control integration with Security Center.

## After you finish

Install the plugin.

# Installing the CCURE access control plugin

The CCURE access control plugin is installed separately from the Security Center system.

## Before you begin

- Perform the pre-installation tasks.
- Close Config Tool and Security Desk.

## What you should know

The plugin needs to be installed on the Security Center client and server computers.

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

**To install the plugin:**

1 Download the CCURE installation package from the GTAP Product Downloads page.

2 Double-click the *Genetec Security Center - CCure Access Control Plugin.exe* file, and follow the installation instructions.

3 If you haven't done so already, make sure you apply the CCURE certificate to your Security Center license.

## After you finish

Create the CCURE access control plugin role.

# Preparing to upgrade the CCURE access control plugin

If you already have Security Center access control integrated with CCURE, and you want to upgrade your CCURE system to version 2.30 or 2.40, you must perform some pre-upgrade steps.

## What you should know

When upgrading Security Center, previous versions of the CCURE access control plugin will still be working.

**Before upgrading the plugin:**

1 Read the release notes.

2 Upgrade your CCURE server and client workstations to version 2.30 or 2.40.

3 Install the Security Center SDK on the CCURE server and client workstations.

**IMPORTANT:** The SDK must be of the same version as Security Center.

4 Upgrade the Security Center video component on the CCURE server.

**IMPORTANT:** The CCURE access control plugin requires an upgrade of the video component.

5 Upgrade your Security Center system to 5.2 SR9 or later.

For more information about upgrading Security Center, see the *Security Center Installation and Upgrade Guide*.

## After you finish

Upgrade the plugin.

# Upgrading the CCURE access control plugin

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

## Before you begin

- Perform the pre-installation tasks.
- Close Config Tool and Security Desk.

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

# 4

# CCURE access control plugin configuration

This section includes the following topics:

# Creating the plugin role

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

## Before you begin

Install the plugin.

**To create the plugin role:**

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

2 At the bottom of the **Plugins** task, click **Plugin** ( ).

3 On the **Specific info** page, select the server to run the plugin, select the plugin type, 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 **Entity name**.

b) Enter the **Entity description**.

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 plugin role appears in the entity browser. The plugin role is yellow because it is not yet configured.

## After you finish

Configure the plugin role.

**Related Topics**

Configuring the CCURE access control plugin role on page 31

# Configuring the CCURE access control plugin role

To receive CCURE access control events in Security Desk, you must connect the CCURE access control plugin role to the CCURE 9000 access control system by configuring the settings in the plugin *Properties* tab.

## Before you begin

Create the access control 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* tab settings, see the *Security Center Administrator Guide*. You can access this guide by pressing `F1` in Config Tool.

**To configure the CCURE plugin:**

1. From the home page in Config Tool, open the **Plugins** task.
2. In the **Plugins** task, select the CCURE access control plugin from the entity browser, and click the **Properties** tab.
3. In the **Server** field, enter the Host name or IP address of the CCURE server.
4. In the **Port** field, enter the port number of the CCURE server.

   The default port number is 5645. It can be changed if required.
5. Set a value in the **Grace period** option for events received from the CCURE system.

   Events received in Security Desk from CCURE that occurred within the grace period are treated as normal events. They appear in the event list in the *Monitoring* task, are recorded in the database, and actions that are associated with the event using event-to-actions are triggered. Events received with a timestamp older than the grace period are only recorded in the database.
6. In **Alarm recipients**, add the users who will be notified when alarms are triggered by the plugin.

   If the list is empty, alarms will still be triggered in Security Center, but no user will be notified.
7. In **Alarm partitions**, select the partitions to which the alarm entities will be added when created by the plugin.

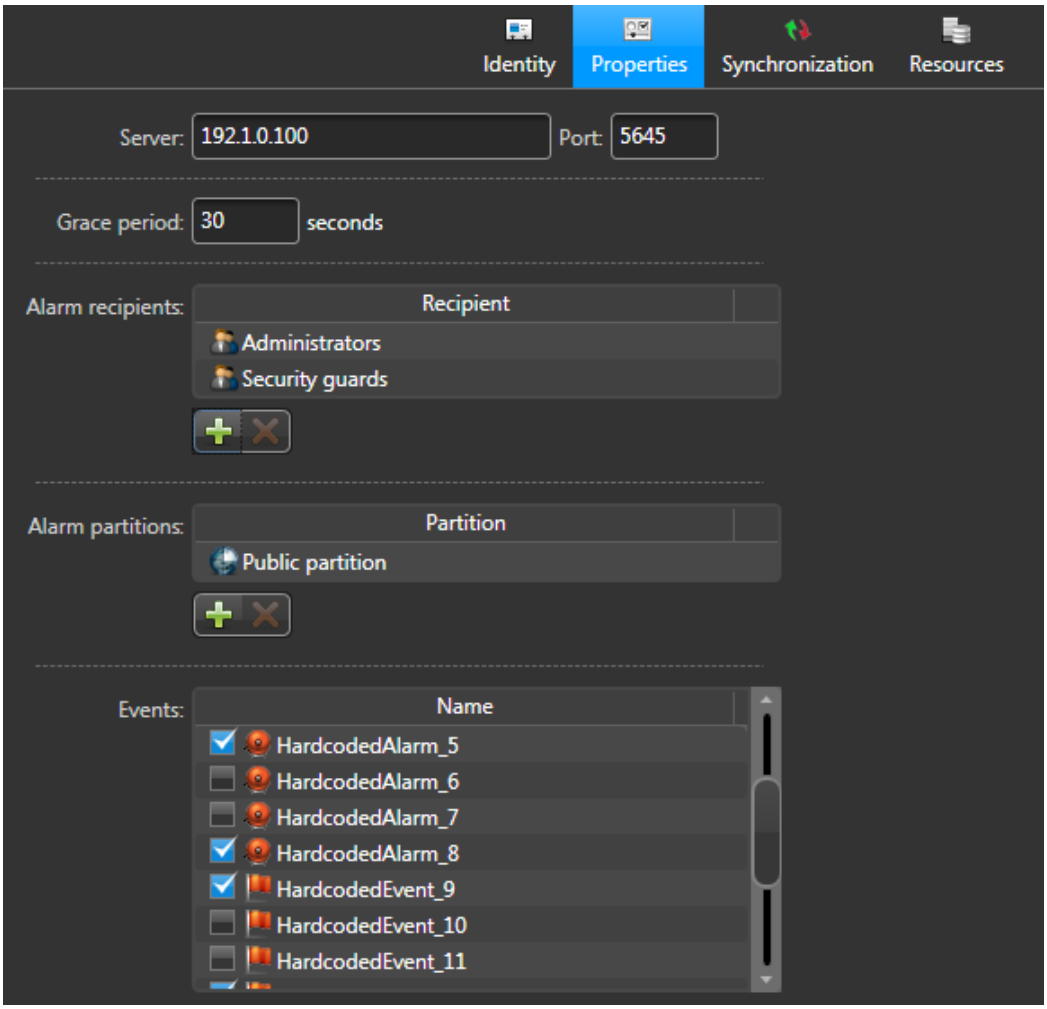
   Alarms created by the plugin will always be members of the those partitions. Partitions added via the **Alarms** task will be removed by the plugin when modifying **Alarm partitions**.
8. Select the events and alarms to be triggered in Security Center when received from CCURE.
9. Click **Apply**.

The access control entities on the CCURE system are synchronized with Security Center, and are added under the CCURE plugin in the *area view*. Alarm entities and custom events are also created to map the events that can be received from CCURE.

**NOTE:** The time required for synchronization varies depending on how many entities need to be synchronized.

## Example

Once configured, the **Properties** can look like this.




## After you finish

Assign Security Center cameras to CCURE devices.

# Assigning Security Center cameras to CCURE devices

To view video with the CCURE access control events received in Security Desk, Security Center cameras must be assigned to CCURE access control devices (doors, elevators, and so on).

## Before you begin

Add and configure cameras in Security Center. For more information, see the *Security Center Administrator Guide*. For information about monitoring entities, creating event to actions, and so on, in Security Desk, see the *Security Desk User Guide*. You can access both guides by pressing `F1` in Config Tool and in Security Desk respectively.

## What you should know

The *Camera mappings* tab available in the previous version of the plugin was removed. You can now assign cameras to door, elevator, floor, area, and intrusion detection area entities by selecting an entity in the logical view and accessing its specific configuration pages in Config Tool. For more information, see the *Security Center Administrator Guide*.

# Disabling CCURE events in Security Center

If you do not want CCURE events triggered in Security Center when received from CCURE, you can disable them in Config Tool.

## What you should know

All CCURE events are enabled by default in Security Center. This means that custom events and alarms will be triggered when corresponding events are triggered in CCURE.

**To disable CCURE events:**

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

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

3 In **Events**, unselect the events that you do not want triggered in Security Center.

4 Click **Apply**.

The unselected events will not be triggered in Security Center when received from CCURE.

# Starting a manual synchronization

Changes made in CCURE are automatically synchronized in Security Center. However, you may want to start a synchronization manually in case you observe an issue with the entities being synchronized.

## Before you begin

Make sure that the plugin role is configured and is connected to the CCURE server.

## What you should know

Starting a synchronization manually will trigger a full synchronization.

**NOTE:** The time required for synchronization varies depending on how many entities are synchronized.

**To start a synchronization manually:**

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

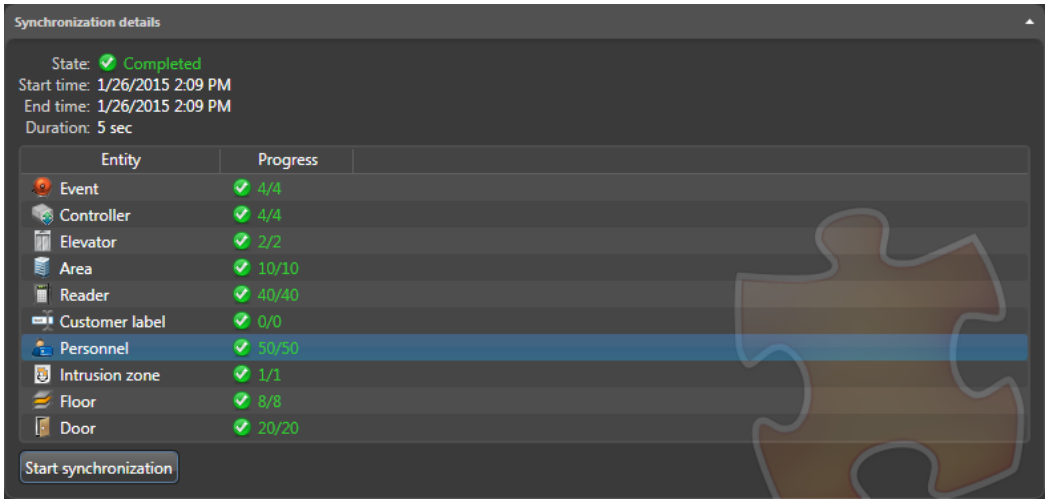
2 In the **Plugins** task, select the CCURE access control plugin from the entity browser, and click the **Synchronization** tab.

3 At the bottom of the page, click **Start synchronization**.

The synchronization progress and the number of entities being synchronized for each type of entity is displayed under *Synchronization details*. If entities were added or deleted in CCURE, check under Latest live updates for entities being added or deleted in Security Center during the synchronization.

**Example:**

*Customer label* shows the number of cardholder custom fields synchronized in Security Center due to the renaming of their corresponding attributes in CCURE. For example, if three attributes are renamed in CCURE and are synchronized properly, you will see **3/3**. If no attribute is renamed, you will see **0/0**.



# Connecting multiple CCURE servers

You can create multiple CCURE access control plugin roles in Security Center to synchronize the entities and receive access control events from more than one CCURE system simultaneously.

## Before you begin

- Make sure that all the CCURE servers to which Security Center will connect have the same version.
- A CCURE access control plugin role already exists in your system.

## What you should know

**IMPORTANT:** Adding multiple CCURE access control plugin roles configured with the same IP address is allowed and will not be notified. Such a configuration must never be used.

**To configure an additional CCURE access control plugin:**

1 Create a new CCURE plugin role.
2 Configure the plugin role.
3 In the **Server** field, make sure to enter a Host name or IP address that is not already used by another plugin.
4 In the **Port** field, make sure to enter a port number that is not already used by another plugin.
5 Change the port number used on the CCURE server.

Security Center can connect to multiple CCURE systems and synchronize the entities and events from each of them.

# Configuring the port number on the CCURE server

If you change the ***Port*** field in the *Properties* tab, you must also configure the same value on the CCURE server so that a connection can be made.

**To configure the port number on the CCURE server:**

1 Log on to the CCURE server.

2 Browse to folder *C:\Program Files (x86)\Tyco\CrossFire\ServerComponents*.

3 Open the file *Genetec.Plugins.CCure.AccessControl.Server.exe.config* in a text editor.

4 In the file, locate the line `<add baseAddress="net.Tcp://localhost:5645/Genetec/CCureAccessControl"/>`.

**NOTE:** The default port number is 5645.

5 Change the port number with the same value configured in the plugin.

6 Save the file, and then close it.

7 Open a *Server Configuration Application* window.

8 Stop the *Genetec Security Center C.CURE Access Control service*, and then restart it.

The plugin and the CCURE server have the same port number configured and should be able to establish a connection.

5

# CCURE access control plugin troubleshooting

This section includes the following topics:

# Troubleshooting: Plugin cannot connect to the CCURE server

If the plugin cannot connect to the CCURE server, verify that the IP address and port properties are properly set.

## What you should know

Connection issues typically occur when IP addresses or ports are not configured properly, or when the network is blocking packets from being exchanged between two endpoints. When this situation occurs, the plugin role turns yellow and provides an connection error message.

**To troubleshoot connection issues with the CCURE server:**

1. From the home page in Config Tool, open the **Plugins** task.
2. In the **Plugins** task, select the CCURE access control plugin from the entity browser, and click the **Properties** tab.
3. Check that the **Server** and **Port** fields are set with the correct values.
4. If you get an error message indicating that the port is already used:
   a) Change the port number to a value that is not used, and then click **Apply**.
   b) Make sure to change the port number used on the CCURE server to match the one configured in the plugin.
5. If you still observe an issue, verify that the IP address of the CCURE server is reachable from the server on which the Plugin role is running.

   You can verify this using the `ping` command.
6. Make sure that the port is not being blocked anywhere on the network.

# Troubleshooting: Plugin cannot synchronize from CCURE

If you see that some CCURE entities and/or events are missing in Security Center, or that the synchronization does not occur at all, try to solve the issue by starting a synchronization manually.

## Before you begin

Make sure that a connection is established between Security Center and the CCURE server.

## What you should know

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

**To troubleshoot synchronization issues:**

1 Make sure that the plugin and the CCURE server are compatible.

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

3 In the **Plugins** task, select the CCURE access control plugin from the entity browser, and click the **Synchronization** tab.

4 Click the **Refresh** ( ) button under *C•CURE 9000 synchronized objects*, and verify that the number of entities currently synchronized matches the number of entities (objects) in CCURE.

5 If the number of entities does not match, or if there is no entity at all being synchronized, click **Start synchronization** to start a full synchronization.

The synchronization progress and the number of entities being synchronized for each type of entity is displayed under *Synchronization details*. If entities were added or deleted in CCURE, check under Latest live updates for entities being added or deleted in Security Center during the synchronization.

6 Verify in *Synchronization details* that the synchronization completed successfully, that is, all entities have been synchronized.

7 If the problem still persists, restart the Plugin role.

8 Restart the server on which the Plugin role is running.

# Troubleshooting: Cannot receive CCURE events

CCURE events are not displayed in Security Center although they are activated in CCURE.

## What you should know

This issue typically occurs when the events are disabled in the plugin configuration.

**To troubleshoot this issue:**

1. From the home page in Config Tool, open the **Plugins** task.
2. In the **Plugins** task, select the CCURE access control plugin from the entity browser, and click the **Properties** tab.
3. In **Events**, make sure that the events and alarms you want triggered in Security Center are selected.
4. In the *Monitoring* task of Security Desk, make sure that you are monitoring the entities for which you should receive events.
5. If you still cannot receive CCURE events, restart the Plugin role.
6. Restart the server on which the Plugin role is running.

# Troubleshooting: Security Center license error about custom fields

If you get an error message indicating that the maximum number of custom fields permitted by the license has been reached, you might want to verify the number of custom fields currently provided by your license, and the total number of custom fields that you require in your system.

## What you should know

This error typically occurs when custom fields are added after the CCURE access control plugin was installed. The license provided with the plugin includes the number of custom fields required to synchronize cardholder entities. However, if you need to add custom fields afterwards, you also need to update the Security Center license with the proper number of custom fields allowed by the system.

**To solve this licensing issue, do one of the following:**

- Increase the number of custom fields provided by the license.
- Remove one or more custom fields from your system.

  **IMPORTANT:** Do not remove custom fields associated with the plugin.

# Troubleshooting: Plugin role fails to load after an upgrade

If, after upgrading the plugin, you get an error message indicating that the role failed to load, and that the database is waiting for upgrade, you must upgrade the plugin role database manually.

## What you should know

The issue occurs because custom fields are added to cardholder entities in this version of the plugin and need to be created in the database.

**To upgrade the database:**

1. From the home page in Config Tool, open the **Plugins** task.
2. In the **Plugins** task, select the CCURE access control plugin from the entity browser, and click the **Resources** tab.
3. In the database actions, click **Database update**.
4. When the database update is completed, restart the Plugin role.

# Part II

## CCURE video integration

This part includes the following chapters:

6

# Introduction to CCURE video integration

This section includes the following topics:

# What is CCURE video integration?

The CCURE video integration allows CCURE users to receive live events and view Security Center video in CCURE 9000 access control systems.

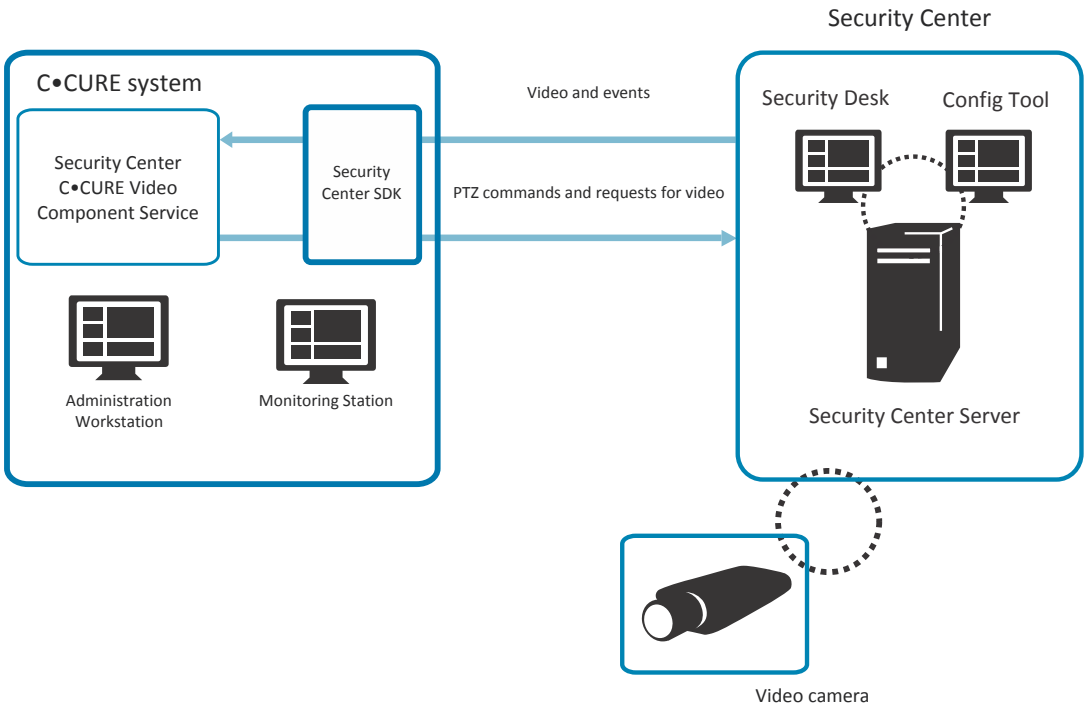
The integration allows you to do the following:

- View and play back Security Center video.
- Record Security Center cameras.
- Control Security Center PTZ cameras.
- Associate CCURE alarms and actions to Security Center events such as:
  - camera motion events
  - camera offline/online events
  - server offline/online events
- Jump to PTZ presets on Security Center cameras, and start PTZ patterns based on events created in CCURE.

  For example, a PTZ camera can be configured to point to the front entrance (preset 1) based on a “door forced” event.
- Monitor the Genetec Video Server and video camera status.

## How CCURE video integration works with Security Center

Through the CCURE video integration, PTZ camera commands and requests for video are sent from the CCURE system to Security Center. In turn, video and video events are sent from Security Center to CCURE, and viewed in the Monitoring Station.




Two components are involved in the video integration:

- **Security Center SDK:** The SDK is installed on CCURE servers and client workstations and is used by external applications to communicate with Security Center.
- **Security Center CCURE video component service:** The service, which is included in the CCURE video integration installation package installed on CCURE servers and client workstations, allows a Security Center system to be added as a video server. It uses the Security Center SDK to create a bridge between Security Center and the CCURE system.

## About integrating Security Center video in CCURE

The CCURE video integration allows CCURE users to receive live events and view Security Center video in CCURE 9000 access control systems.

- All cameras that are visible to the user in Security Center are imported to the CCURE Video Tree. As a result, the import might take a long time.
- After you initially import Security Center cameras into CCURE, when you add new cameras in Security Center, you must create them manually in CCURE if you do not want to re-import all the cameras.
- New cameras that are added or deleted in Security Center are not synchronized in the CCURE Video Tree. You must create or delete them manually.

- Cameras are imported with the camera name and logical ID used in Security Center. If you change the name or ID of the camera in Security Center, you must manually change it in CCURE, and vice versa.
- Cameras that have the same name are not supported in CCURE. If you import cameras that share the same name in Security Center, they are automatically renamed with a numeric identifier. For example, if you import three cameras called Back Door into CCURE, they are renamed Back Door, Back Door (1), and Back Door (2).
- If you try to import a camera with a name and logical ID that already exists in CCURE, you are prompted to change its name and description to the corresponding Security Center name and description, or leave it as is.
- All users on a CCURE system have the same PTZ priority in Security Center. PTZ usage is decided on a first come first serve basis. Once a user gains control over a PTZ camera, it is implicitly locked by that user.

# How failover works with the CCURE video integration

The CCURE video integration supports the failover of the following components in Security Center and in the CCURE system.

- Archiver
- Media Router
- Security Center Directory
- CCURE server

Failover of the CCURE server requires the CCURE system to be deployed in a high availability configuration, EverRunMX for example.

To configure backup servers for the Archiver, Media Router, 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 any component listed above fails and a backup server is configured, Security Center will automatically switch the component to its backup server and have the CCURE video integration to communicate with it. No user action is required when a failover occurs.

7

# Security Center video component installation

This section includes the following topics:

# Preparing to install the Security Center video component

Before you install the Security Center video component to integrate Security Center cameras in CCURE, you must perform some pre-installation steps.

**Before installing the Security Center video component:**

1 Read the release notes.
2 Install CCURE Server and Client version 2.30 or 2.40.
3 Install the Security Center SDK on the CCURE server and client workstations.

**IMPORTANT:** The SDK must be of the same version as Security Center.

4 Install Security Center 5.2 SR9 or later.

For more information about installing Security Center, see the *Security Center Installation and Upgrade Guide*.

5 Make sure you have the *CCURE Video* certificate supported in your Security Center license. You can verify this in the Config Tool home page by clicking **About** > **Certificates**.

## After you finish

Install the Security Center video component.

# Installing the Security Center video component

To integrate Security Center cameras in CCURE, the Security Center video component must be installed on the CCURE server and client workstations.

## Before you begin

- Perform the pre-installation tasks.

## What you should know

The video component needs to be installed on CCURE client and server computers.

**To install the video component:**

1 Download the Security Center video component installation package from the GTAP Product Downloads page.

2 Double-click the *Genetec Security Center - CCure Video Integration.exe* file, and follow the installation instructions.

**IMPORTANT:** Just before the installation begins, you are prompted to indicate if your installation is for a redundant setup, you must select the **Redundant server installation using supported third party redundancy** option and provide the virtual server (alias) name.

3 When prompted, allow the InstallShield Wizard to create the necessary firewall rules.

4 Once the InstallShield Wizard is complete, if you have an EMC Autostart or everRun MX Extend system, you should clear the **Start Tyco CrossFire services** option.

**NOTE:** You can leave the option checked if you are installing on a standalone CCURE server, or have an everRun MX High Availability setup.

5 Click **Finish**.

## After you finish

**IMPORTANT:** For CCURE systems setup for redundancy, you must install the Security Center video component on additional servers:

- If your CCURE 9000 system is configured for EMC AutoStart redundancy, you must also install the Security Center video component on each EMC host server.
- If your CCURE 9000 systems is configured for everRun MX High Availability redundancy, you must also install the Security Center component on one of the redundant virtual machines.
- If your CCURE 9000 system is configured using everRun MX Extend redundancy, you must also install the Security Center video component on one of the servers that share a host name, and on the external physical host.

# Preparing to upgrade the Security Center video component

If you already have Security Center video integrated with CCURE, and you want to upgrade your CCURE system to version 2.30 or 2.40, you must perform some pre-upgrade steps.

**Before upgrading the Security Center video component:**

1 Read the release notes.
2 Upgrade your CCURE server and client workstations to version 2.30 or 2.40.
3 Install the Security Center SDK on the CCURE server and client workstations.

**IMPORTANT:** The SDK must be of the same version as Security Center.

4 Upgrade your Security Center system to 5.2 SR9 or later.

For more information about upgrading Security Center, see the *Security Center Installation and Upgrade Guide*.

5 Make sure you have the *CCURE Video* certificate supported in your Security Center license. You can verify this in the Config Tool home page by clicking **About** > **Certificates**.

## After you finish

Upgrade the video component.

# Upgrading the Security Center video component

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

## Before you begin

## What you should know

The video component must be upgraded on CCURE client and server computers.

**To upgrade the video component:**

1 Uninstall the video component.

2 Download the Security Center video component installation package from the GTAP Product Downloads page.

3 Double-click the *Genetec Security Center - CCure Video Integration.exe* file, and follow the installation instructions.

**IMPORTANT:** Just before the installation begins, you are prompted to indicate if your installation is for a redundant setup, you must select the **Redundant server installation using supported third party redundancy** option and provide the virtual server (alias) name.

4 If prompted, allow the InstallShield Wizard to create the necessary firewall rules.

5 Once the InstallShield Wizard is complete, if you have an EMC Autostart or everRun MX Extend system, you should clear the **Start Tyco CrossFire services** option.

**NOTE:** You can leave the option checked if you are installing on a standalone CCURE server, or have an everRun MX High Availability setup.

6 Click **Finish**.

## After you finish

**IMPORTANT:** For CCURE systems setup for redundancy, you must install the Security Center video component on additional servers:

- If your CCURE 9000 system is configured for EMC AutoStart redundancy, you must also install the Security Center video component on each EMC host server.
- If your CCURE 9000 systems is configured for everRun MX High Availability redundancy, you must also install the Security Center component on one of the redundant virtual machines.
- If your CCURE 9000 system is configured using everRun MX Extend redundancy, you must also install the Security Center video component on one of the servers that share a host name, and on the external physical host.

8

# CCURE video integration configuration

This section includes the following topics:

# Creating a Security Center Video Server

To import Security Center cameras into CCURE, you must connect CCURE to Security Center by creating and configuring a Security Center Video Server.

## Before you begin

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

**NOTE:** Only settings specific to this integration are described. For information about other CCURE settings, see your CCURE documentation.

**To create the Security Center Video Server:**

1 Open the Administration Workstation application.

2 In the Navigation pane, click **Video**.

3 Right-click on the **Video folder**, and click **Video Folder** > **New**.

4 Enter a **Name** and **Description** for the new folder, and then click **Save and Close**.

5 In the **Video Tree**, right-click on the new folder, and click **Security Center Video Server** > **New**.

6 In the *Security Center Video Server* dialog box, enter a **Name** and **Description** for the server, and select the **Enabled option**.

7 In the **General** tab, and under **Server ID**, enter a **Time Zone**.

**TIP:** You should use the time zone of Security Center, so your cameras are in sync.

8 Under **Server Info**, enter the **User Name**, **Password**, and **IP address** of the Security Center server you want to connect to, and then click **Connect**.

**NOTE:** You can also select the **Log on using active directory** option to connect using active directory.

The **Online** option beside the **Connect** button should be selected.

9 In the **Poll Period** option under **Event Action Info**, select how often (in seconds) you want CCURE to check if Security Center is running.

10 Click **Import Cameras**.

If you have already imported cameras with the same ID number into CCURE, you are prompted to overwrite and name and description of the cameras with the information used in Security Center.

11 Click **Yes** to use the Security Center name and description, or click **No** to leave the information as is.

12 Click **Save and Close**.

You can now view video from your Security Center cameras in the Monitoring Station application. For information about viewing video in CCURE, see your CCURE documentation.

# Installing Security Center video component on EMC host machines

The Security Center video component service needs to be installed on all EMC host machines. The EMC resource group must be taken offline before the installation, and then some services must be manually restarted before the installation.

## What you should know

For more information about installing and configuring EMC AutoStart, see your EMC AutoStart documentation.

**To install Security Center video component on EMC host machines:**

1 Connect to an EMC host server.

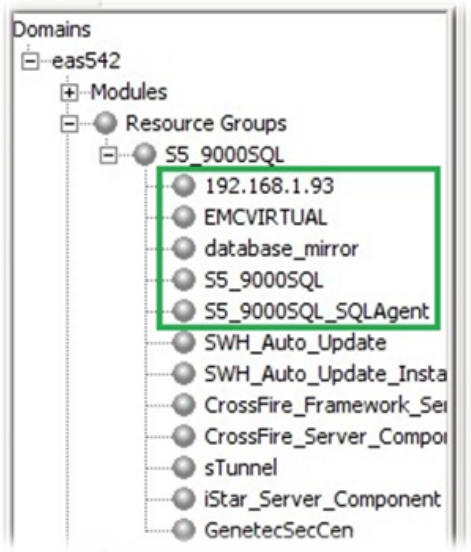
2 Open the **EMC AutoStart Console**. In the tree view of the AutoStart console under **Resource Groups**, right-click on the appropriate EMC resource group and select **Take Offline**.

**IMPORTANT:** Wait until all services listed under the resource group appear offline before proceeding to the next step. When a service is offline, it will turn grey.

Once all services in the resource group are offline, you must manually restart the following services:

- IP address
- Node Alias
- Database_mirror
- SQL server
- SQL Agent

**IMPORTANT:** The services must be started in the order that they appear under the resource group. For example, you must start with the IP Address and finish with the SQL Agent.




3 In the tree view of the AutoStart console, expand IP Addresses. Right-click on the virtual IP address and select Assign IP, then select the EMC host server on which you want to do the video component installation. Wait for the service to be online (green) before continuing to the next step.

4 In the tree view of the AutoStart console, expand **Node Aliases**. Right-click on the virtual node alias and select **Assign Node Alias**, then select the EMC host server on which you want to do the video component installation. Wait for the service to be online (green) before continuing to the next step.

5 In the tree view of the AutoStart console, expand **Data Sources**. Right-click on the data source and select **Attach Data Source**, then select the EMC host server on which you want to do the video component installation. Wait for the service to be online (green) before continuing to the next step.

6 In the tree view of the AutoStart console, expand **Services**. Right-click on the resource group and select Start Service, then select the EMC host server on which you want to do the video component installation. Wait for the service to be online (green) before continuing to the next step.

7 Right-click on the SQL Agent and select Start Service, then select the EMC host server on which you want to do the video component installation. Wait for the service to be online (green) before continuing to the next step.

8 Install the Security Center SDK on the EMC host server on which you have manually restarted the services.

**IMPORTANT:** The SDK must be of the same version as Security Center.

9 Install the Security Center video component on the EMC host server on which you have manually restarted the services.

**IMPORTANT:** During the install you must select the **Redundant server installation using supported third party redundancy** option and provide the virtual server (alias) name. You must also clear the **Start the Tyco CrossFire** services option at the end of the installation.

Once the installation is done on the selected server, to install the video component on another EMC host server, you must manually stop all the services in the reverse order that you started them. For example, stop the SQL Agent service first and unassign the IP last.

## After you finish

Add the Genetec Security Center video component service in the EMC AutoStart console.

**Related Topics**

Installing the Security Center video component on page 52

# Adding the Security Center video component service to the EMC AutoStart Console

Once you have installed the Security Center video component service, it needs to be added as a new service in the EMC Auto Start Console.

**To add Security Center video component service to the EMC AutoStart Console:**

1. Connect to one of the EMC host servers.
2. Open the EMC AutoStart Console. In the tree view of the AutoStart console under **Resource Groups**, right-click on the appropriate EMC resource group and select **Take Offline**.
3. In the AutoStart console tree view, right-click on **Services** and select **Create New Service**.
4. In the *New Service* dialog box beside **Service Name**, enter a name for the Security Center video component service.
5. Beside **Service to run**, select **Genetec CCURE Video Component Service** from the drop-down list.
6. Click **Apply**.
7. Under **Resource Groups**, click on the resource group and click the **Settings** tab.
8. Click the **Add** button and select **Service** from the drop-down list.
9. In the **Service Properties** page, under **Service Failure Action**, select **No Action**.
10. Under **Wait Settings**, select the **Wait until service is running** option and type "60 seconds."
11. Under **Wait Settings**, select the **Wait until service is stopped** option and type "60 seconds."
12. Click **Apply**.

    The Security Center CCURE Video Component Service is added to the end of the **Startup Sequence**, and is added as the first service in the **Shutdown sequence** in the *EMC AutoStart Console* dialog box.
13. Click **Apply**.

    The Security Center video component service is added to the services listed under the resource group.
14. Right-click the resource group and select **Bring Online**, then select the EMC host server you want to start.

You can now receive live events and view Security Center video in your CCURE system.

# Installing Security Center video component on an everRun MX system with two nodes

On a CCURE system configured for everRun MX High Availability, the Security Center video component service needs to be installed on one of the redundant virtual machines.

## What you should know

This task only covers the steps necessary to install the Security Center Video component. For more information about installing and configuring everRun MX High Availability, see your everRun MX documentation.

**To install Security Center video component on an everRun MX system with two nodes:**

1 Connect to Citrix XenCenter.

2 In the XenCenter tree view, select the active server and click the *Console* tab.

**NOTE:** If you connect to a console and cannot click inside the Windows, that server is not active, select the second server.

3 Install the Security Center SDK on the console.

**IMPORTANT:** The SDK must be of the same version as Security Center.

4 Install the Security Center video component on the console.

**IMPORTANT:** Make sure you leave the **Redundant server installation using supported third party redundancy option** unchecked, and at the end of the installation select **Start the Tyco CrossFire services**.

Once the Security Center video component is installed on one of the servers, the two servers will synchronize. You can monitor the synchronization status between he two nodes by connecting to the web interface of the everRun MX console. For more information, see your everRun MX documentation.

You can now receive live events and view Security Center video in your CCURE system.

**Related Topics**

Installing the Security Center video component on page 52

# Installing Security Center video component on an everRun MX system with three nodes

On a CCURE system configured for everRun MX Extend redundancy, the Security Center video component service needs to be installed on one of the host servers that share the same host name, and on the external physical host.

## What you should know

This task only covers the steps necessary to install the Security Center Video component. For more information about installing and configuring everRun MX Extend, see your everRun MX Extend documentation.

**To install Security Center video component on an everRun MX system with three nodes:**

1 Using your web browser, enter the IP address (or hostname) and the port number (separated by a colon) for the host on which the CA ARCserve Replication and High Availability (RHA) is running.

2 In the CA ARCserve RHA web application under **Quick Start**, click on **Scenario Management**.

3 In the CA ARCserve RHA Manager, under the **Scenario view**, right-click on the scenario and select **Stop**.

You can now install the Security Center on the first server set (first pair of nodes).

4 Connect to the first available server in the first pair of nodes.

5 Open the Server Configuration application and click on **Stop** in the CrossFire Framework Service.

6 Install the Security Center SDK.

**IMPORTANT:** The SDK must be of the same version as Security Center.

7 Install the Security Center video component on the console.

**IMPORTANT:** Make sure you leave the **Redundant server installation using supported third party redundancy option** unchecked, and at the end of the installation select **Start the Tyco CrossFire services**.

Once the installation is done, you must remove the services from the Extended Monitor. You do not need to install anything on the second server in the first pair of nodes.

8 In the **CA ARCserve RHA Manager**, click the **Root Directory** tab and double-click on **Custom Services**.

9 In the *Custom Service Management* dialog box, click **Uncheck All**, then click **OK**.

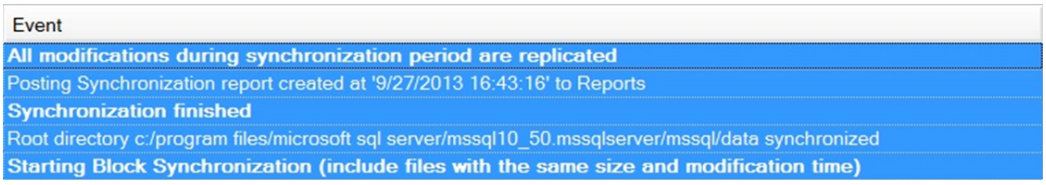
10 In the **CA ARCserve RHA Manager**, under **Scenario View**, right-click on the scenario and select **Run**.

a) When prompted to save the scenario since it was recently modified, click **OK**.

b) When prompted to run the scenario, click **Run**.

11 In the Run dialog box, select **Block synchronization** then click **OK**.

Wait for the replication process to finish. Once done you should see messages similar to the following in the Event pane:




You can now initiate a manual switchover of the Active Control service to perform the installation on the Replication server.

12 In the **CA ARCServe RHA Manager**, click on **Tools** > **Perform a Switchover**.

13 When prompted to perform the switchover, click **Yes**.

**IMPORTANT:** Make sure you do not select the **Run a Reverse replication Scenario** after the **Switchover** option.

Wait for the switchover to complete.

14 Connect to the last server node and install the Security Center SDK.

**IMPORTANT:** The SDK must be of the same version as Security Center.

15 Install the Security Center video component.

**IMPORTANT:** During the install you must select the **Redundant server installation using supported third party redundancy** option and provide the virtual server (alias) name. You must also clear the **Start Tyco CrossFire services** option at the end of the installation.

Once the installation is done, you must remove the services from the Extended Monitor. You do not need to install anything on the second server in the first pair of nodes.

16 In the **CA ARCserve RHA Manager**, select Tools > **Recover Active Server**.

17 In the *Recover Active Server* dialog box, select **Make Master Active**.

You will receive a message under **Event** telling you when the server is active.

18 In the **CA ARCserve RHA Manager**, right-click on the scenario and select **Stop**.

19 Click the **Root Directory** tab and double-click on **Custom Services**.

20 In the *Custom Service Management* dialog box, select the following services:

- SQL Server
- SQL Server Agent
- SoftwareHouse CrossFire Framework Service
- SoftwareHouse CrossFire Server Component Framework Service
- SoftwareHouse CrossFire iStar Driver Service
- Genetec CCURE Video Component Service

21 Set the **Start Order** for each service in the order specified in the previous step.

22 Click **OK**.

23 In the **CA ARCserve RHA Manager**, right-click on the scenario and select **Run**.

Wait for the replication process to finish. When it is finished you will see the **All modifications during synchronized period are replicated** event.

| Event |
| --- |
| **All modifications during synchronization period are replicated** |
| Posting Synchronization report created at '9/27/2013 17:20:49' to Reports |
| **Synchronization finished** |
| Root directory c:/program files/microsoft sql server/mssql10_50.mssqlserver/mssql/data synchronized |
| **Starting Block Synchronization (include files with the same size and modification time)** |
| SQL services started |
| Starting SQL services |
| **Starting scenario Genetec** |

You can now receive live events and view Security Center video in your CCURE system.

**Related Topics**

Installing the Security Center video component on page 52

# 9

# CCURE video integration troubleshooting

This section includes the following topics:

# Troubleshooting: Installation of the Security Center video component fails

If installation of the Security Center video component on the CCURE server fails and displays the error `InsertLicenseOption command failed with exit code -1003. The setup will abort.`, you may want to perform the following steps.

**To troubleshoot this issue:**

1 Restart installation of the video component.

2 When the installer prompts you to open the installation log, click **Yes**.

3 In the log file, locate the line similar to: `Z:\Program Files (x86)\Software House\SWHSystem\Crossfire\Tools\InsertLicenseOption.exe /U /V /S:DATABASE\INSTANCE /N:"Genetec Security Center Integration" /A:"Genetec Inc." /GUID:A59E0080-67F9-46EC-9F2A-9700FFE3DC09 /C:0 /P:92 /ObjectType:"Genetec.NextGenConnectedProgram.Video.Objects.SecurityCenterVideoServer"`

4 Copy both the path and the command, which starts with `InsertLicenseOption.exe`.

5 Open a command prompt in Windows, and then navigate to the copied path.

**Example:** *Z:\Program Files (x86)\Software House\SWHSystem\Crossfire\Tools*

6 Run the `InsertLicenseOption.exe` with the copied parameters.

**Example:** `InsertLicenseOption.exe /U /V /S:DATABASE\INSTANCE /N:"Genetec Security Center Integration" /A:"Genetec Inc." /GUID:A59E0080-67F9-46EC-9F2A-9700FFE3DC09 /C:0 /P:92 /ObjectType:"Genetec.NextGenConnectedProgram.Video.Objects.SecurityCenterVideoServer"`

7 If the command is successful, start the installation of the video component again.

# Where to find product information

You can find our product documentation in the following locations:

- **Installation package:** The documentation is available in the Documentation folder of the installation package. Some of the documents also have a direct download link to the latest version of the document.
- **Genetec Technical Assistance Portal (GTAP):** The latest version of the documentation is available from the GTAP Documents page. Note, you'll need a username and password to log on to GTAP.
- **Help:** Security Center client and web-based applications include help, which explain how the product works and provide instructions on how to use the product features. Patroller and the Sharp Portal also include context-sensitive help for each screen. To access the help, click Help, press F1, or tap the ? (question mark) in the different client applications.

# Technical support

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

- **Genetec Technical Assistance Portal (GTAP):** GTAP is a support website that provides in-depth support information, such as FAQs, knowledge base articles, user guides, supported device lists, training videos, product tools, and much more.

  Prior to contacting GTAC or opening a support case, it is important to look at this website for potential fixes, workarounds, or known issues. You can log in to GTAP or sign up at https://gtap.genetec.com.

- **Genetec Technical Assistance Center (GTAC):** If you cannot find your answers on GTAP, you can open a support case online at https://gtap.genetec.com. For GTAC's contact information in your region see the Contact page at https://gtap.genetec.com.

  **NOTE:** Before contacting GTAC, please have your System ID (available from the About button in your client application) and your SMA contract number (if applicable) ready.

- **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).

## Additional resources

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

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