



# **AutoVu Red Light Violation Detection Plugin Guide 2.1.0**

# Copyright notice

---

©2026 Genetec Inc. All rights reserved.

Genetec Inc. distributes this document with software that includes an end-user license agreement and is furnished under license and may be used only in accordance with the terms of the license agreement. The contents of this document are protected under copyright law.

The contents of this guide are furnished for informational use only and are subject to change without notice. Genetec Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

This publication may not be copied, modified, or reproduced in any form or for any purpose, nor can any derivative works be created therefrom without Genetec Inc.'s prior written consent.

Genetec Inc. reserves the right to revise and improve its products as it sees fit. This document describes the state of a product at the time of document's last revision, and may not reflect the product at all times in the future.

In no event shall Genetec Inc. be liable to any person or entity with respect to any loss or damage that is incidental to or consequential upon the instructions found in this document or the computer software and hardware products described herein.

Genetec™, AutoVu™, Citywise™, Community Connect™, Genetec Citigraf™, Federation™, Flexreader™, Genetec Clearance™, Genetec Retail Sense™, Genetec Traffic Sense™, Genetec Airport Sense™, Genetec Motoscan™, Genetec Mission Control™, Genetec ClearID™, Genetec Patroller™, Omnicast™, Stratocast™, Streamvault™, Synergis™, their respective logos, as well as the Mobius Strip Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions. KiwiSecurity™, KiwiVision™, Privacy Protector™ and their respective logos are trademarks of KiwiSecurity Software GmbH, and may be registered or pending registration in several jurisdictions.

Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

Patent pending. Genetec™ Security Center, Omnicast™, AutoVu™, Stratocast™, Citigraf™, Genetec Clearance™, and other Genetec™ products are the subject of pending patent applications, and may be the subject of issued patents, in the United States and in other jurisdictions worldwide.

All specifications are subject to change without notice.

## **Document information**

Document title: Red Light Violation Detection Plugin Guide 2.1.0

Document number: EN.410-036-V2.1.0.B(1)

Document update date: January 26, 2026

You can send your comments, corrections, and suggestions about this guide to [documentation@genetec.com](mailto:documentation@genetec.com).

## Contents

<b>Copyright notice</b> .....	<b>ii</b>
<b>Introduction to the Red Light Violation Detection plugin</b> .....	<b>4</b>
About the Red Light Violation Detection plugin.....	5
How the Red Light Violation Detection plugin works.....	6
Red Light Violation Detection Live report .....	7
Red Light Violation Detection report .....	11
<b>Release notes</b> .....	<b>12</b>
What's new in the Red Light Violation Detection plugin 2.0 .....	13
Resolved issues in the Red Light Violation Detection plugin 2.0 .....	15
Known issues in the Red Light Violation Detection plugin 2.1.0.....	16
Limitations in the Red Light Violation Detection plugin 2.1.0 .....	17
System requirements for the Red Light Violation Detection plugin 2.1.0 .....	<b>Error! Bookmark not defined.</b>
License options for the Red Light Violation Detection plugin.....	18
<b>Deploying the Red Light Violation Detection plugin</b> .....	<b>20</b>
Downloading and installing the Red Light Violation Detection plugin.....	21
Granting user privileges for the Red Light Violation Detection plugin.....	22
Setting up the SharpV camera in Security Center .....	24
Creating the plugin role .....	25
Configuring the Red Light Violation Detection plugin .....	26
Export bundle specifications.....	27
<b>Maintaining and troubleshooting the Red Light Violation Detection plugin</b> .....	<b>28</b>
Plugin installed, but missing from Security Desk and Config Tool .....	29
Error messages .....	30
<b>Additional procedures and resources</b> .....	<b>31</b>
Enabling failover on the plugin role .....	32
<b>Where to find product information</b> .....	<b>33</b>
<b>Technical support</b> .....	<b>34</b>

# Introduction to the Red Light Violation Detection plugin

This section includes the following topics:

What is the Red Light Violation Detection plugin? .....	5
How the Red Light Violation Detection plugin works with Security Center .....	6
Red Light Violation Detection Live report .....	7
Red Light Violation Detection report .....	11

## About the Red Light Violation Detection plugin

---

The Red Light Violation Detection plugin allows users and sworn officers to monitor and process potential red light violations in Security Center.

The Red Light Violation Detection plugin is installed on the Security Center expansion server and client workstations and is required to create the Red Light Violation Detection role.

You can use the plugin to do the following:

- Review potential red light violations
- Enter information about the infraction
- Replace the automatic snapshots from the video
- Exempt false positives
- Pre-validate violations (user)
- Validate violations and export a set of snapshots and information (officer)

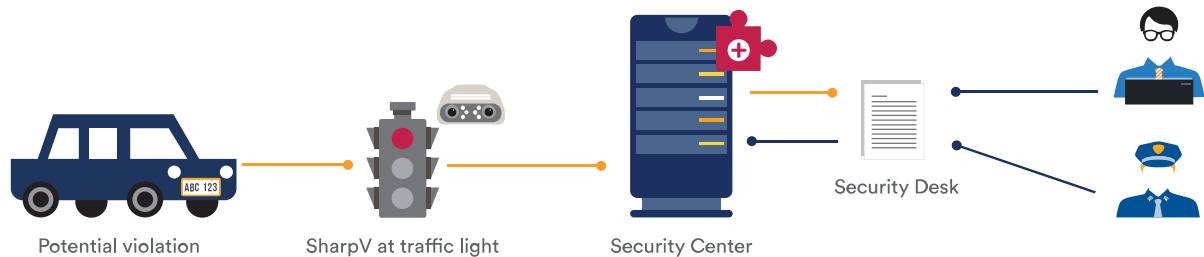
### **Other Security Center features you can use with the Red Light Violation Detection plugin**

The following native Security Center features give you these additional benefits:

- Failover improves the availability of imported entities. By assigning a secondary server to host the SDS Guardian plugin role, imported entities remain available if the primary server fails.
- The Federation™ feature joins multiple, independent Genetec™ systems into a single virtual system. With this feature, Security Center users can view and control entities that belong to remote systems, directly from their local Security Center system.

## How the Red Light Violation Detection plugin works

When the Red Light Violation Detection plugin is installed, you can integrate SharpV units as red light cameras in Security Center.



### Components

A typical deployment involves the following components:

The following components are required to integrate SharpV units as red light cameras in Security Center:

- **Genetec™ Red Light Violation Detection plugin:** The Red Light Violation Detection plugin is a software package installed on the Security Center expansion server and client workstations. The plugin is required to create the Red Light Violation Detection role.

The Red Light Violation Detection role is the Security Center role that manages the detection of potential violations when a license plate read is done while the light is red. The role handles communication between Security Center and the SharpV units.

- Records potential violations in its local database.
- Provides the *Red Light Violation Detection* task to manage these violations.

# Red Light Violation Detection Live report

The live report shows the 100 most recent violations and is refreshed automatically.

The following example show the *Red Light Violation Detection LIVE Report* task in Security Desk.

Id	Lpr unit	License plate	Timestamp	Pre-approved by	Approved by	Exempted by	Status	Locked by
5908	SharpV01507 (Entrance - AE Row-1)	E17PJJ	2019-07-03 8:07:15 AM				Unprocessed	dbauwens
5909	SHARPV02288 (India SR Entrance - AE Row-1)	E17PJJ	2019-07-03 8:07:15 AM				Unprocessed	
5910	SHARPV02288 (India SR Entrance - AE Row-1)	E17PJJ	2019-07-03 8:07:16 AM				Unprocessed	
5911	SHARPV00016 (Exit Middle - AE)	E17PJJ	2019-07-03 8:07:28 AM				Unprocessed	
5912	SharpV01507 (Entrance - AE Row-1)	G02RVG	2019-07-03 8:09:38 AM				Unprocessed	
5913	SHARPV05562 (New CPU Rev) (Entrance - AE)	G02RVG	2019-07-03 8:09:40 AM				Unprocessed	
5914	SHARPV02288 (India SR Entrance - AE Row-1)	G02RVG	2019-07-03 8:09:38 AM				Unprocessed	
5915	SHARPV02288 (India SR Entrance - AE Row-1)	G02RVG	2019-07-03 8:09:38 AM				Unprocessed	
5916	SHARPV05562 (New CPU Rev) (Entrance - AE)	G11EEH	2019-07-03 8:10:05 AM				Unprocessed	
5917	SharpV01507 (Entrance - AE Row-1)	G11EEH	2019-07-03 8:10:02 AM				Unprocessed	
5918	SHARPV02288 (India SR Entrance - AE Row-1)	G11EEH	2019-07-03 8:10:02 AM				Unprocessed	
5919	SHARPV02288 (India SR Entrance - AE Row-1)	G11EEH	2019-07-03 8:10:02 AM				Unprocessed	
5920	SHARPV05562 (New CPU Rev) (Entrance - AE)	E55GLX	2019-07-03 8:10:17 AM				Unprocessed	

## Description

- 1 Filter by selected SharpV unit.
- 2 Filter by selected status.
- 3 Filter by license plate.  
The field allows alphanumeric characters (for the license plate) and special characters such as "\*" and "?" as wildcards.
  - "\*" represents one or more alphanumeric characters. For example, A\*123 would return AB123, ABC123, A000123.
  - "?" represents one alphanumeric character. For example, A?123 would only return AB123 or A0123).

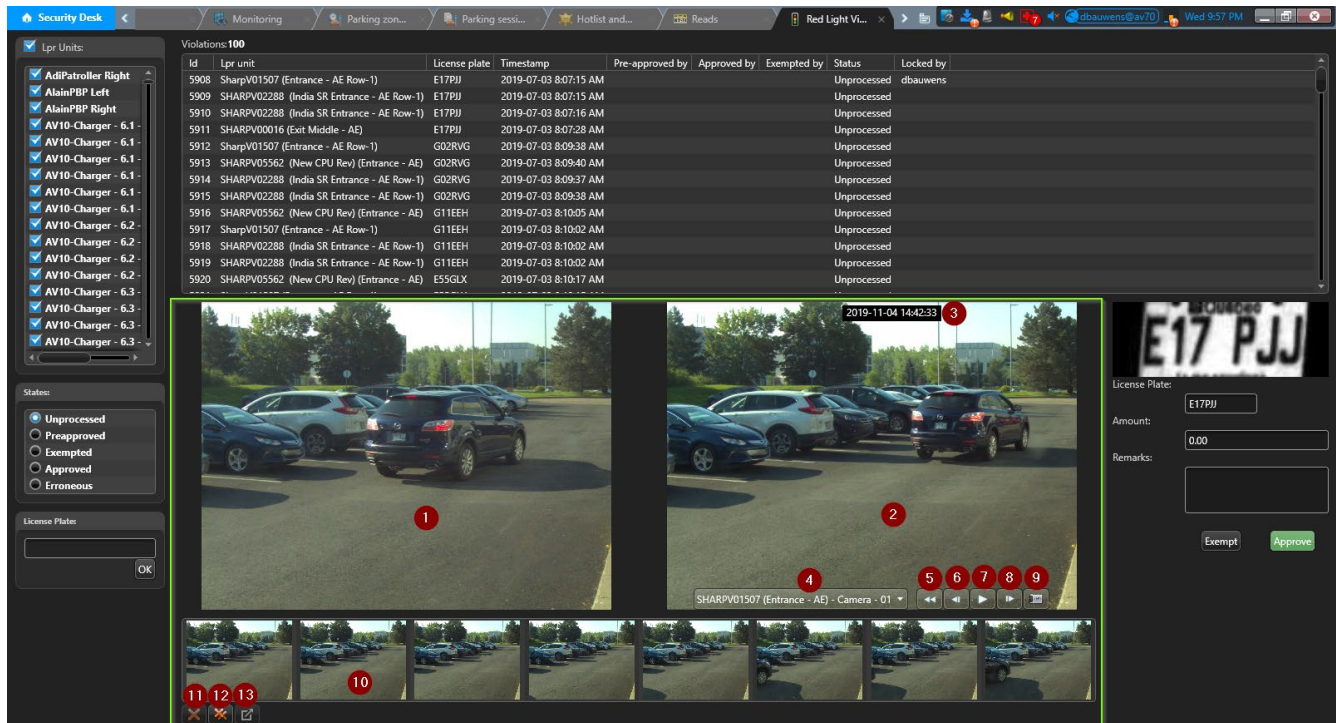
NOTE: If you use \* at the beginning of the license plate filter, the search will be slower because it will browse all the data.

The screenshot displays the Red Light Violation Detection plugin interface. On the left, there is a list of Lpr Units with checkboxes for various units like 'AdiPatroller Right', 'AlainPBP Left', and several 'AV10-Charger' units. The main area features a table titled 'Violations: 100' with the following columns: Id, Lpr unit, License plate, Timestamp, Pre-approved by, Approved by, Exempted by, Status, and Locked by. A red circle with the number '1' highlights this table. Below the table, there are two large video player windows showing a parking lot scene with a car. The bottom right of the interface includes a form for processing a violation, with fields for License Plate (E17PJJ), Amount (0.00), and Remarks, along with 'Exempt' and 'Approve' buttons.

Id	Lpr unit	License plate	Timestamp	Pre-approved by	Approved by	Exempted by	Status	Locked by
5908	SharpV01507 (Entrance - AE Row-1)	E17PJJ	2019-07-03 8:07:15 AM				Unprocessed	dbauwens
5909	SHARPV02288 (India SR Entrance - AE Row-1)	E17PJJ	2019-07-03 8:07:15 AM				Unprocessed	
5910	SHARPV02288 (India SR Entrance - AE Row-1)	E17PJJ	2019-07-03 8:07:16 AM				Unprocessed	
5911	SHARPV00016 (Exit Middle - AE)	E17PJJ	2019-07-03 8:07:28 AM				Unprocessed	
5912	SharpV01507 (Entrance - AE Row-1)	G02RVG	2019-07-03 8:09:38 AM				Unprocessed	
5913	SHARPV05562 (New CPU Rev) (Entrance - AE)	G02RVG	2019-07-03 8:09:40 AM				Unprocessed	
5914	SHARPV02288 (India SR Entrance - AE Row-1)	G02RVG	2019-07-03 8:09:37 AM				Unprocessed	
5915	SHARPV02288 (India SR Entrance - AE Row-1)	G02RVG	2019-07-03 8:09:38 AM				Unprocessed	
5916	SHARPV05562 (New CPU Rev) (Entrance - AE)	G11EEH	2019-07-03 8:10:05 AM				Unprocessed	
5917	SharpV01507 (Entrance - AE Row-1)	G11EEH	2019-07-03 8:10:02 AM				Unprocessed	
5918	SHARPV02288 (India SR Entrance - AE Row-1)	G11EEH	2019-07-03 8:10:02 AM				Unprocessed	
5919	SHARPV02288 (India SR Entrance - AE Row-1)	G11EEH	2019-07-03 8:10:02 AM				Unprocessed	
5920	SHARPV05562 (New CPU Rev) (Entrance - AE)	E55GLX	2019-07-03 8:10:17 AM				Unprocessed	

## Description

- 1 Live filtered report table.  
Select a row to review and process the violation.  
  
NOTE: When a row is selected, it is locked by the user currently reviewing it.



## Description

- 1 Context image.
- 2 Camera archive feed linked to the ALPR unit.
- 3 Video timestamp.
- 4 List of video sources associated with the ALPR unit.
- 5 Rewind video.
- 6 Previous video frame.
- 7 Play video.
- 8 Next video frame.
- 9 Take a snapshot of the video.  
NOTE: You can take a maximum of 8 snapshots.
- 10 List of snapshots. The first time the violation is loaded, the list is filled by 8 autogenerated snapshots (configurable).

- 11 Delete selected snapshot.
- 12 Delete all snapshots.
- 13 Open the selected snapshot in a popup.

The screenshot displays the Red Light Violation Detection plugin interface. On the left, there is a sidebar with 'Lpr Units' and 'Status' sections. The main area shows a table of violations with columns for Id, Lpr unit, License plate, Timestamp, Pre-approved by, Approved by, Exempted by, Status, and Locked by. Below the table, there are two video player windows showing a car in a parking lot. A popup window is open over the right video player, showing the license plate 'E17 PJJ', a corrected license plate 'E17PJJ', an amount of '0.00', and a remarks field. At the bottom of the popup are 'Exempt' and 'Approve' buttons.

## Description

- 1 Plate image.
- 2 Corrected license plate information, in case the report license plate is misread or incomplete.
- 3 Infraction fees.
- 4 Remarks about the violation.
- 5 Exempt the violation. It flags the violation detection as a false positive.
- 6 Preapprove or approve depending on the current user privileges.
  - **Preapprove:** Changes the status to *Preapprove*.
  - **Approve:** Changes the status to *Approve* and exports the data bundle to the configured

# Red Light Violation Detection report

The report is very similar to the live report but is not automatically refreshed. It shows the violations within a selected time range.

The following screenshots shows the *Red Light Violation Detection Report* task in Security Desk.

The screenshot displays the Security Desk interface for the Red Light Violation Detection Report task. The interface is divided into several sections:

- Violations List:** A table showing a list of violations with columns for Id, Lpr unit, License plate, Timestamp, Pre-approved by, Approved by, Exempted by, Status, and Locked by. The table contains 11 rows of data.
- Video Player:** A central video player showing a parking lot scene. The timestamp is 2019-11-04 16:42:33. The license plate E17 PJJ is visible in the video.
- License Plate:** A field showing the license plate E17 PJJ.
- Amount:** A field showing the amount 0.00.
- Remarks:** A text area for entering remarks.
- Buttons:** Exempt and Approve buttons.
- Time Frame:** A section with radio buttons for 'During the last' and 'Specific range'. The 'During the last' option is selected. The time range is set to 1 Day.
- Generate Report:** A green button at the bottom left of the interface.

## Description

- 1 Relative time frame.
- 2 Specific range time frame.
- 3 Generate the report.

# 2

## Release notes

This section includes the following topics:

- What’s new in the Red Light Violation Detection plugin 2.1.0 ..... 13
- What’s new in the Red Light Violation Detection plugin 2.0 ..... 13
- Resolved issues in the Red Light Violation Detection plugin 2.0 ..... 15
- Known issues in the Red Light Violation Detection plugin 2.1.0..... 16
- Limitations in the Red Light Violation Detection plugin 2.1.0 ..... 17
- System requirements for the Red Light Violation Detection plugin 2.1.0 ..... **Error! Bookmark not defined.**
- License options for the Red Light Violation Detection plugin..... 18

# What's new in the Red Light Violation Detection plugin

## 2.1.0

---

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

### **Plate tilt filtering**

You can now ignore license plates that fall outside a specified tilt range. This helps reduce false violations caused by vehicles turning right on a red light.

### **Platform compatibility**

This release ensures the plugin remains fully compatible with upcoming versions of Security Center and supports future platform updates.

# What's new in the Red Light Violation Detection plugin 2.0.0

---

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

## **Red Light Violation Detection 2.0**

- The new *Red Light Violation Detection Report* is similar to the live report but is not automatically refreshed. It allows you to search for violations using a timeframe filter.

## **Red Light Violation Detection 1.1**

- The minimum number of snapshots is no longer 1. A detection can be exported with 0 snapshots.
- The number of pre-selected snapshots is now configurable in the options.
- Configuration of tolerance for relevant video in a detection.

# Resolved issues in the Red Light Violation Detection plugin 2.0.0

---

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

The following software issues were resolved in the Red Light Violation Detection plugin 2.0.

Issue	Description
2236599	Violations are removed from the list when using the <i>State + license plate</i> filters.
2318620	Unable to find video with a certain combination of acceptable delta and the snapshot start time before the read.

# Known issues in the Red Light Violation Detection plugin 2.1.0

---

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

The Red Light Violation Detection plugin 2.1.0 includes the following known issues.

Issue	Description
2236387	Snapshots are sometime not created in the logical time stamp order.

---

# Limitations in the Red Light Violation Detection plugin

## 2.1.0

---

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

The Red Light Violation Detection plugin 2.1.0 includes the following known limitations.

Limitation	Description
1	Because the plugin uses a custom privilege (Approve / Export), then it must be installed on all the machines where we can have the Directory (expansion server, failover server), so the Directory can know this privilege.
2	The plugin must be up and running to record potential violations (only works on live reads).
3	The input value for the red light must be the same for all the Sharp units. It is advised not to use "Low" as it is the default value for all the units if no input.
4	The LprUnit must have an available video archive at the time of the infraction.
5	If multiple cameras are associated to the LprUnit, the first one in the configured list will be used for the violation report. It is possible to select the feed once the violation is loaded, but the snapshots will be done on the first one (if available).
6	The role must have sufficient privileges to be able to export in the configured export folder.
2354501	Federated units have no information in the report grid.

## Product compatibility

---

To be eligible for technical support, you must install the Red Light Violation Detection plugin with versions of Security Center that are certified or supported by design.

For the latest compatibility information, see [Supported plugins in Security Center](#) on the Genetec™ TechDoc Hub.

- As a minimum, the Red Light Violation Detection plugin requires Security Center 5.8.
- The minimum SharpV OS version must be 12.7. SharpV OS 12.7 includes management of the SharpV inputs, which is required for the red light integration.

# License options for the Red Light Violation Detection plugin

---

Before installing the plugin, you must update your Security Center license to include a certificate for the plugin. To update your license, contact us and provide the part numbers listed in this topic.

Part number	Description	Requirements
GSC-AV-S-RLVD	Base package for the Red Light Violation Detection plugin.	<ul style="list-style-type: none"><li>• Synergis™ Enterprise</li><li>• AutoVu</li></ul>

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

In addition to a certificate for your plugin, ensure that your Security Center license includes all the options you expect to use in Security Center. For example, if you integrated a system that has visitors, you need the 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](#).

# Deploying the Red Light Violation Detection plugin

This section includes the following topics:

Downloading and installing the Red Light Violation Detection plugin.....	21
Granting user privileges for the Red Light Violation Detection plugin.....	22
Creating the plugin role .....	24
Configurations of the Red Light Violation Detection.....	<b>Error! Bookmark not defined.</b>
Export bundle specifications.....	27

# Downloading and installing the Red Light Violation Detection plugin

---

You must install the Red Light Violation Detection plugin on a Security Center expansion server and on all client workstations from which you want to manage Red Light Violation Detection entities.

## Before you begin

Ensure the following:

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

## What you should know

**BEST PRACTICE:** Install the plugin on an expansion server to ensure the availability of Security Center.

- (Optional) To improve system availability, you can enable failover for the plugin server.
- If you want all plugin functionality, you must install the plugin on all Security Center client workstations.

## To install the Red Light Violation Detection plugin:

- 1 Open the GTAP [Product Download](#) page.
- 2 Under **Download Finder**, select your version of Security Center.
- 3 From the **Genetec Plugins** section, download the package for your product.
- 4 Run the `.exe` file, and then unzip the file.  
By default, the file is unzipped to `C:\Genetec`.
- 5 Open the extracted folder, right-click the `setup.exe` file, and click **Run as administrator**.
- 6 In the extracted folder, browse to the plugin folder, and then right-click the `setup.exe` file, and click **Run as administrator**.
- 7 Follow the installation instructions.
- 8 On the *Installation Wizard Completed* page, click **Finish**.  
**IMPORTANT:** The **Restart Genetec™ Server** option is selected by default. You can clear this option if you do not want to restart the Genetec™ Server immediately. However, you must restart the Genetec™ Server to complete the plugin installation.
- 9 Close, and then open, any instances of Config Tool and Security Desk to load the plugin.

## After you finish

Create the plugin role.

# Granting user privileges for the Red Light Violation Detection plugin

To integrate and monitor red light cameras in Security Center, you must have the correct user privileges. The users who will use the task in Security Desk should have the basic AutoVu investigation rights.

## What you should know

For administrators to install and configure the plugin in Config Tool, and for operators to monitor the integrated devices in Security Desk, the correct user privileges must be granted to their user accounts.

This topic lists the minimum user privileges required. You might require more privileges, depending on the tasks you want to perform in Config Tool and Security Desk.

For a complete list of privileges in Security Center, refer to the [Security Center privileges](#) spreadsheet.

## To grant user privileges:

- 1 From the Config Tool home page, open the *User management* task.
- 2 Select the user that will monitor Red Light Violation Detection, and click the **Privileges** tab.
- 3 Set the following privileges to **Allow**.

Privilege	Task
<b>Application privileges</b>	
Config Tool	To use Config Tool (mandatory for the admin to configure the plugin).
Security Desk	To use Security Desk (mandatory for the user/officer to review the violations).
<b>Task privileges &gt; Administration</b>	
Plugins	To use the <i>Plugins</i> task in Config Tool (mandatory for the admin to configure the plugin).
<b>Task privileges &gt; Investigation &gt; Video</b>	
Archives	To be able to use the video archives in a report (mandatory for the user/officer to review the violations).
<b>Task privileges &gt; Investigation &gt; LPR</b>	
Approve / Export	To give the rights to Approve a violation and export

the data in Security Desk (otherwise Preapprove by default).

---

**Action privileges > Cameras**

---

Save/Modify/print snapshots

To be able to take snapshots from the video (mandatory for the user/officer to review the violations).

---

View playback

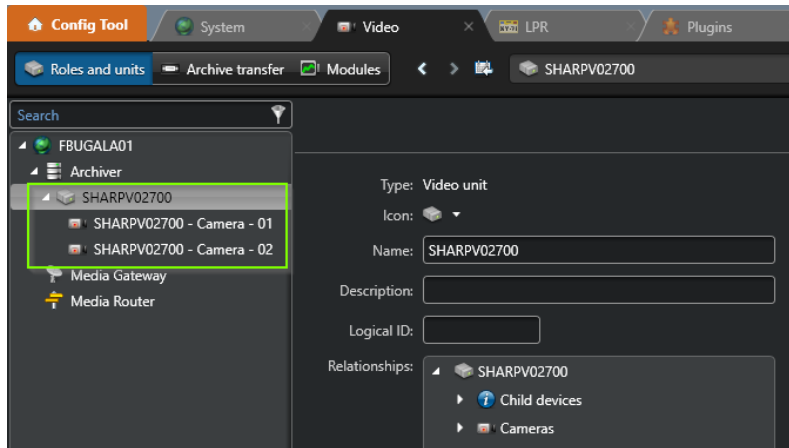
To be able to play the archive video (mandatory for the user/officer to review the violations).

- 4 Click **Apply**.

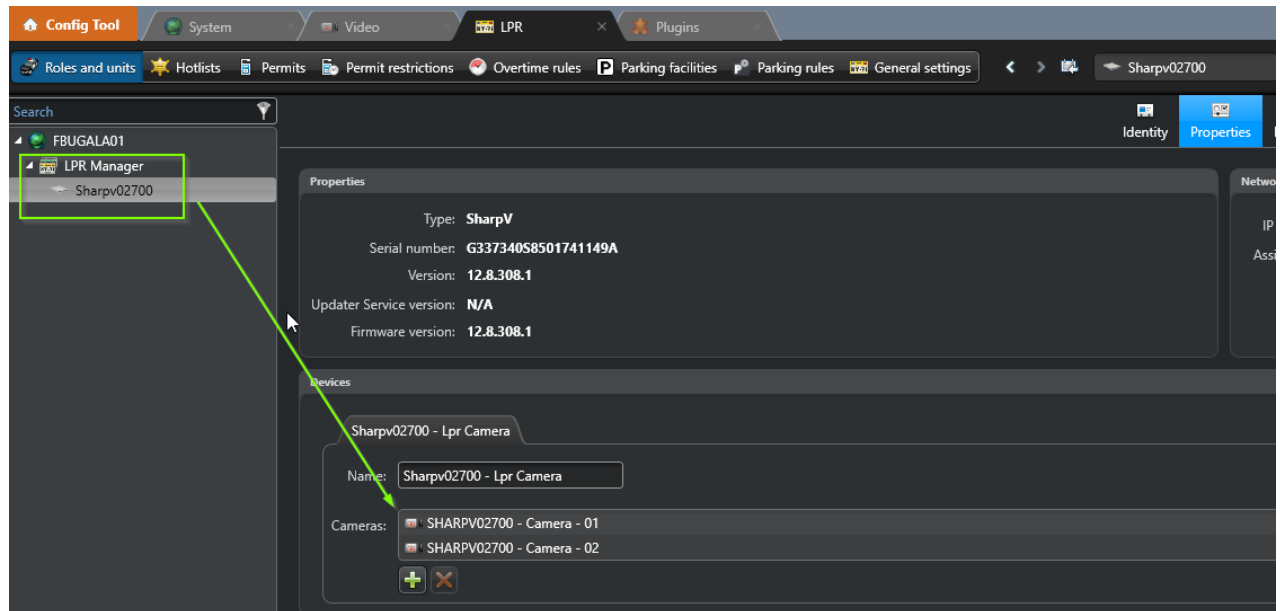
# Setting up the SharpV camera in Security Center

Before you create the plugin role, you must add the SharpV in the Archiver role.

1. Add the SharpV unit in the Archiver role. For more information, see the [Security Center Administrator Guide](#).



2. You must associate a video unit with the SharpV. Video and snapshots from the video unit are added to the report. You can add one or more video units. You can also include the SharpV, which adds the video feed from the SharpV context camera.



# Creating the plugin role

---

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

## Before you begin

- Link the SharpV cameras to the proper video units. For more information, see [Setting up the SharpV camera in Security Center](#).
- 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.**

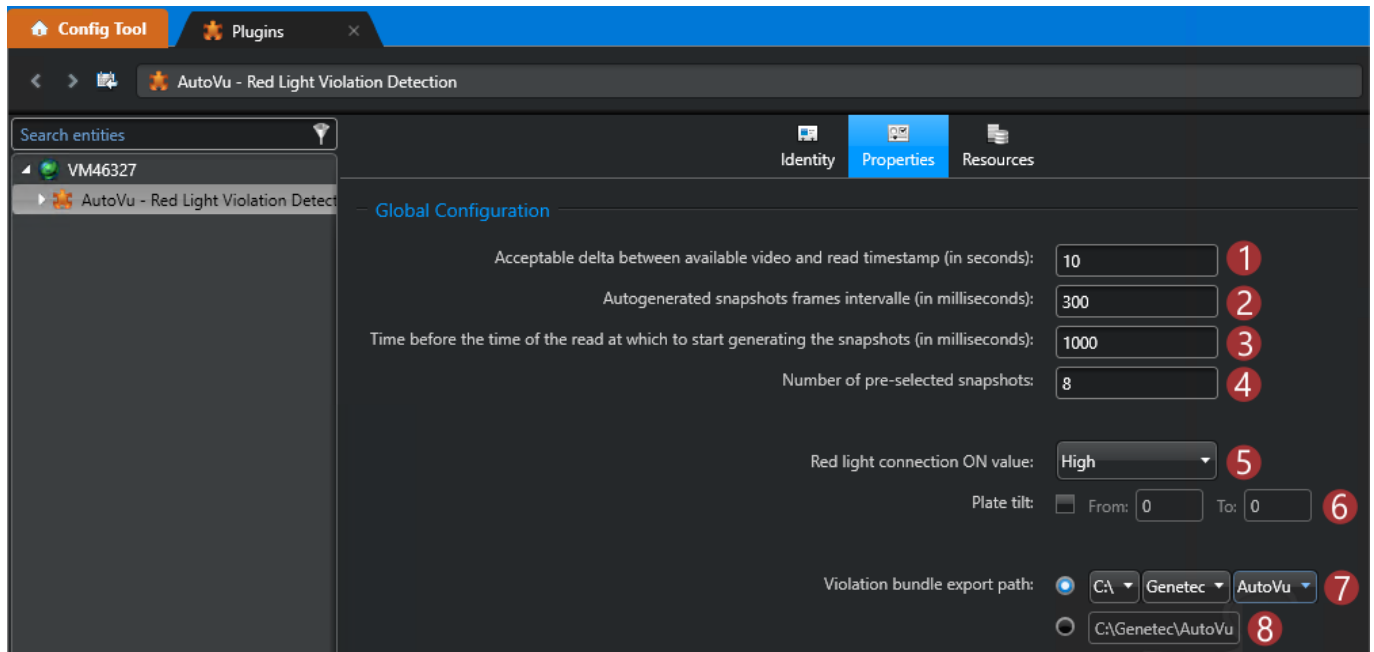
- 5 Click **Next**.
- 6 On the *Creation summary* page, review the information, and then click **Create**, or **Back** to make changes.
- 7 After the plugin is created, the following message appears: `The operation was successful.`
- 8 Click **Close**.

The plugin role appears in the entity browser.

# Configuring the Red Light Violation Detection plugin

You must configure the plugin to specify the timing of license plate reads and how reads are exported.

To configure the plugin:



1. Configure the acceptable delay between the time of the read and the time of the available video, for it to be considered relevant.
2. Set the time in milliseconds between each automatic video snapshot (the first time a violation is reviewed).
3. Set the time for the first automatic snapshot, before the actual time of the read.
4. Set the number of pre-selected snapshots to be generated automatically.
5. Select the input value that will enable the recording of potential violations (light is red). This value is common to all the ALPR units.
6. Configure the plugin to ignore license plates where the angle of the plate is outside a certain range. This allows the plugin to ignore cars that are turning right on a red light.
7. Select the path on the main server that will be used to export the JSON bundle containing the violation data.
8. (Optional) Enter a path manually. It can be a server path (\\server\export).

**IMPORTANT:** The plugin role must have sufficient privileges to read/write in the folder.

NOTE: For the plugin to be able to generate relevant snapshots, it is advised to have a minimum of 1 key frame per second for the video feed.

## Export bundle specifications

---

Every time a violation is approved, a bundle is exported in the configured export folder. The bundle is a JSON file with the following structure:

```
{
  "LprUnitName": "Sharp",
  "ReadTimestamp": "2019-06-19_03-15-45",
  "ReadImage": "/9j/4AAQSkZJRgABAQEAYABgAAD...",
  "ContextImage": "/9j/4AAQSkZJRgABAQEAYABgAAD...",
  "Snapshots": ["iVBORw0KGgoAAAANSUhEUgAAAPA...", "iVBORw0KGgoAAAANSUhEUgAABQA..."],
  "ViolationInformation": {
    "Amount": 200.0,
    "LicensePlate": "ABC123",
    "Remarks": null
  }
}
```

- All the images are bytes arrays encoded in a base 64 string.
- The amount is a float value.
- The license plate and the remarks are both strings.

The exported file is created as follows: **violationDetectionId\_ReadTimestamp\_LicensePlate.js**

Example: **1\_2019-06-25\_08-40-01-ABC123.js**

Timestamp format is **yyyy-MM-dd\_hh-mm-ss**

# 4

## Maintaining and troubleshooting the Red Light Violation Detection plugin

This section includes the following topics:

Plugin installed, but missing from Security Desk and Config Tool .....	29
Error messages .....	30

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

---

If the plugin role's **Properties** tab and task 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 the red light units.

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 Red Light Violation Detection task for this plugin.

## 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**.
- **Solution 5:** Make sure the user has access to the partition the plugin is installed on.

## Error messages

---

You notice that the Plugin role icon is yellow or red. To help you troubleshoot the various issues, learn about their possible causes and their respective solutions.

If the problem persists, restart the plugin role. Eventually try restarting the server on which the plugin role is running.

# 5

## Additional procedures and resources

This section includes the following topics:

Enabling failover on the plugin role .....	32
--	----

# 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 server. The process follows a standard set of steps.

## 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.

# Where to find product information

You can find our product documentation in the following locations:

- Genetec™ TechDoc Hub: The latest documentation is available on the TechDoc Hub. To access the TechDoc Hub, log on to [Genetec™ Portal](#) and click [TechDoc Hub](#). Can't find what you're looking for? Contact [documentation@genetec.com](mailto: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](mailto: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](mailto: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](mailto: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.