



SharpV Administrator Guide 12.6

Document last updated: August 9, 2018

Legal notices

©2018 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: SharpV Administrator Guide 12.6

Document number: EN.400.008-V12.6.B(1)

Document update date: August 9, 2018

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

About this guide

This guide provides you with a complete source of information about the SharpV web portal and how to configure your SharpV cameras. It explains the basic settings you must configure before your SharpV can be used.

Last-minute updates can be found in the *SharpOS Release Notes*.

You'll still need to refer to the *Security Center Administrator Guide* since some of the configuration for LPR is done in Security Center Config Tool. For example, information about configuring the LPR Manager role and creating hotlists is covered in the *Security Center Administrator Guide*.

This guide assumes you are familiar with Security Center systems.

Notes and notices

The following notes and safety notices might appear in this guide:

TIP: Provides a useful hint, suggestion, or practical application of a topic or step.

NOTE: Describes a special case or expands on an important point.

IMPORTANT: Points out critical information about a topic or step.

CAUTION: Indicates that an action or step might cause loss of data, security problems, or performance issues.

WARNING: Indicates that an action or step might cause physical harm or damage the hardware.

Contents

Preface

Legal notices	ii
About this guide	iii

Chapter 1: Introduction

About AutoVu	2
About the AutoVu SharpV	4
SharpV LPR using deep learning	4
Logging on to the SharpV web portal	5
SharpV web portal interface overview	7
Changing your logon password in the SharpV web portal	8
Rebooting cameras from the SharpV web portal	9
Importing and exporting settings in the SharpV web portal	10
Synchronizing the SharpV clock	11

Chapter 2: Configuration

Security configuration in SharpV Portal	13
Encrypting connection to the SharpV using a self-signed certificate	14
Encrypting connection to the SharpV using a signed certificate	17
Configuring SharpV network settings	19
Connecting to a SharpV camera using the fallback IP address	19
Viewing the camera feeds from a SharpV camera	20
Calibrating the SharpV zoom and focus	21
Plate read distances for SharpV lenses	24
About SharpV exposure adjustment for indoor installations	25
Setting custom SharpV LPR camera exposure levels for indoor installations	25
Setting custom SharpV context camera exposure levels for indoor installations	26
About SharpV exposure adjustment for outdoor installations	27
Setting custom SharpV LPR camera exposure levels for outdoor installations	27
Troubleshooting outdoor exposure issues for the SharpV LPR camera	28
Troubleshooting outdoor exposure issues for the SharpV context camera	29
Configuring SharpV analytics	31
Calibrating the virtual loop	32
Calibrating speed estimation	38
Configuring where the SharpV sends its LPR data	41
SharpV camera connections to Security Center	41
SharpV communication ports	42
Adding a SharpV camera to the LPR Manager	43
Adding a SharpV camera to the Archiver	44
Configuring the SharpV FTP extension	45
Modifications you can make to the SharpV FTP XML template	45
Configuring the SharpV HTTP extension	47
Examples of JSON and XML LPR events for the SharpV HTTP extension	47
Configuring Syslog for SharpV log files	50

Chapter 3: Upgrade

Updating the SharpV from the Sharp Portal	52
Updating the SharpV from Security Center	53

Chapter 4: Sharp Portal reference

Sharp Portal - Overview page	55
Sharp Portal - Camera feeds page	57
Sharp Portal - Network page	58
Sharp Portal - Security page	59
Sharp Portal - Zoom and focus page	60
Sharp Portal - Cameras page	62
Sharp Portal - Analytics page	63
Sharp Portal - Extension page	65
Sharp Portal - Date and time page	67
Sharp Portal - Power options page	68
Sharp Portal - Maintenance page	69
Sharp Portal - Logs page	70

Chapter 5: Troubleshooting for SharpV fixed installation

LED status on the SharpV camera unit	72
Resetting a lost password for the SharpV web portal	74

Glossary	76
--------------------	----

Where to find product information	95
---	----

Technical support	96
-----------------------------	----

Introduction

This section includes the following topics:

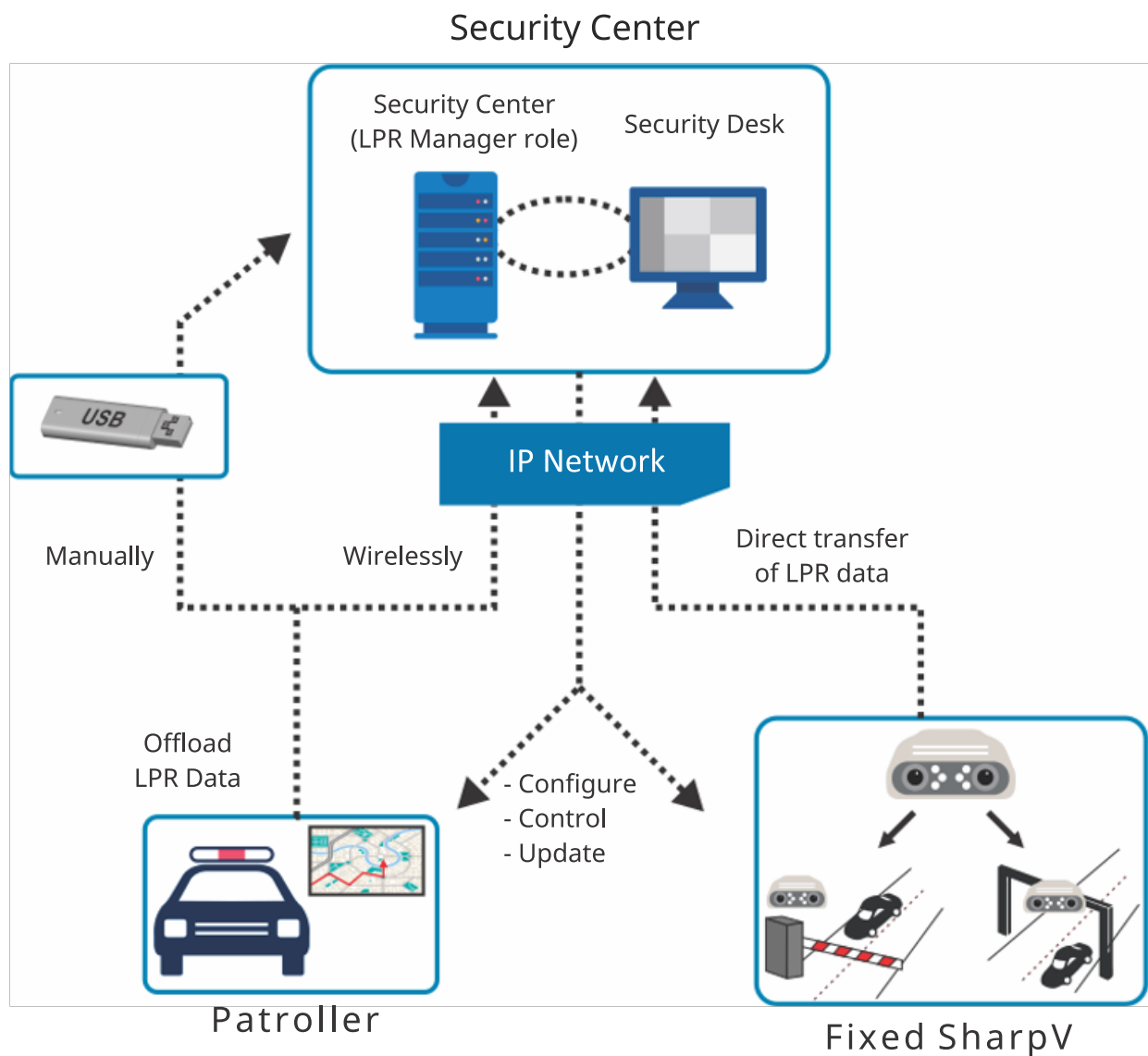
- ["About AutoVu" on page 2](#)
- ["About the AutoVu SharpV" on page 4](#)
- ["Logging on to the SharpV web portal" on page 5](#)
- ["SharpV web portal interface overview" on page 7](#)
- ["Changing your logon password in the SharpV web portal" on page 8](#)
- ["Rebooting cameras from the SharpV web portal" on page 9](#)
- ["Importing and exporting settings in the SharpV web portal" on page 10](#)
- ["Synchronizing the SharpV clock" on page 11](#)

About AutoVu™

AutoVu™ is the automatic license plate recognition (ALPR) system of a Security Center system that automates license plate reading and identification. Deployed in both fixed and mobile installations, it lets you extend your physical security into your parking lots and perimeter, so you are always aware of vehicles moving in and out of your facilities.

AutoVu™ Sharp cameras capture license plate images, and send the data to Genetec Patroller™ or Security Center to verify against lists of vehicles of interest (hotlists) and vehicles with permits (permit lists). You can install AutoVu™ in a fixed configuration (for example, on a pole in a parking lot), or in a mobile configuration (for example, on a police car). You can use AutoVu™ for scofflaw and wanted vehicle identification, city-wide surveillance, parking enforcement, parking permit control, vehicle inventory, security, and access control.

The following diagram shows how a typical AutoVu™ system works:



Example

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

<https://www.youtube.com/embed/U-fF-2yvDMw>

About the AutoVu™ SharpV

The AutoVu™ SharpV is an all-in-one specialized automatic license plate recognition (ALPR) device which combines two high-definition cameras with onboard processing and illumination in a ruggedized, environmentally sealed unit.



* Depending on the camera options, the five LPR illuminators might emit light that is visible in dark conditions. The single context camera illuminator does not emit visible light.

SharpV LPR using deep learning

SharpV cameras running SharpOS 12.5 or higher uses deep learning to classify license plates and to perform character recognition.

While off-the-shelf deep learning solutions are commercially available for LPR, their results can be unpredictable. With Genetec's hardware and software engineering expertise, we have built our own deep learning system from the ground up. This includes development of the Deep Neural Network (DNN), training of the DNN using Sharp camera images, and optimizing the system to run on existing SharpV hardware. As a result, depending on the regional contexts, you can expect more than a 50% reduction in plate capture errors and character recognition errors when compared to widely-used classical algorithms. This represents a significant reduction in the time spent manually correcting plate reads.

As our DNN continues to develop, we will introduce it to more aspects of the LPR process. You will be able to take advantage of these improvements with future SharpOS releases.

Logging on to the SharpV web portal

To configure SharpV cameras, you must first log on to the web portal.

Before you begin

- You need to know the IP address or name of the SharpV camera you want to connect to:
 - **SharpV name:** You can find the SharpV name (for example, SharpV12345) on the label on the back of the camera.
 - **SharpV fallback IP address:** The fallback IP address is 192.168.10.100. The fallback IP address is only available if the camera is in DHCP mode (default). After camera startup, the camera searches for a DHCP server. If no DHCP server is present on the network after two minutes, the fallback IP address is made available.

What you should know

- You can access the SharpV web portal using the following browsers:
 - Internet Explorer version 11 and later
 - Google Chrome version 46 and later
- To ensure that camera feeds are displayed correctly, only open one instance of the SharpV web portal at a time.
- To log onto the web portal, the SharpV must be provided with PoE+ power that conforms to IEEE 802.3at standards. If the camera encounters power issues, you can see details in the *Sharp Portal - Logs* page. For more information on specifications for the SharpV, see the *AutoVu Handbook for SharpV Fixed Installations*.

To log on to the SharpV web portal:

- 1 Open your Web browser, and go to `http://<SharpV name or IP address>`.

Example:

- If the SharpV camera's IP address is 192.168.10.100, enter `http://192.168.10.100`.
- If the SharpV camera's name is SharpV12345, enter `http://SharpV12345`.

- 2 Enter the **Username** and **Password**.

Default for first logon: Username: admin, Password: Genetec

- 3 Click **Connect**.

If this is the first time you are logging on to the SharpV:

- 1 Select the power line frequency and click **Next**.
 - **60 Hz:** Generally used in North America and South America
 - **50 Hz:** Generally used in Africa, Australia, Asia, and Europe

For more information on the power line frequency used in your installation location, [click here](#).

- 2 Change the password.

Enter and confirm the new password, and click **Next**.

NOTE:

- If you forget your password, [you can reset it from the logon page](#).
- You cannot modify the username.

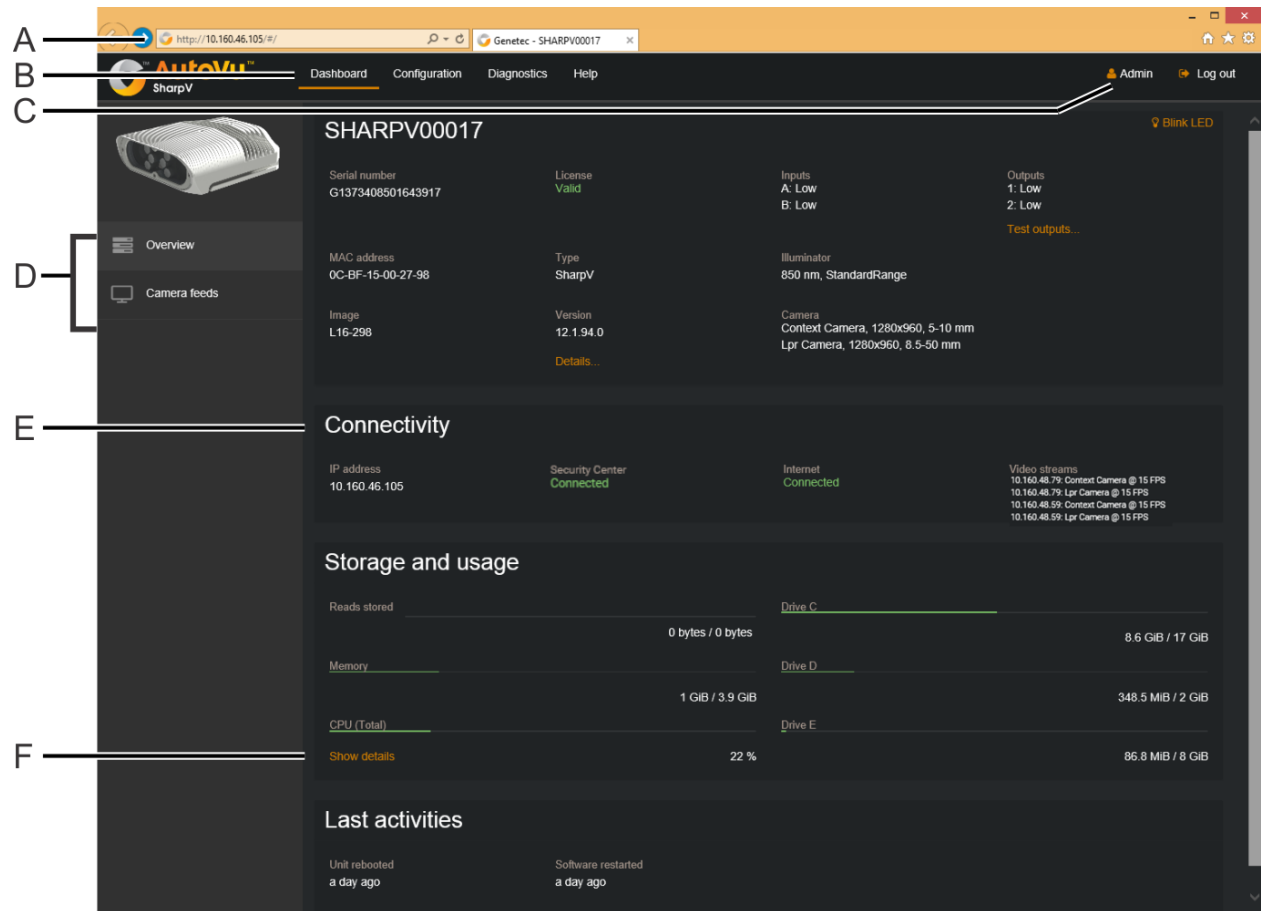
After successfully logging on, the web portal for the SharpV camera opens to the **Overview** page of the **Dashboard** menu.

Related Topics

[Sharp Portal - Logs page](#) on page 70

SharpV web portal interface overview

To familiarize yourself with the SharpV web portal, you can take a tour of the main areas of the user interface.



A	SharpV web portal address	Type the SharpV name or the IP address. The format is <code>http://Sharp12345</code> or <code>http://192.168.10.100</code>
B	Menu	Displays the main categories of the SharpV web portal.
C	Current user	Shows the current user and log out command.
D	Pages	Shows the available pages for the selected portal menu.
E	Sections	Shows the available information, status, or settings for the selected portal page.
F	Additional information	Orange text indicates that the text is clickable. This can indicate a hyperlink, can trigger actions, or can display additional information.

Changing your logon password in the SharpV web portal

For security reasons, you might need to change the logon password for the SharpV camera. You can do this in the SharpV web portal.

What you should know

You are required to change the default password when you first log on to the SharpV web portal.

NOTE: If you forget your password, [you can reset it from the logon page](#).

To change your password:

- 1 [Log on to the SharpV web portal](#).
- 2 From the **Configuration** menu, select the **Security** page.
- 3 In the **Access** section, click **Modify password**.
- 4 Enter your old password, then enter and confirm your new password.
- 5 Click **Apply**.

Rebooting cameras from the SharpV web portal

Certain configuration procedures require you to reboot the SharpV camera. You can do this from the SharpV web portal.

To reboot the SharpV:

- 1 [Log on to the SharpV web portal.](#)
- 2 From the **Configuration** menu, select the **Maintenance** page.
- 3 Click the **Reboot unit** button.
The connection to the SharpV web portal is momentarily lost.
- 4 Wait approximately 2 minutes to allow the SharpV web portal to restart.

Importing and exporting settings in the SharpV web portal

You can export SharpV settings for use as diagnostic information if required by Genetec™ technical support. You can also use the exported settings file to restore the configuration of the SharpV unit or to copy the configuration to another unit.

What you should know

When you import settings to a SharpV, the password to for the web portal is not affected.

WARNING: When you import settings to a SharpV, the camera's current configuration is lost.

To export SharpV settings:

- 1 [Log on to the SharpV web portal](#) of the SharpV that you want to export settings from.
- 2 From the **Configuration** menu, select the **Maintenance** page.
- 3 From the **Settings** section, click **Export settings**.
The system prepares the files and displays the message "Download succeeded".
- 4 Save the diagnostics zip file to a location that is accessible to the browser that is used to view the portal and to the Windows user that will be importing the file. The file is named with the date and time the file was created, for example, `Diagnostics-2016-10-25_12_49_36`.

To import SharpV settings:

- 1 [Log on to the SharpV web portal](#) of the SharpV that you want to import settings to.
- 2 From the **Configuration** menu, select the **Maintenance** page.
- 3 From the **Settings** section, click **Import settings**.
- 4 Enter the path and filename, or browse to the ZIP file with the SharpV settings you want to import and click **Yes, import**.
- 5 Follow the on-screen instructions and import the settings to the camera.

Synchronizing the SharpV clock

You can configure the SharpV camera to synchronize time and date settings with the computer you are using to access the SharpV web portal. Alternatively, you can synchronize the date and time with an NTP server or with the Security Center server.

What you should know

- The SharpV unit automatically synchronizes clocks with its server whenever the Plate Reader service is restarted, unless the **No synchronization** option is selected.
- If you select **Synchronize with client browser now**, the camera performs a one-time synchronization with the date and time of the client browser.
- If you select **No synchronization**, the camera keeps its internal time indefinitely.
- If you select **NTP server**, the date and time update according to your selection every hour.

To synchronize the SharpV clock:

- 1 [Log on to the SharpV web portal](#).
- 2 From the *Configuration* menu, select the **Date and time** page.
- 3 Select one of the following options:

- **No synchronization:** The camera does not synchronize with any server.

If you select **Synchronize with client browser now**, the camera performs a one-time synchronization with the date and time of the client browser.

IMPORTANT: Do not synchronize the SharpV clock with the client browser unless you are connecting to the SharpV web portal from the server (computer hosting the LPR Manager role). If you synchronize clocks with a computer other than the server, the camera's reads and hits might not have accurate timestamps.

- **NTP server:** The camera synchronizes with an NTP server. Typically, the NTP server is either a foreign computer or a server within your organization that synchronizes itself with an external NTP server. The latter is recommended if synchronization is crucial to your organization. Click **Server** and enter the URL of the machine running the NTP server. Clicking **Test connection** tests the connection between the camera and the NTP server. The camera synchronizes with the NTP server every hour.
- **Active extension:** If you select **Active extension (Security Center)**, the camera's date and time are synchronized with the Security Center server that the camera is connected to. The camera synchronizes with the **Security Center** server upon connection, then again every 24 hours.

NOTE: If you have not yet configured the active extension (see [Configuring where the SharpV sends its LPR data](#) on page 41), you can select **Active extension (none)**, and it will be updated when you configure the extension.

NOTE: The **Active extension** option displays whichever extension is currently selected for the camera in *Configuration > Extensions*, however, selecting this option has no effect if you are using an extension type other than **Security Center** (not valid for FTP, HTTP, and so on).

- 4 Click **Save**.

Configuration

This section includes the following topics:

- ["Security configuration in SharpV Portal" on page 13](#)
- ["Encrypting connection to the SharpV using a self-signed certificate" on page 14](#)
- ["Encrypting connection to the SharpV using a signed certificate" on page 17](#)
- ["Configuring SharpV network settings" on page 19](#)
- ["Viewing the camera feeds from a SharpV camera" on page 20](#)
- ["Calibrating the SharpV zoom and focus" on page 21](#)
- ["About SharpV exposure adjustment for indoor installations" on page 25](#)
- ["About SharpV exposure adjustment for outdoor installations" on page 27](#)
- ["Configuring SharpV analytics" on page 31](#)
- ["Configuring where the SharpV sends its LPR data" on page 41](#)
- ["Configuring the SharpV FTP extension" on page 45](#)
- ["Configuring the SharpV HTTP extension" on page 47](#)
- ["Configuring Syslog for SharpV log files" on page 50](#)

Security configuration in SharpV Portal

The first time you connect to the SharpV web portal, it is over a non-encrypted HTTP connection, which means that anyone on the network can intercept the data transmitted (including the password).

It is always recommended that you use the HTTPS protocol to log on to the SharpV web portal. This is especially important if you are on a public network. Using HTTPS ensures that logon credentials and the data transmission (except for video feeds) are encrypted.

After you connect to the SharpV web portal, you can configure it to accept logons with SSL encryption (HTTPS), using an SSL certificate. You can either generate a self-signed SSL certificate for the SharpV using the tools provided in the portal, or use a signed certificate from a Certificate Authority such as VeriSign.

Related Topics

[Encrypting connection to the SharpV using a self-signed certificate](#) on page 14

[Encrypting connection to the SharpV using a signed certificate](#) on page 17

Encrypting connection to the SharpV using a self-signed certificate

You can secure the SharpV web portal by configuring it using HTTP Secure (HTTPS) using a self-signed SharpV certificate.

Before you begin

- Read about why the connection to the Sharp Portal [should be encrypted](#).
- **IMPORTANT:** If your Security Center version is 5.3 SR3 or higher, if you want to add the SharpV unit to the Archiver using HTTPS, you must modify the Archiver's HTTPS options using the instructions in the Knowledge Base article [KBA01405](#).
- If you are adding the SharpV to the Archiver using HTTPS, [configure the camera's network configuration](#) to use a static IP address before you install a certificate.

What you should know

- The first time you log on to the SharpV web portal, the system logs you on using HTTP mode (no certificate). Your organization's security policy might require that you configure either a self-signed certificate or a signed certificate from a trusted certificate authority.
- You must install the certificate on all machines that communicate with the SharpV camera, which includes the LPR Manager, the Archiver, and all machines that connect to the web portal
- You can install multiple certificates and then select a specific certificate to activate.
- For more information on installing certificates that are signed by a trusted authority, see [Encrypting connection to the SharpV using a signed certificate](#) on page 17.


To encrypt connection to the SharpV web portal using a self-signed certificate:

- 1 [Log on to the SharpV web portal](#) as an Administrator.
- 2 From the **Configuration** menu, select the **Security** page.
- 3 From the **Certificate** section, select + **Self-signed**.
- 4 Enter the required information for the certificate and click **OK**.
You must enter a two-letter **Country** code, the **Server name**, and you must define the **Validity (in years)**. The other fields are optional.

NOTE: If you are also using the certificate to connect to the Archiver, the **Server name** defined in the certificate must be the SharpV IP address, not the SharpV name.

The message *Operation succeeded* is displayed and the signing request is added to the certificate list.

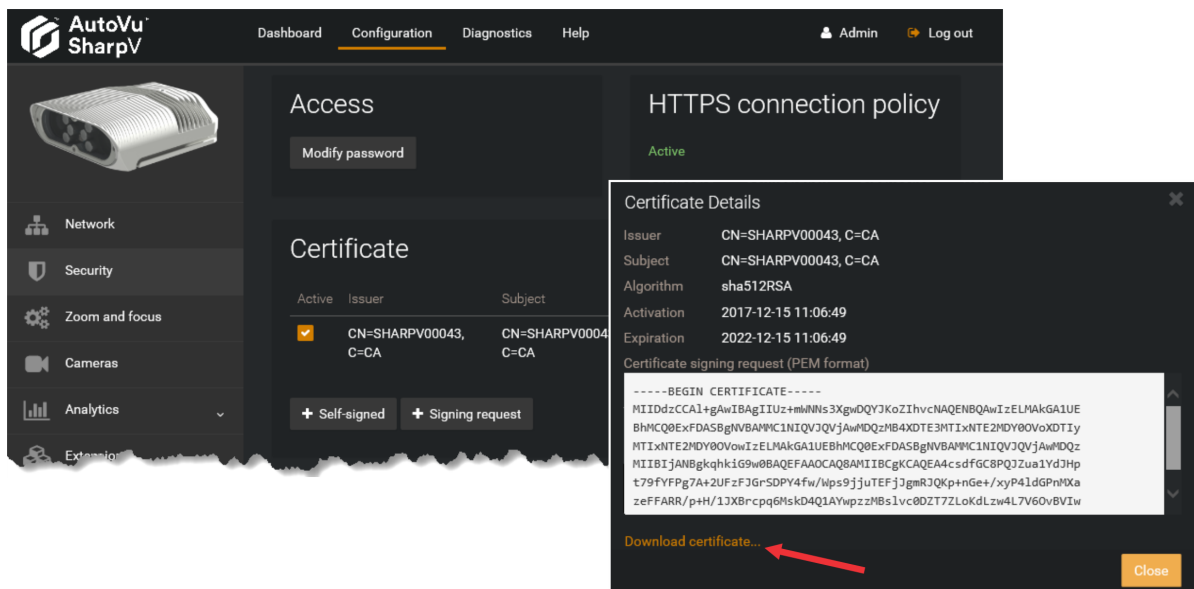
- 5 Select the **Active** check box for the certificate.
- 6 Click **Save and reboot** and click **OK** to confirm the reboot.

When the you log in to the SharpV, the *HTTPS connection policy* on the *Security* page displays *Active*. A lock icon () in the browser's address bar indicates that you are now logged on to the SharpV with a secure connection.

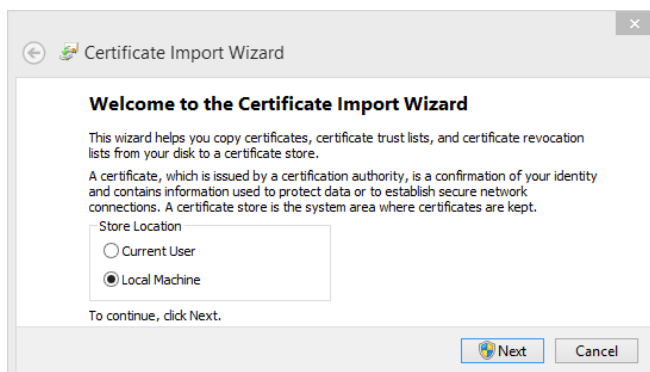
NOTE: Depending on the browser you are using, you might receive warnings because the certificate is not signed by a trusted certificate authority.

To install the certificate on a workstation:

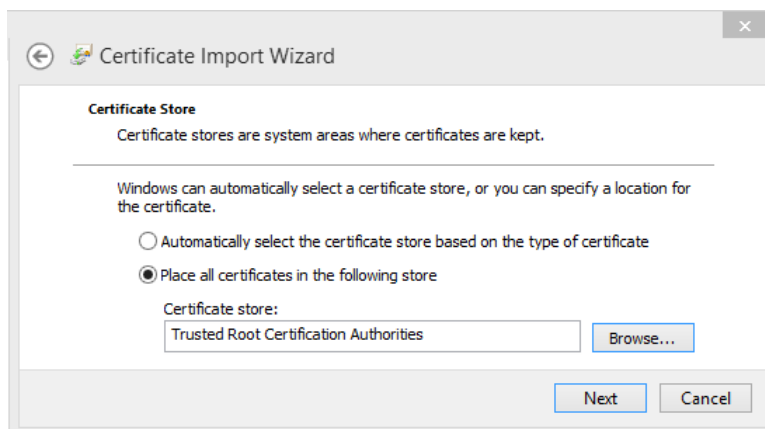
- 1 Click on the certificate to display the *Certificate details*.
- 2 Click **Download certificate** and save the certificate file as prompted by your browser.



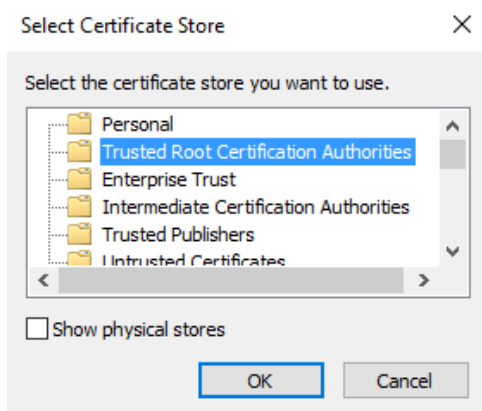
- 3 Double-click the *certificate.cer* file and click **Install Certificate**.
- 4 The *Certificate Import Wizard* prompts you to select a store location. Select **Local Machine** and click **Next**.



- 5 The wizard prompts you to select the certificate store you want to use. Select **Place all certificates in the following store** and click **Browse**.



- 6 From the **Select Certificate Store** window, select **Trusted root certification Authorities** and click **OK**.




- 7 Click **Next** to continue, and click **Finish** to close the *Certificate Import Wizard*.

The system displays the message "The import was successful."

If you see a warning indicating that there is a problem with the website's security certificate, note that for the certificate to be properly registered, you must be logged on as an Administrator on the machine where you want to register the certificate.

- 8 Log on to the SharpV web portal. You are automatically logged on in HTTPS mode.

A lock icon () in the browser's address bar indicates that you are now logged on to the SharpV with a secure connection.

After you finish

As a best practice, [change your password](#) after configuring the SharpV for HTTPS communication.

Encrypting connection to the SharpV using a signed certificate

You can secure the SharpV web portal connection by configuring the camera in secure HTTP mode (HTTPS) using a certificate that has been signed by a trusted certificate authority.

Before you begin

- Read about why the connection to the SharpV web portal [should be encrypted](#).
- **IMPORTANT:** If your Security Center version is 5.3 SR3 or higher, if you want to add the SharpV to the Archiver using HTTPS, you must modify the Archiver's HTTPS options using the instructions in the Knowledge Base article [KBA01405](#).
- If you are adding the SharpV to the Archiver using HTTPS, [configure the camera's network configuration](#) to use a static IP address before you install a certificate.

What you should know

- The first time you log on to the SharpV web portal, the system logs you on using HTTP mode (no certificate). Your organization's security policy might require that you configure either a self-signed certificate or a signed certificate from a trusted certificate authority.
- You must install the certificate on all machines that communicate with the SharpV camera, which includes the LPR Manager, the Archiver, and all machines that connect to the web portal
- You can install multiple certificates and then select a certificate to activate.

IMPORTANT: If the current certificate is a signed certificate, deleting the certificate signing request prevents the certificate from being reinstalled.

To encrypt the connection to the SharpV web portal using a signed certificate:

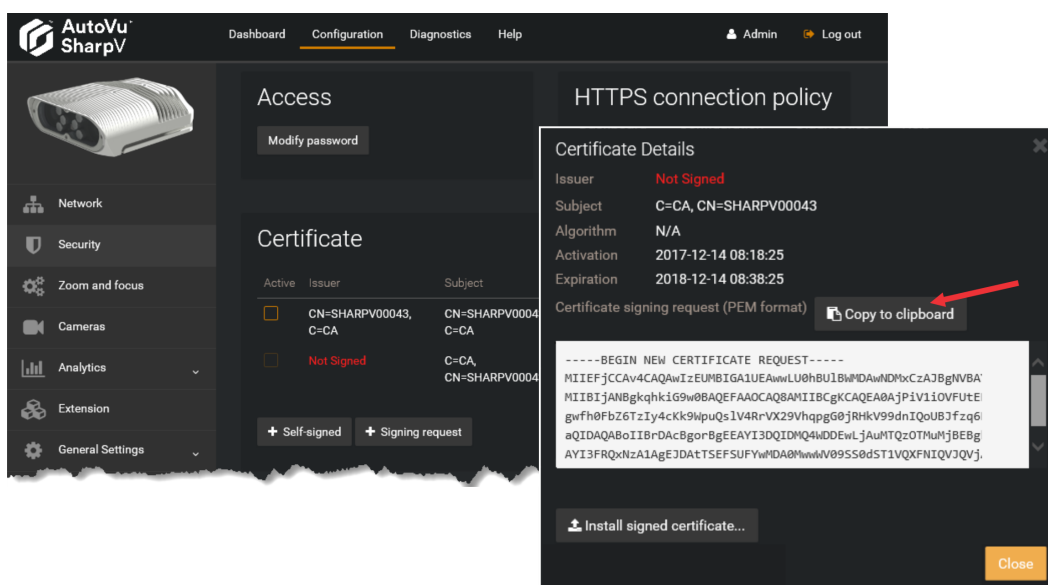
- 1 [Log on to the SharpV web portal](#) as an Administrator.
- 2 From the **Configuration** menu, select the **Security** page.
- 3 Click + **Signing request**.
- 4 Enter the required information for the certificate signing request and click **OK**.

NOTE:

- The "Country" field requires a two-letter country code.
- If you are also using the certificate to connect to the Archiver, the **Server name** defined in the certificate must be the SharpV IP address, not the SharpV name.

The message *Operation succeeded* is displayed and the signing request is added to the certificate list with *not signed* displayed for the **Issuer**.

- 5 Click on the certificate to display the *Certificate details*.
- 6 Click **Copy to clipboard**.



- 7 Send the certificate signing request to a certificate authority.

IMPORTANT: Do not delete the signing request if it has been used to request a certificate.

You will receive an SSL certificate signed by the certificate authority.


- 8 In the *Certificate Details* window, click **Install signed certificate** then browse to the certificate location and click **Open**.
- 9 Click **Save**.

The system displays the message "Installed signed certificate... successful".

- 10 Refresh the browser (F5).

The certificate is displayed in the *Certificate* list.

- 11 Select the Active check box for the certificate and click **Save and Reboot**.

When the system comes back online, notice that the URL displays that you are in HTTPS mode. A lock icon () in the browser's address bar indicates that you are now logged on to the SharpV with a secure connection.

After you finish

As a best practice, [change your password](#) after configuring the SharpV for HTTPS communication.

Configuring SharpV network settings

You can configure the SharpV to use Dynamic Host Configuration Protocol (DHCP) or a static IP address.

What you should know

DHCP is used by default if no option is selected on the Network page of the SharpV web portal.

To configure the SharpV's network settings:

- 1 [Log on to the SharpV web portal.](#)
- 2 From the **Configuration** menu, select the **Network** page.
- 3 Select one of the following:
 - **Use DHCP:** This is the default mode for SharpV cameras. Select DHCP if you are connecting the SharpV to a DHCP server, which assigns the required IP address. When you are on a DHCP server with DNS capability, you can connect to the SharpV using the SharpV name (for example, SharpV12345) rather than the IP address (for example, 192.186.10.100).
 - **Use static IP address:** Select this option to use a static address for the SharpV.

IMPORTANT: You must use a static IP address if you want to stream video to the Security Center Archiver role.
- 4 If you selected **Use static IP address** configure the following:
 - **IP address:** Type the new IP address you want to assign to the SharpV. 10.0.0.1 is the default.
 - **Subnet mask:** Type the new **Subnet mask** if applicable. 255.255.0.0 is the default.
 - **Gateway:** Type the new **Gateway** if applicable. 10.0.0.0 is the default.
 - **DNS:** Type the new **DNS** if applicable. 10.0.0.0 is the default.
- 5 Click **Save**.

Connecting to a SharpV camera using the fallback IP address

If you cannot connect to a SharpV camera on your network, you can try connecting to the camera by using the camera's fallback IP address.

What you should know

- You may need to connect to the camera using the fallback IP address if, for example, the DHCP server is not available.
- If the camera is powered up and is not connected to the network for a few minutes, the fallback IP address will be available.
- The fallback IP address is only available if the camera is in DHCP mode.

To connect to a camera using the fallback IP address:

- 1 If there is more than one Sharp camera on the network, isolate the camera by connecting it directly to a computer with the use of a PoE+ injector.
- 2 Connect to the camera using the fallback IP address (192.168.10.100).
- 3 Reconfigure the camera as required and reconnect to the network.

Viewing the camera feeds from a SharpV camera

Use the **Camera feeds** page to test if your SharpV camera units are working.

To view the camera feeds from a SharpV:

- 1 [Log on to the SharpV web portal](#) as an Administrator.
- 2 From the **Dashboard** menu, select the **Camera feeds** page.
- 3 From the **Camera** drop-down list, select a camera group to view its live feeds.

After you finish

To reduce network bandwidth, after you have finished viewing the camera feeds, select **No camera** from the **Camera** drop-down list, or close the browser.

Calibrating the SharpV zoom and focus

To ensure that the SharpV reads license plates clearly and that the plate characters appear in an acceptable size, you must adjust the zoom and focus of your SharpV camera.

Before you begin

- Read about [optimal reading distance for plate reads](#) for the SharpV.
- Install a stationary license plate to adjust the SharpV camera's zoom and focus. If this necessitates closing a lane of traffic, observe all local regulations. Alternatively, you can adjust the zoom and focus by pointing the camera to the side of the street and placing the stationary plate at the expected distance for plate reads. When the camera is pointed back to the traffic lane, you must evaluate plate read images to adjust the focus.

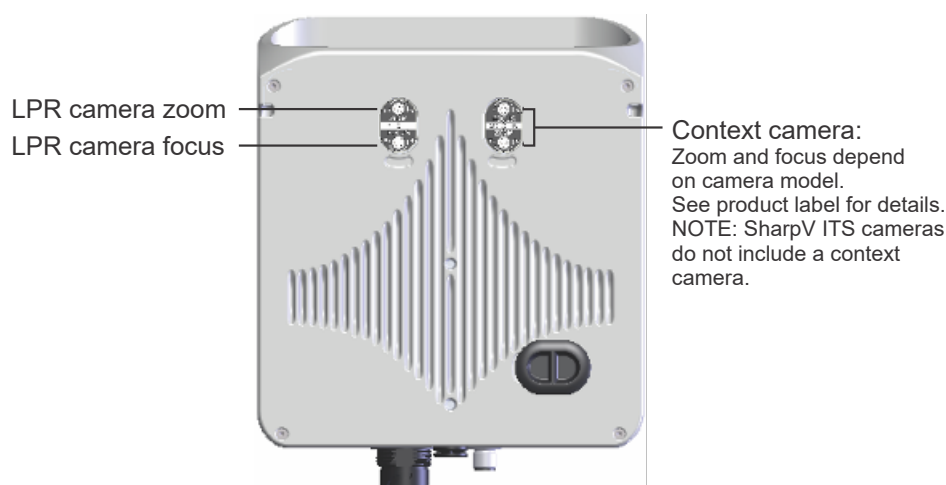
What you should know

- In the images acquired by the LPR camera, the optimal size of license plate characters is 30 pixels high. The system captures accurate plate reads if characters are between 25 and 60 pixels high.
- The position of the zoom and focus adjustment screws on the context camera might be reversed depending on whether you are installing the SharpV SR (Standard-Range) or LR (Long-Range). Refer to the product sticker on the camera for specific adjustment screw information.

NOTE: Information on context cameras is not applicable to SharpV ITS cameras.

Zoom and focus adjustment screws

The SharpV includes zoom and focus adjustment screws for the LPR camera and the context camera. You can access the adjustment screws by removing the rubber plugs on the bottom of the camera. A hex key is provided for making the adjustments.



The following information appears on the zoom / focus adjustment label:

Label	Description
Zoom: T/W	Telephoto/wide
Focus: F/N	Far/near

Label	Description
LPR / CTX	LPR camera/context camera
SR / LR	Standard range/long range

To adjust the zoom and focus of the LPR camera:

- 1 Open the SharpV web portal at <http://<Sharp name or IP address>> or <https://<Sharp name or IP address>>, if you have installed a certificate.
By default, the SharpV is configured to use DHCP. If no DHCP server is available on the network, you can use the IP address 192.168.10.100 to access the SharpV.
- 2 If this is the first time you are logging on the portal, you are prompted to change the password for security reasons. For more information, see [Logging on to the SharpV web portal](#) on page 5.

NOTE: If you forget your password, [you can reset it from the logon page](#).

- 3 Click **Configuration > Zoom and focus**.
- 4 From the **Select your camera** drop-down list, select the **LPR Camera**.
The live feed of the LPR camera is displayed.
- 5 Adjust the exposure as required for the best plate image.

NOTE: The SharpV camera only uses the exposure setting that are visible in the *Zoom and Focus* page during the adjustment process. After the camera has been adjusted, this setting is ignored and the camera returns to the configured exposition settings.

- 6 Adjust the camera's zoom level.
 - a) Select **Show ruler**. A ruler is displayed on the LPR camera image. Drag the ruler so that it appears next to the license plate.
 - b) Enter a new pixel (px) value to change the size of the ruler on the page to match the height of the license plate characters.
 - c) Adjust the zoom and alignment so that the image has the largest field of view and the longest plate transit time, while keeping the height of the plate characters in the image between 25 - 60 pixels. The optimal performance is 30 pixels.

TIP: Click on the license plate to use digital zoom. There are three zoom levels: 1:1, 2:1, and 4:1. A preview of the zoomed area is displayed in the top right corner of the image.

NOTE: When you change the camera's zoom level, the focus is lost. You need to perform a basic focus adjustment each time you change the zoom level so that you have a relatively clear view of the license plate.



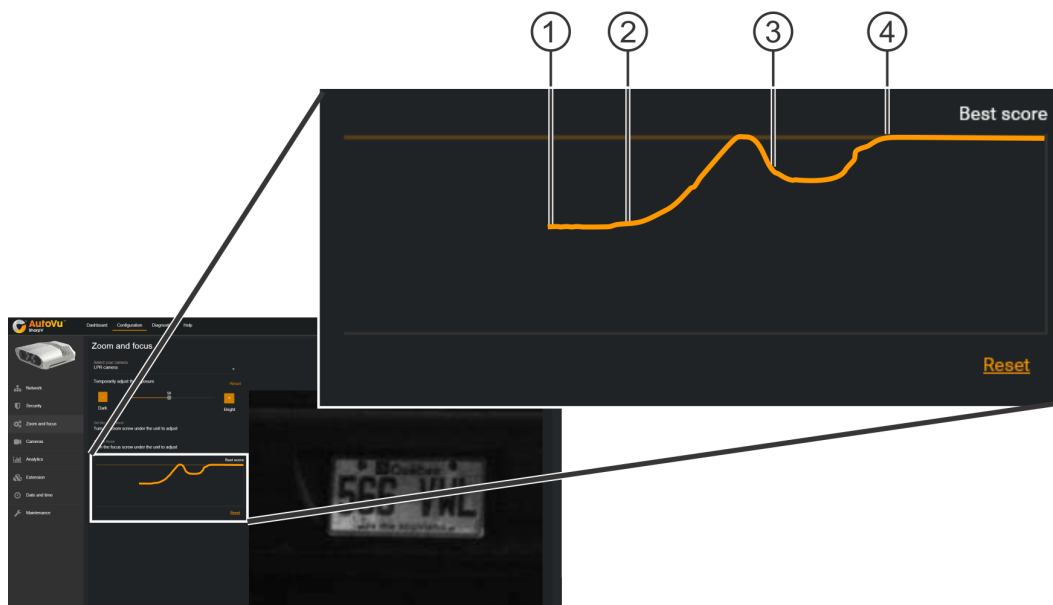
7 Adjust the camera focus.

- Focus the camera on a stationary plate located at the mid-point of the vehicle's expected trajectory.
- Click the image to digitally zoom in on the plate.

NOTE:

- Use the **Best score** graph to visually monitor when the optimal setting is reached for the focus while you are adjusting the screws on the bottom of the SharpV, two orange lines are displayed. The 'bold' orange line indicates the current focus value. The 'dim' orange line indicates the best focus that has been achieved since the graph was last reset.
- For best results, make sure that there is no movement in the camera's field of view when using the **Best score** graph.

Example:



- c) Click **Reset** to start the focus adjustment (1).
- d) Start turning the focus adjustment screw for the LPR camera (2). For this example, the screw is being turned clockwise.
Both the bold and dim orange lines move higher on the graph and are intersecting.
- e) At a certain point, the bold line starts to move lower on the graph and the lines are no longer intersecting (3). At this point you have exceeded the best focus.
It is important to note that the dim orange line now displays the best focus point.
- f) Start turning the adjustment screw in the opposite direction (for this example, counter-clockwise).
- g) When the bold line reaches the level of the dim line (4), the focus adjustment is completed. Click **Done**.

To adjust the zoom and focus of the context camera:

Adjust the context camera using the same method described for the LPR camera, with the following exceptions:

- You can focus the camera's context image based on the image's sharpness, but you can also use the graph tool to help you fine-tune the focus.
- The pixel height of the license plate characters is not important when adjusting the context camera. You must only ensure that the vehicle is clear and recognizable in the image.
- If you need to adjust the zoom and focus of the context camera in low light conditions, enable the IR illuminator. To enable the IR illuminator, click **Configuration > Zoom and focus > Enable flash**. The IR illuminator enables you to see the image more clearly; however, the video feed from the context camera is converted to a black and white image.
- If you adjust the zoom and focus of the context camera in very bright conditions (sunlight), you might need to use very low level on the exposure level slider. At very low levels, the camera iris aperture is reduced. If the focus is adjusted in this position, the result might not be optimal because focus quality can degrade in lower light conditions. The web portal displays a warning to indicate when such conditions exist. To achieve the best possible focus quality, you should not adjust the focus in very bright sunlight.

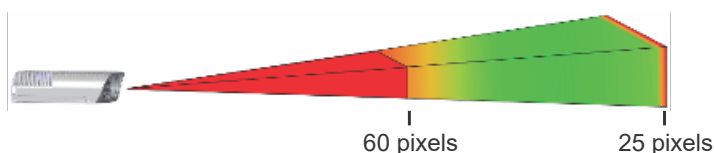
NOTE: Information on context cameras is not applicable to SharpV ITS cameras.

- 8 Click **Done**.

Plate read distances for SharpV lenses

The maximum plate reading distance and field of view that SharpV cameras can support depend on the lens type and zoom setting of the camera.

For optimal performance, respect the following installation distances for standard and long-range SharpV cameras.



Lens type	Zoom level	60 pixels (maximum)	25 pixels (minimum)
Standard lens	Reading distance	2.75 m (9 ft)	18.25 m (60 ft)
Long-range lens	Reading distance	18.25 m (60 ft)	35 m (115 ft)

About SharpV exposure adjustment for indoor installations

By default, the SharpV is configured to automatically adjust exposure settings for changing light conditions when capturing license plate reads. Alternatively, if you are installing a SharpV camera indoors, for example, in an underground parking lot, you can define fixed values for the camera's iris, shutter time, and gain settings. Doing this can result in more consistent exposure for LPR and context images.

IMPORTANT: Modifying the SharpV exposure settings can greatly impact LPR performance. Vanity plates, or plates that are damaged or dirty can have different reflective properties. Improving the exposure using a stationary test plate can result in reduced LPR performance on every-day traffic which includes plates with a wide range of reflective properties. You must test the system after modifying these settings.

Setting custom SharpV LPR camera exposure levels for indoor installations

If the default exposure settings do not produce acceptable results, you can adjust the iris, shutter time, and gain settings of the SharpV LPR camera to work best with your indoor installation.

Before you begin

- Ensure that the lighting conditions match what is expected during normal camera operation.
- [Adjust the zoom and focus](#) of the camera.

What you should know

- In a correctly-exposed license plate image, the characters and the plate state are dark and well-defined, and the background is white or very bright.



- In the LPR image, it is normal that the surroundings of the plate are under-exposed while the plate itself is correctly-exposed. In the LPR image, make sure that the plate is correctly exposed and ignore the quality of the surroundings.

To adjust the LPR camera exposure settings:

- 1 [Log on to the SharpV web portal](#).
- 2 From the **Configuration** menu, select the **Zoom and focus** page.
- 3 From the **Select your camera** drop-down list, select the **LPR Camera**.
The live feed of the LPR camera is displayed.
- 4 Select the **Show ruler** check box.
- 5 Place a stationary license plate in front of the camera so that the character height is 25 pixels.

IMPORTANT: Do not modify the focus. The license plate might appear out of focus, but you are only adjusting the exposure in these steps.

- 6 From the **Configuration** menu, select the **Cameras** page.
- 7 From the **Select your camera** drop-down list, select the **LPR camera**.
The live feed from the LPR camera is displayed.
- 8 From the **Exposure** drop-down list, select **Fixed (indoor)**.
Gain, Exposure time and Iris settings are displayed.

- 9 Clear the **Iris** check box.
- 10 Open the iris to 100% by moving the slider to the right.
- 11 Set the **Gain** level to the minimum default value (0).
- 12 Adjust the **Exposure time** to be as high as possible without resulting in an over-exposed image.
- 13 If you reach the maximum **Exposure time** level and the plate image is still too dark, increase the **Gain** level and adjust the **Exposure time** until you are satisfied with the plate image.
TIP: Increasing the gain level introduces noise in the image. Keep the gain as low as possible.
- 14 When you are satisfied with the appearance of the plate images in the video feed window, click **Save**.
The system displays the message: *Configuration saved successfully*.

Setting custom SharpV context camera exposure levels for indoor installations

If the default exposure settings do not produce acceptable results, you can adjust the shutter time, and gain settings of the SharpV context camera to work best with your indoor installation.

Before you begin

- Ensure that the lighting conditions match what is expected during normal camera operation.
- [Adjust the zoom and focus](#) of the camera.

What you should know

- Adjusting the exposure settings of the context camera has no impact on LPR performance. Performing this procedure simply improves the quality of the context image.
- If you configure a long exposure time, you might notice motion blur in the context image. This is not apparent when using a fixed license plate for calibration, and might require adjustment after testing the camera in normal operation.
- Information on context images is not applicable to SharpV ITS cameras.

To adjust the context camera exposure settings:

- 1 [Log on to the SharpV web portal](#).
- 2 From the **Configuration** menu, select the **Cameras** page.
- 3 From the **Select your camera** drop-down list, select the **Context camera**.
The live feed from the context camera is displayed.
- 4 From the **Lighting type** drop-down list, select the setting that best describes the installation's normal lighting conditions.
- 5 From the **Exposure** drop-down list, select **Fixed (indoor)**.
Gain and **Exposure time** settings are displayed.
- 6 Set the **Gain** level to the minimum default value (0).
- 7 Adjust the **Exposure time** until you are satisfied with the image and license plates are clearly visible.
- 8 If you reach the maximum **Exposure time** level and the plate image is still too dark, increase the **Gain** level.
NOTE: If, due to poor lighting, the plate image is still not visible even after increasing the gain level, or if increasing the gain level adds too much noise to the image, you can select **Enable illuminator** to turn on the camera's IR illuminator. The IR illuminator makes the plate more visible, but removes color from the context image.
- 9 When you are satisfied with the appearance of the plate images in the video feed window, click **Save**.
The system displays the message *Configuration saved successfully*.

About SharpV exposure adjustment for outdoor installations

For SharpV cameras that are installed outdoors, we recommend that you keep the default exposure settings. If you notice that license plates are often under-exposed (too dark) or over-exposed (too bright), you can adjust the exposure settings. However, there are many factors to consider in order to account for changing lighting conditions.

IMPORTANT: Modifying the SharpV exposure settings can greatly impact LPR performance. Vanity plates, or plates that are damaged or dirty can have different reflective properties. Improving the exposure using a stationary test plate can result in reduced LPR performance on every-day traffic which includes plates with a wide range of reflective properties. You must test the system after modifying these settings.

Setting custom SharpV LPR camera exposure levels for outdoor installations

If the default exposure settings do not produce acceptable results, you can adjust the iris, shutter time, and gain settings of the SharpV LPR camera to work best with your outdoor installation.

Before you begin

- Ensure that the lighting conditions match what is expected during normal camera operation.
- [Adjust the zoom and focus](#) of the camera.

What you should know

- In a correctly-exposed license plate image, the characters and the plate state are dark and well-defined, and the background is white or very bright.



- In the LPR image, it is normal that the surroundings of the plate are under-exposed while the plate itself is correctly-exposed. In the LPR image, make sure that the plate is correctly exposed and ignore the quality of the surroundings.
- The ranges for the **Exposure time** and **Gain** settings must be large enough to allow good quality images in all lighting conditions, but you should reduce the range as much as possible. If the range is too large, it increases the risk of over-exposure or under-exposure. It is normal that the SharpV constantly varies the exposure of the LPR camera in order to get a correct exposure of a plate.
- Modifying settings to improve read performance at night can have a negative impact on read performance during the day, and vice versa. Therefore, you must test the settings both at night and during the day (under sun illumination).
- If the SharpV is expected to read both embossed and flat license plates, perform the day instructions with the flat plate and the night instructions with the embossed plate.

Adjust the LPR camera under sun illumination:

- 1 Place a stationary license plate as close to the camera as possible while still being within range for the camera to capture plate reads.
- 2 [Log on to the SharpV web portal](#).

- 3 From the **Configuration** menu, select the **Cameras** page.
- 4 From the **Select your camera** drop-down list, select the **LPR camera**.
The live feed from the LPR camera is displayed. Do not modify the focus. The license plate might appear out of focus, but you are only adjusting the exposure in these steps.
- 5 From the **Exposure** drop-down list, select **Range (outdoor)**.
Gain, Exposure time and **Iris** settings are displayed.
- 6 Set the **Gain** and **Exposure time** minimum and maximum levels to their minimum values.
- 7 Clear the **Iris** check box.
- 8 Move the **Iris** slider towards the right as much as possible without over-exposing image.
- 9 When you are satisfied with the appearance of the plate images in the video feed window, click **Save**.
The system displays the message *Configuration saved successfully*.

Adjust the LPR camera at night:

- 1 Place a stationary license plate as far from the camera as possible while still being within range for the camera to capture plate reads.
- 2 [Log on to the SharpV web portal](#).
- 3 From the **Configuration** menu, select the **Cameras** page.
- 4 From the **Select your camera** drop-down list, select the **LPR camera**.
The live feed from the LPR camera is displayed. Do not modify the focus. The license plate might appear out of focus, but you are only adjusting the exposure in these steps.
- 5 From the **Exposure** drop-down list, select **Range (outdoor)**.
Gain, Exposure time and **Iris** settings are displayed.
- 6 Increase the **Exposure Time** maximum as much as possible without getting an over-exposed image.
- 7 If the **Exposure Time** is set at the maximum value and the image is still dark, increase the **Gain** maximum until you are satisfied with the image.
- 8 When you are satisfied with the appearance of the plate images in the video feed window, click **Save**.
The system displays the message *Configuration saved successfully*.

Troubleshooting outdoor exposure issues for the SharpV LPR camera

You can resolve exposure adjustment issues that result in under-exposed or over-exposed license plate images in fixed SharpV installations.

If LPR images (or some specific plate models) are always too dark at night:

- 1 Make the first adjustments under sun illumination.
- 2 Set the **Gain** and **Exposure time** minimum and maximum levels to the minimum value.
- 3 Increase the **Iris** value as much as possible without over-exposing the plate.
- 4 Perform the remaining exposure adjustment at night.
- 5 Increase the maximum **Exposure time** value until you are satisfied with the plate images.
- 6 If you reach the maximum **Exposure time** level and the LPR images are still too dark, increase the maximum **Gain** value.

If LPR images are often too dark at night:

In this case, the exposure setting range might be too large, causing exposure to be too low. To reduce the range, start by increasing the minimum values. Because higher minimum values might lead to over-exposure for daytime reads, perform the adjustment during the day.

In this case, the exposure setting range might be too large, causing exposure to be too low. You can reduce the range by increasing the minimum values, but you should do this carefully because increasing the minimum values can cause over-exposure during the day. Therefore, this adjustment should be done during the day.

- 1 Make the adjustment under sun illumination.
- 2 Increase the minimum **Exposure time** value as much as possible without compromising image quality.
- 3 If the minimum **Exposure time** value reaches its maximum value, then you can increase the minimum **Gain** value. Test to make sure image quality is still satisfactory.

If LPR images (or some specific plate models) are always too dark even under sunlight:

- 1 Make the adjustment under sun illumination.
- 2 Increase the **Iris** value as much as possible without over-exposing the plate.
- 3 If the **Iris** reaches its maximum value and the plate is still under-exposed, increase the maximum **Exposure time** level as much as possible without over-exposing the plate.
- 4 If the maximum **Exposure time** reaches its maximum value and the plate is still under-exposed, increase the maximum **Gain** value one step at the time until you are satisfied with the images.

If LPR images (or some specific plate models) are always too bright under sunlight:

- 1 Make the adjustment under sun illumination.
- 2 Decrease the minimum **Gain** value until you are satisfied with the plate images.
- 3 If you reach the minimum **Gain** level and the LPR images are still too bright, decrease the minimum **Exposure time** value.
- 4 If you reach the minimum **Exposure time** level and the LPR images are still too bright, decrease the iris aperture until you are satisfied with the plate images.

If LPR images are often too bright under sunlight:

In this case, the exposure setting range might be too large, causing exposure to be too high. You can reduce the range by decreasing the maximum values, but you should do this carefully because decreasing the maximum values can cause under-exposure at night. Therefore, this adjustment should be done during the night.

- 1 Make the adjustment at night.
- 2 Decrease the maximum **Gain** value as much as possible without compromising image quality.
- 3 If the maximum **Gain** value reaches its minimum value, then you can decrease the maximum **Exposure time** value. Test to make sure image quality is still satisfactory.
- 4 If you reach the minimum **Exposure time** level and you are still not satisfied with the image quality, [perform the complete day and night exposure adjustment](#) again.

Troubleshooting outdoor exposure issues for the SharpV context camera

You can resolve exposure adjustment issues that result in under-exposed or over-exposed license context images in fixed SharpV installations.

If context images are blurry on fast-moving vehicles:

- 1 Make the adjustment at night.
- 2 Decrease the maximum **Exposure time** value until the blur caused by vehicle motion is acceptable.

If context images are noisy during the night:

- 1 Make the adjustment at night.
- 2 (Optional) Select **Enable illuminator**. This allows the camera to turn on the IR illuminator under dark conditions, but removes color from the image as the light level diminishes.
- 3 Decrease the maximum **Gain** value. This prevents the camera from amplifying the noise, but it can result in darker images.

If context images are too dark during the night:

- 1 Make the adjustment at night.
- 2 (Optional) Select **Enable illuminator**. This allows the camera to turn on the IR illuminator under dark conditions, but this progressively removes color from the image as the light level diminishes.
- 3 Increase the maximum **Exposure time** value until you are satisfied with the image quality. However, do not exceed the level that causes unacceptable motion blur on fast-moving vehicles.
- 4 If you reach the maximum **Exposure time** value and the image is still too dark, increase the maximum **Gain** value.

If context images are too bright during the day:

- 1 Make the adjustment under sun illumination.
- 2 Decrease the minimum **Gain** value until you are satisfied with the image quality.
- 3 If you reach the minimum **Gain** value and the image is still too bright, decrease the minimum **Exposure time** value.

Configuring SharpV analytics

You can configure the analytics performed by the SharpV, such as which plates the SharpV will read, and whether the SharpV should attempt to read the plate origin and vehicle make.

To configure SharpV analytics:

- 1 [Log on to the SharpV web portal.](#)
- 2 Click **Configuration > Analytics**.
- 3 From the **Context** drop-down list, select which license plates the SharpV will read.
- 4 From the **Reading mode** drop-down list, select one of the following reading modes:
 - **Continuous:** Select this for plates to be captured continuously. This is the default setting.
 - **Conditional:** Select this to capture plate reads continuously as long as the selected input signal meets the condition defined (high/low).
 - **Single read on trigger:** Select this option to force the SharpV to capture a plate read after a signal is received from an electrical trigger, or after a Security Center event-to-action or hot action. This configuration is useful for controlling vehicle access to gated parking lots. You can configure the plate read capture to occur before or after the trigger is activated.
- 5 (Optional) If you selected **Single read on trigger**, click **Add trigger** and configure the following:
 - a) Under **Trigger**, select when an input (A or B) triggers a plate read based on its state (Low or High). For example, you can specify that **Input A** triggers a plate read when it **transitions to a Low** state. You can also select an **External** input such as a Security Center event-to-action or hot action.
 - b) Under **Capture window**, specify when the SharpV starts capturing (in milliseconds) and whether to do it **before** or **after** the trigger. You also need to specify the **Duration** (in milliseconds) that the SharpV will attempt to capture a plate read.
 - c) Under **If no plates**, indicate how long (in milliseconds) to wait after a trigger before capturing a context image of the vehicle. Select the **Use the LPR image as context image** option, when you want an image from the LPR camera to be used for the *no plate read*.
- 6 From the **Read strategy** list, select a read strategy:
 - **Slow moving vehicle:** Applicable when vehicles are traveling slowly when the license plates are captured. For example, select this option for monitoring parking lot entrances.
 - **Fast moving vehicle:** Applicable when vehicles are traveling at moderate to high speeds when the license plates are captured. For example, select this option for a SharpV overlooking a highway.
 - **Gate control:** Applicable when vehicles must come to a stop when the license plates are captured. For example, select this option for a SharpV that is monitoring a gated parking lot entrance or toll booth.
- 7 Under **Camera orientation**, select the pictograph that describes how the road appears from the camera's perspective. This helps the system to determine the direction that vehicles are traveling.
- 8 Under **Read contents**, select the contents of the plate you would like the SharpV to attempt to read. You can select the following:

NOTE: You can add the state, vehicle make, and confidence score as annotation fields in Security Center to query for this information in Security Desk reports.

- **State:** Select this option if you want the SharpV unit to try to read the license plate origin. For example, the state, province, or country.

NOTE: State recognition is available for certain contexts.

- **Vehicle make:** Select this option if you want the SharpV unit to attempt to read the vehicle's make from the brand or logo. For example, Honda, Toyota, and so on.
- **Confidence score:** Assigns a numerical value (from 0 to 100) to each license plate read. This value indicates how confident the SharpV is in the accuracy of the read.

- 9 Click **Save**.

Calibrating the virtual loop

For parking applications where the license plate capture rate is critical, the SharpV virtual loop feature can detect vehicles with damaged or dirty license plates that are not detected by the SharpV's LPR camera. The plate numbers of these vehicles can then be manually modified in Security Desk.

Before you begin

- Install the SharpV camera in a fixed location.
- [Adjust the zoom and focus](#) of the camera.

IMPORTANT: To use the virtual loop, the zoom level of the LPR and context cameras must be adjusted so that the context camera field of view is more than double the width of the LPR camera field of view.

NOTE: If you move the location of the camera, or if you modify the zoom and focus or the pan and tilt angles of the camera, you must reconfigure and recalibrate the virtual loop detection zone.

What you should know

- For best results when using the virtual loop feature, ensure that the detection area is well illuminated. If there is not enough light for reliable operation, the virtual loop is temporarily disabled until lighting conditions improve.
- To be detected by the virtual loop, at least 25% of the vehicle must pass through the red detection zone and at least 20% of the vehicle must pass through the orange LPR field of view, in any order. The vehicle must also either enter or exit the context camera field of view, depending on the settings you choose.
- You must respect the recommended SharpV positioning guidelines. For more information, see the *SharpV Handbook*.
- For the calibration to finish quickly, choose a time when vehicles are expected to be traveling in the appropriate direction in the designated area.
- The virtual loop feature is not available on SharpV ITS cameras.
- You cannot use the virtual loop as a trigger for gate control.

To configure SharpV virtual loop:

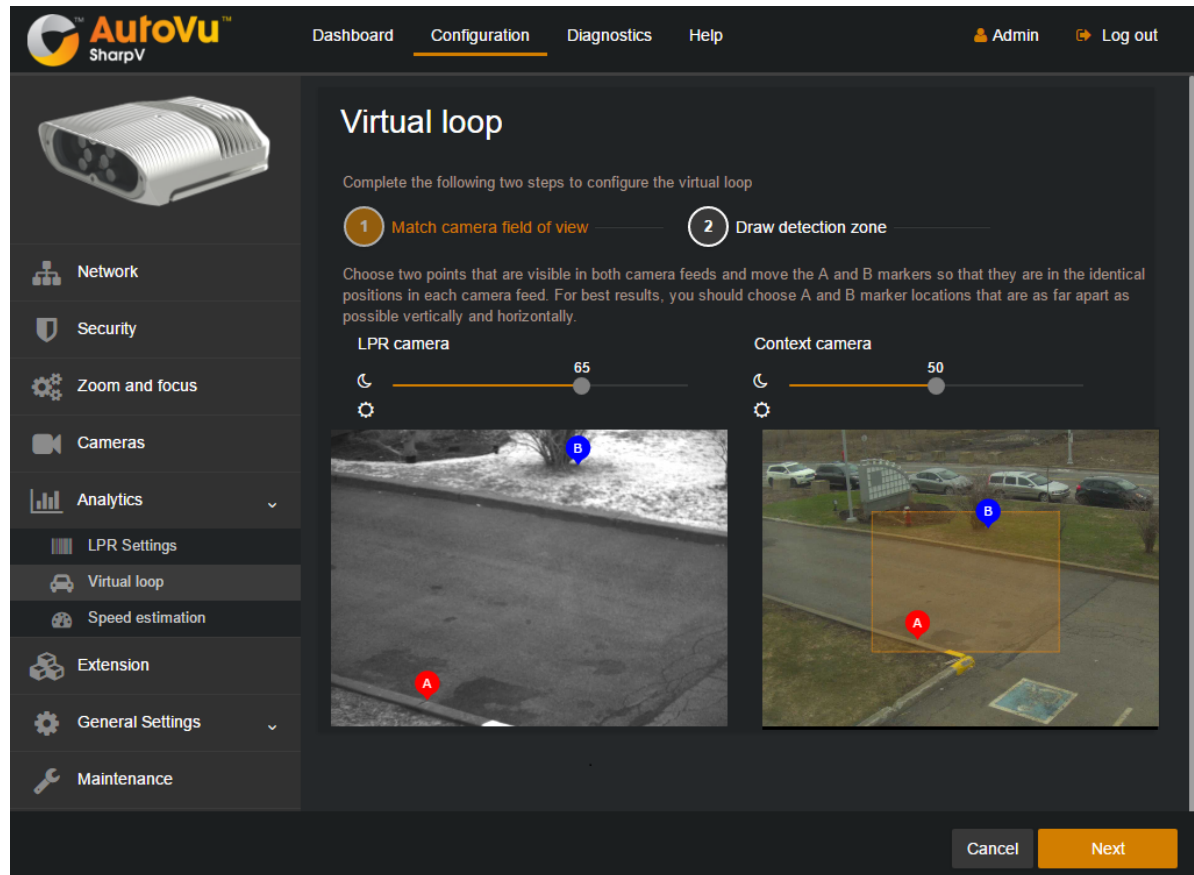
- 1 [Log on to the SharpV web portal](#).
- 2 Click **Configuration** > **Analytics** and select **Virtual loop**.
- 3 Click **Enable**.
The camera saves the configuration and displays the message "Configuration saved successfully".
- 4 Click **Configure**.
The status LED on the SharpV flashes red and green during the configuration.
- 5 Match the markers.
 - a) In the virtual loop configuration page, the video feeds from the LPR camera and context camera are displayed with an *A* and *B* marker for each camera. Choose two points that are visible in both camera feeds and move the *A* and *B* markers so that they are in the identical positions in each camera feed. When the markers are close to the correct position, an orange box appears in the context camera video feed. Fine tune the marker positioning so that the orange box matches the field of view of the LPR camera.

NOTE:

- For best results, choose *A* and *B* marker locations that are as far apart as possible vertically and horizontally.

- If either of the video feeds are too dark or too bright to accurately place the markers, you can temporarily adjust the brightness using the sliders located above each video feed. When the calibration is finished, the exposure returns to its default mode.

b) Click **Next**.



6 Configure a detection zone.

a) To configure the system to detect vehicles that are moving in a specific direction, select one of the following detection modes from the drop-down list:

- Enters the field of view in the detection zone.
- Exits the field of view in the detection zone.
- Enters or exits the field of view in the detection zone.

b) To draw a detection zone in the camera video feed, create a polygon by clicking on at least three points.

NOTE:

- Clicking in the field of view clears any existing polygon. You can also click **Clear the zone** to remove an existing polygon.
- To draw a polygon that covers the entire context camera field of view, click **Select all** and use the *Enters or exits the field of view in the detection zone* setting.

Consider the following when drawing the detection zone:

- The polygon must touch the border of the image. This is necessary for all direction of travel settings, for example, *Enters the field of view in the detection zone*.
- The polygon lines cannot intersect.

- To be detected, at least 25% of the visible part of the vehicle must pass through the red detection zone (if configured) when the vehicle enters or exits the image. The vehicle must also cover at least 20% of the orange LPR field of view somewhere along its trajectory.
- Try to draw your detection zone so that cyclists and pedestrians do not pass through the zone. For example, if you have too many false detections when you draw a polygon far from the camera and use the *Exits the field of view in the detection zone* setting, try drawing a polygon close to the camera and use the *Enters the field of view in the detection zone* setting.

For more information, see [Virtual loop detection zone examples](#) on page 35.

- c) When you have finished drawing the polygon, click **Done**.

The system displays *In progress - Waiting for 5 more vehicles* and counts down the number of license plate reads that are required for calibration to finish. During this calibration, the system evaluates the expected vehicle size and trajectory.

NOTE:

- The system completes the calibration on its own. No further steps are required.
- If, before the calibration ends, you make any other change to the SharpV configuration, the calibration is restarted.

After you finish

- For troubleshooting purposes, virtual loop diagnostic information is available from the **Diagnostics** > **Logs** page. Before calibration, using the *VehicleDetection* source, and after calibration using the *VehicleDetection (verbose)* source (must be enabled from the **Sources to log** drop-down list).
- If the LPR camera fails to capture a vehicle's license plate and the vehicle is then detected by the virtual loop, the license plate event sent by the SharpV uses the string *NOPLATE*. To let the operator know that the license plate needs to be manually modified, you can configure an event-to-action to trigger an alarm, to send a message, or to add a bookmark.

Example: Event-to-action to send a message

The screenshot shows the 'Event-to-action' configuration window. It has a dark theme with a light gray border. The title bar says 'Event-to-action'. Inside, there are several sections:

- When:** A dropdown menu shows 'License plate read' with a small icon to its left. To the right of the dropdown is the word 'occurs'. Below this is a text box containing '[PlateNumber] = "NOPLATE"' with a small 'X' icon to its right.
- From:** A dropdown menu showing 'Any entity'.
- For:** A dropdown menu showing 'Any entity'.
- Action:** A dropdown menu showing 'Send a message' with a small icon to its left.
- Recipient:** A dropdown menu showing 'AutoVu operators' with a small icon to its left.
- Message:** A text box containing 'Manually enter the plate number.'
- Has timeout:** A toggle switch is turned 'ON'. To its right is the text 'automatically close after' followed by a spinner box showing '10' and the word 'seconds'.
- Effective:** A dropdown menu showing 'Always'.

At the bottom right, there are two buttons: 'Cancel' and 'Save'.

Example: Event-to-action to create a bookmark

The screenshot shows the 'Event-to-action' configuration window. It is divided into two main sections: 'When' (trigger) and 'Action' (response).

When (Trigger):

- When:** License plate read (with a license plate icon)
- occurs** (dropdown menu)
- and** (operator)
- [PlateNumber] = "NOPLATE"** (condition with a delete icon)
- From:** SHARPV00014 (Exit - AE) (dropdown menu)
- For:** Any entity (text)

Action (Response):

- Action:** Add bookmark (with a bookmark icon)
- Camera:** SHARPV00014 (Exit - AE) - Camera - 0 (dropdown menu)
- Message:** Manually enter the plate number. (text input)
- Effective:** Always (text)

At the bottom right are 'Cancel' and 'Save' buttons.

Virtual loop detection zone examples

To reduce the number of false detections when using the virtual loop feature in a fixed SharpV installation, you must consider the guidelines for drawing the detection zone.

Virtual loop detection zone guidelines:

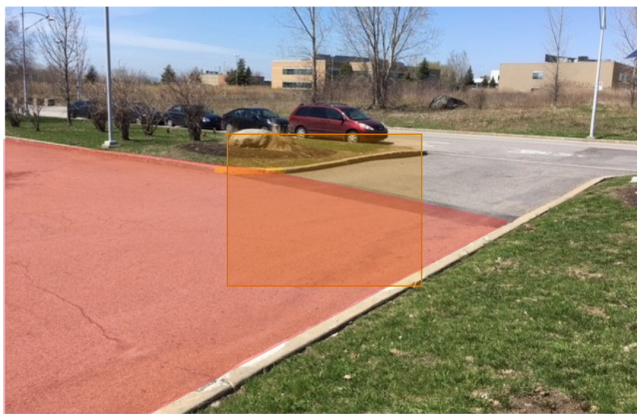
- The polygon must touch the border of the image. This is necessary for all direction of travel settings, for example, *Enters the field of view in the detection zone*.
- The polygon lines cannot intersect.
- To be detected, at least 25% of the visible part of the vehicle must pass through the red detection zone (if configured) when the vehicle enters or exits the image. The vehicle must also cover at least 20% of the orange LPR field of view somewhere along its trajectory.
- Try to draw your detection zone so that cyclists and pedestrians do not pass through the zone. For example, if you have too many false detections when you draw a polygon far from the camera and use the *Exits the field of view in the detection zone* setting, try drawing a polygon close to the camera and use the *Enters the field of view in the detection zone* setting.

Issue: The detection zone does not touch the edge of the field of view

- **Bad:** The detection zone does not touch the edge of the context camera field of view. With this detection zone, no vehicles are detected.



- **Good:** The detection zone touches the edge of the context camera field of view. To detect only vehicles exiting the parking lot, use the *Enters the field of view in the detection zone* setting.



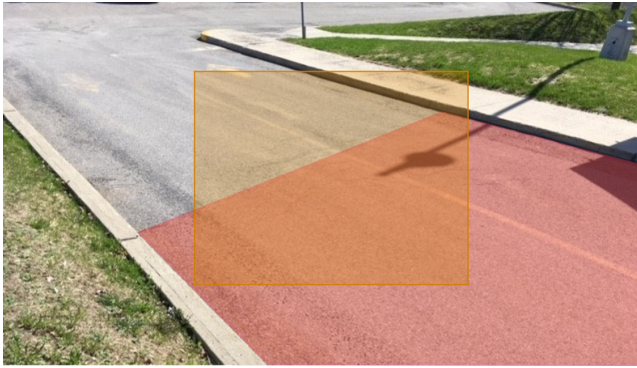
Issue: Vehicles do not leave the field of view

- **Bad:** To be detected, vehicles must exit the context camera field of view. Some of the parking spaces in this parking lot are within the detection zone. As a result, the vehicles in those spaces are not detected.



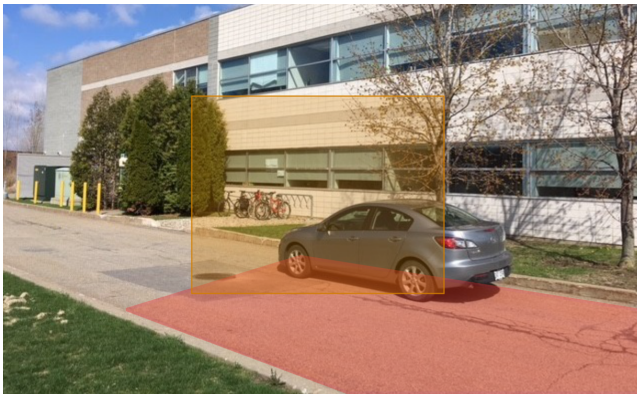
- **Good:** To correct this issue, the camera angle has been lowered (which requires zoom and focus recalibration) and the *Enters the field of view in the detection zone* setting is used.

Alternatively, you could reduce the size of the context camera's field of view so that the vehicles in the parking lot are not visible.

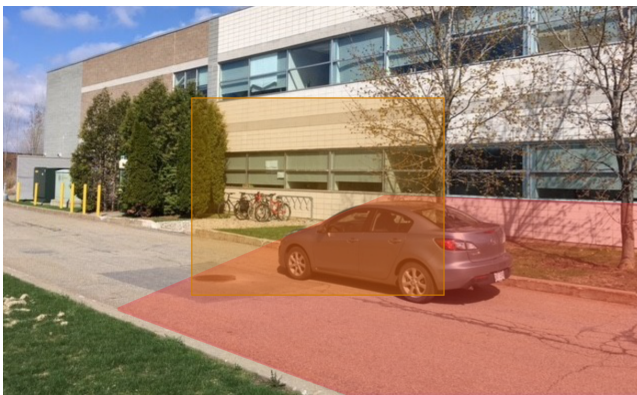


Issue: 25% of the vehicle is not within the detection zone

- **Bad:** In this example, the detection zone is drawn to match the road. Especially when the camera is installed close to the ground, this can mean that vehicles are excluded.



- **Good:** To correct this issue, when drawing the detection zone, consider the path and size of vehicles as they pass through the field of view.



Calibrating speed estimation

For systems that include a fixed SharpV camera, you can configure the camera to include an estimated vehicle speed when performing license plate reads.

Before you begin

- Install the SharpV camera in a fixed location. To use this feature, cameras should be installed higher than the level of the license plates with respect to the road. This means a camera installation height of at least 1.5 m (5 ft). The camera should be pointing downward with respect to the horizontal by at least 5°.
- [Adjust the zoom and focus](#) of the camera.

NOTE: If you modify the zoom and focus or the pan and tilt angles of the camera, you must recalibrate speed estimation.

- [Configure the LPR context](#). Do this so that the speed and measurement units are displayed in the format for your region.

What you should know

- For more accurate speed estimation, vehicles that pass the camera during calibration should travel at a constant speed of at least 30 km/h (20 mph). This recommendation only applies during calibration. In general, the system can estimate speeds for vehicles moving slower than 30 km/h (20 mph).
- **To calibrate speed estimation, the system needs the following, in any order:**
 - At least one license plate read from a calibration vehicle with a known speed. You can do this by driving the calibration vehicle at a specific speed, or by using a radar device to detect the speed of a passing vehicle.
 - 20 additional license plate reads. You do not need to know the speed of these vehicles.

NOTE: For the calibration to finish quickly, choose a time when vehicles are expected to be traveling in the appropriate direction in the designated area. If no traffic is expected to pass during the calibration, you can use one vehicle to make 20 passes in front of the camera, leaving at least 15 seconds between passes.

To configure SharpV speed estimation:

- 1 [Log on to the SharpV web portal](#).
- 2 Click **Configuration** > **Analytics** and select **Speed estimation**.
- 3 Click **Enable**.

The camera saves the configuration and displays the message "Configuration saved successfully".

- 4 Click **Start calibration**.

The system starts to capture license plate reads for calibration and displays *Calibrating....* A counter indicates the number of plate reads remaining to complete the calibration.

If you use a calibration vehicle moving at a specific speed:

- 1 From the main speed estimation screen, click **Edit**.
- 2 Click **Plate number** and enter the license plate of the calibration vehicle.
- 3 Click **Add**.

The system displays the message: *The system is now expecting to read a plate for this vehicle. The vehicle should maintain a constant speed.*

When the system detects the calibration plate, it displays the license plate read with a time stamp.

- 4 Click **Validate**.

Two images of the calibration plate are displayed.

- As shown in the following image, the orange line in each image must follow the bottom of the characters and must be as wide as the license plate. If required, move the end points to correct the line placement.

IMPORTANT: Speed estimation accuracy depends on precise positioning of the end points.

Y25BHT

< Previous Next >

Make sure that the yellow lines follow the bottom of the characters and match the plate width

Speed 30 km/h Width 30 cm Distance from ground to plate cm

Delete Cancel Validate

- Enter the **Speed** at which the vehicle was traveling when it was read by the SharpV camera.
- The **Width** of the plate is entered for you based on the LPR context that you have configured. If necessary, modify the plate width.
- (Optional) For more accuracy, measure the distance from the ground to the bottom of the calibration vehicle's license plate and enter the measurement in the **Distance from ground to plate** field.
- Click **Validate**.

A green check mark is displayed over the calibration plate, indicating that the step is complete.

NOTE: You can add plate numbers for additional calibration vehicles. This is not required, but can increase speed estimation accuracy.

If you use a radar device to detect the speed of a passing vehicle:

- From the main speed estimation screen, click **Edit**.
- Click **Advanced** on the right side of the screen.
The license plates from passing vehicles are displayed.
- Take note of the license plate of a passing vehicle and use your radar device to detect the vehicle's speed.
- Click the license plate image of the vehicle with the known speed.
Two images of the calibration plate are displayed.
- The orange line on each image must follow the bottom of the characters and must be as wide as the license plate. If required, move the end points to correct the line placement.

IMPORTANT: Speed estimation accuracy depends on precise positioning of the end points.

- Enter the **Speed** of the vehicle as detected by your radar device.
- The **Width** of the plate is entered for you based on the LPR context that you have configured. If necessary, modify the plate width.
- Click **Save**.

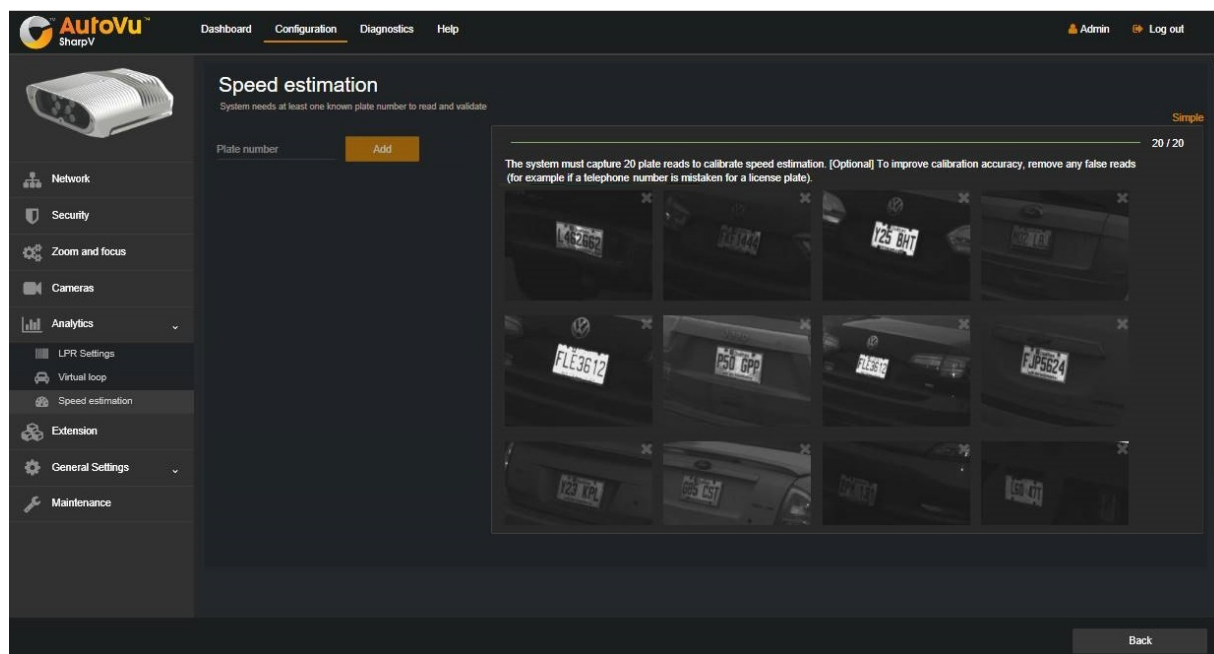
The camera captures 20 license plate reads:

The system must analyze plate reads from 20 passing vehicles. The vehicles can be traveling at any speed and you do not need to know the speed of these vehicles. There is no user action required for this step, however, you can improve speed estimation accuracy by editing the plate reads using the following steps:

NOTE: It might take more than 20 vehicle passes to complete the calibration.

- 1 From the main speed estimation screen, click **Edit**.
- 2 Click **Advanced** on the right side of the screen.

The license plates from passing vehicles are displayed.



- 3 If you notice an incorrect plate read, for example, if a sticker on the back of a vehicle was mistaken for a license plate, delete the image.
- 4 You can click on an image to display two images of the license plate. You can inspect the position of the end points of the orange line. If the position is inaccurate, you can either move the end points to correct the line placement or delete the image.
- 5 Click **Back** to return to the main speed estimation screen.

When the system has successfully read 20 license plates, and when you have entered the speed of at least one license plate, the **State** displayed on the main calibration screen is *Ready*.

When the speed estimation calibration is complete, vehicle speed is displayed in the *Live Feed* page of the portal. It is also possible to configure the vehicle speed to be included as an annotation field in Security Center. For more information, see the *Security Center Administrator Guide*.

Configuring where the SharpV sends its LPR data

Depending on whether you want to receive license plate read information in Security Center, or an FTP or HTTP server, you must configure where the SharpV sends its LPR data accordingly.

What you should know

The default extension is **None**; you must select one of the available extensions to make sure that the SharpV sends its data somewhere.

To configure the SharpV extension:

- 1 [Log on to the SharpV web portal.](#)
- 2 From the **Configuration** menu, select the **Extension** page.
- 3 From the **Extension type** drop-down list, select one of the following:
 - **FTP:** Send LPR data to an FTP server.
 - **HTTP:** Send LPR data to an HTTP server.
 - **Security Center:** Send LPR data to the LPR Manager.
- 4 If you selected **FTP** as your extension, you can configure the FTP XML template which can be integrated by third-party applications. For more information, see [Configuring the SharpV FTP extension](#) on page 45.
- 5 If you selected **HTTP** as your extension, you can configure the system to send the data in XML or JSON format. For more information and examples of the exported XML and JSON files, see [Configuring the SharpV HTTP extension](#) on page 47.
- 6 If you selected **Security Center** as your extension, configure the following:
 - **This unit manages the connection to Security Center:** Use this **only** if the autodiscovery of the connected SharpV does not work (see [SharpV camera connections to Security Center](#)). You must enter the **Server** address and **Port** of the server running the LPR Manager role. For example, if a SharpV is connected to a WiFi router, and the camera's IP address is then changed, the LPR Manager cannot detect the change automatically, so you can use this to reconnect to the Security Center computer.
 - **Discovery port:** Port on which the SharpV listens for discovery requests. This port number must match the discovery port entered on the LPR Manager *Properties* page.
NOTE: When setting the discovery port, do not use port 5050 as it is reserved for the logger service.
 - **Control port:** Used in Security Center Config Tool when creating a new LPR unit (SharpV) manually.
 - **Update Provider port:** The SharpV receives updates from LPR Manager on this port. To update the SharpV, you need to enable the **Update provider** on the LPR Manager *Properties* page, and the port numbers must match.
- 7 Click **Save**.

Related Topics

[Configuring the SharpV FTP extension](#) on page 45

[Modifications you can make to the SharpV FTP XML template](#) on page 45

SharpV camera connections to Security Center

If you are using the Security Center extension to send LPR data from a SharpV camera to Security Center, you must first enroll the camera in the Security Center *LPR* task under *Roles and units*.

The easiest way to add a SharpV camera in Security Center is to configure the LPR Manager to discover the camera. If this connection method is not possible, you can add the camera manually in Security Center or in the camera's web portal.

You can add a camera to Security Center in one of the following ways:

Connection Method	When to use this method	Requirements
Configure the LPR Manager to discover the camera: You can configure the LPR Manager's <i>Discovery port</i> to find the camera on the subnet.	This is the preferred method if the camera and Security Center are on the same subnet.	To use this method, you must set the same <i>Discovery port</i> in the LPR Manager's <i>Properties</i> tab and in the camera's web portal. The camera and Security Center must be on the same subnet. For more information on configuring LPR Managers for fixed AutoVu™ system, refer to the <i>Security Center Administrator Guide</i> .
Manually add the camera in Security Center: You can add the camera to the LPR Manager in Config Tool's <i>LPR</i> task.	Use this method when the camera and Security Center are on different subnets within the same LAN. You can use this method if the <i>Discovery port</i> is not available, however the <i>Discovery port</i> can be changed in Security Center and in the camera's web portal. NOTE: <ul style="list-style-type: none"> You cannot use this method if communication must go across the Internet. If the camera is behind a NAT, you must configure port forwarding. 	To use this method, you must know the IP address and port (control port) for the camera. The camera and Security Center must be on the same network.
Add a SharpV from the camera's web portal: You can force a connection from the camera's web portal when you select the <i>Security Center</i> extension and select Connect to Security Center . For assistance, contact your Genetec™ representative.	Use this method if the camera and Security Center must communicate across the Internet and where the network topology includes NATs. NOTE: If the camera is behind a NAT, you must configure port forwarding.	To use this method, you must enter the <i>Hostname</i> or <i>IP address</i> and <i>port</i> (listening port) of the Security Center computer.

Related Topics

[Configuring where the SharpV sends its LPR data](#) on page 41

SharpV communication ports

For SharpV cameras to communicate with Security Center, the correct communication ports must be defined.

The following table lists the default network ports used for SharpV communication with Security Center:

Computer	Inbound	Outbound	Port usage
SharpV	HTTP 8001		Control port.
	HTTP 2323		Used by the SharpV to determine which extension to load.
	UDP 5000		Used to discover SharpV units connected to the network.
		TCP 8731	Default listening port.
		TCP 8832	Used by the SharpV to communicate with the Security Center updater service.
	80		Used for HTTP communication with Security Center.
	443		Used for HTTPS communication with Security Center.

Adding a SharpV camera to the LPR Manager

To send LPR data from the camera to Security Center, you must add the camera to an LPR Manager.


Before you begin

To add a camera in Security Center, you must first configure an LPR Manager role.

What you should know

The easiest way to add a camera in Security Center is to add the camera automatically using the Unit enrollment tool. If the system cannot discover the camera, use the following method to add it manually. For more information about the Unit enrollment tool, see the *Security Center Administrator Guide*.

To manually add a camera in Security Center:

- 1 From the Config Tool home page, click the *LPR* task and select **Roles and units**.
- 2 Click  **LPR unit**.
The **Creating a unit** dialog box opens.
- 3 Enter a **Name** for the camera.
- 4 Enter the **IP address** and **Port** of the camera.
This information should match what is displayed in the camera's web portal.
- 5 Select the **LPR Manager** role from the drop-down list, and click **Next**.
- 6 Complete all other settings as necessary, and click **Create**.

The new camera is added under the selected LPR Manager.

Adding a SharpV camera to the Archiver

If you want to view the context camera video feed in Security Center, you must add the camera to the Archiver.


Before you begin


- To add a camera in Security Center, you must first configure an Archiver role.
- Log on to the camera's web portal and change the default password.
- By default, SharpV cameras are in DHCP mode. To add the context camera to the Archiver, you must configure the camera to use a static IP address that is defined in the web portal.

What you should know

- By default, the Archiver uses the H.264 stream from SharpV cameras. If you want to use the MJPEG stream, you can select it in the *Video* task from the SharpV camera's screen.
- **NOTE:** Information on context cameras is not applicable to SharpV ITS cameras.

To manually add a camera to a Security Center Archiver:

- 1 From the Config Tool home page, open the **Video** task.
- 2 If you have multiple Archiver roles, select the Archiver role to manage the video unit from the Archiver drop-down list.
- 3 Click  **Video unit**.
The **Manual add** dialog box opens.
- 4 From the **Manufacturers** drop-down list, select **Genetec AutoVu**.
- 5 From the Product type drop-down list, select **All**.
- 6 Enter the static IP address of the camera.

TIP: Use a range () of IP addresses to add multiple units in a single operation.

- 7 To use HTTP communication, enter **HTTP port 80**. To use HTTPS communication, turn on **Use HTTPS** and enter port 443.
- 8 Select the **Authentication** method for the camera.
 - **Default logon:** The camera uses the default logon defined for the Archiver in the *Extensions* tab. Using this method, you can define the same logon credentials for multiple cameras.
 - **IMPORTANT:** You cannot use the default logon when adding a SharpV camera. You must use the credentials you configured when you first logged on to the SharpV portal.
 - **Specific:** Enter the logon credentials for the camera. Turn on **Use HTTPS** if you have applied a self-signed or signed certificate to the camera connection.
- 9 From the **Location** drop-down, assign the camera to an area entity.
- 10 Click **Add**.

The notification tray displays the message "Adding unit started". If successful, it displays the message "Unit added successfully".

The camera is added under the selected Archiver.

Configuring the SharpV FTP extension

You can configure the SharpV to send LPR data to an FTP server. LPR data that is sent to an FTP server can then be integrated by third-party applications.

To configure the SharpV for FTP:

- 1 [Log on to the SharpV web portal.](#)
- 2 From the **Configuration** menu, select the **Extension** page.
- 3 From the **Active extension** section, select **FTP** from the **Extension type** drop-down menu.
- 4 Configure the following:
 - **Server:** Enter the FTP server name and location for the LPR data. You'll need the server name, port number (if different than the standard FTP server port 21), and the name of the folder. For example, `ftp://<ServerName>:<PortNumber>/<FolderNameOnServer>/.`
 - **Username:** Enter the username for the FTP server.
 - **Password:** Enter the password for the FTP server.
 - **Content Template:** LPR data is sent in XML format, using the template shown. You can change certain elements if you choose.
 - **Export context images:** Export the context image (in JPEG format).

NOTE: Information on context images is not applicable to SharpV ITS cameras.

- **Export LPR images:** Export the plate image (in JPEG format).
- **Retain data when the connection is lost:** If the check box is selected, plate read events are saved locally in the SharpV's database if the connection with the FTP server is lost. The SharpV can store up to 70 000 plate read events, however, note that event size varies based on the complexity of the scene being observed. The system tries to re-connect with the server every 30 seconds. Stored reads are pushed to the server when the connection is re-established. If the check box is cleared, the SharpV does not store reads locally if the connection with the FTP server is lost. You can see how many reads are stored on the SharpV in the *Dashboard > Overview > Storage and usage* section.

NOTE: If there are any plate reads in the SharpV's database, clearing this check box and saving the configuration deletes the plate reads.

- 5 Click **Test connection** to test the connection to the FTP server.
- 6 Click **Send sample** to send a test plate to verify that the system can connect to the server using these settings.
- 7 Click **Save**.

Modifications you can make to the SharpV FTP XML template

The XML code defines the structure of the XML files generated by the SharpV. You can re-sort or remove any of the fields. The XML file name consists of the SharpV name and a unique identification number (for example, SHARPV12345_6ee17b00-82c1-466b-9fd6-003417bc82c4_lpr.xml).

Template:

```
<?xml version="1.0" encoding="utf-8"?>
<AutoVu>
  <Plate>#PLATE_READ#</Plate>
  <State>#CUSTOM_FIELDS#{State Name}</State>
  <UTCDate>#DATE_UTC#{yyyy:MM:dd}</UTCDate>
  <UTCTime>#TIME_UTC#{HH:mm:ss.fff}</UTCTime>
  <CameraName>#CAMERA_NAME#</CameraName>
  <SourceName>#SHARP_NAME#</SourceName>
  <ContextImage>#CONTEXT_IMAGE#</ContextImage>
  <PlateImage>#PLATE_IMAGE#</PlateImage>
```

```
<LongitudeX>#LONGITUDE#</LongitudeX>
<LatitudeY>#LATITUDE#</LatitudeY>
<Guid>#GUID#</Guid>
</AutoVu>
```

Note the following:

- Hotlist matching is not supported.
- LocalDate, LocalTime, UTCDate, UTCTime, and TimeZone display the Windows date and time properties.
- CameraName is set in the Patroller Config Tool.
- SourceName is the SharpV name (e.g. Sharp12345).
- ContextImage and PlateImage are encoded into text.

NOTE: Information on context images is not applicable to SharpV ITS cameras.

- Guid is the unique identification of the event read.
- You can add the following custom fields to the template:
 - **State Name:** The SharpV attempts to read the plate's origin in addition to the plate number (some plates include the issuing state or province). This may not be possible for all types of license plates. To use this field, add <State>#CUSTOM_FIELDS#{State Name}</State> to the XML, and then select *State* on the **Analytics** page of the **Configuration** menu in the SharpV web portal.

NOTE: The LPR Context you are using must support the state name feature.
 - **Relative Motion:** When the SharpV reads a plate, it detects and displays if the vehicle is approaching or moving away. To use this field, add the following line to the XML:


```
<RelativeMotion>#CUSTOM_FIELDS#{Relative Motion}</RelativeMotion>.
```
 - **Vehicle Type:** Certain license plates include character symbols that identify specific vehicle types (for example, taxi, transport, and so on). If the SharpV can read these symbols, it displays the vehicle type along with the other read/hit information. To use this field, add the following line to the XML:


```
<VehicleType>#CUSTOM_FIELDS#{Vehicle Type}</VehicleType>.
```
- If using FTP with GPS coordinates, you'll need to add longitude and latitude fields.

Example

```
<?xml version="1.0" encoding="utf-8"?>
<AutoVu>
  <Plate>#PLATE_READ#</Plate>
  <LocalDate>#DATE_LOCAL#{HH:mm:ss}</LocalTime>
  <UTCDate>#DATE.UTC#{yyyy:MM:dd}</UTCDate>
  <UTCTime>#TIME.UTC#{HH:mm:ss.fff}</UTCTime>
  <TimeZone>#TIME_ZONE#</TimeZone>
  <CameraName>#CAMERA_NAME#</CameraName>
  <SourceName>#SHARP_NAME#</SourceName>
  <ContextImage>#CONTEXT_IMAGE#</ContextImage>
  <PlateImage>#PLATE_IMAGE#</PlateImage>
  <LongitudeX>#LONGITUDE#</LongitudeX>
  <LatitudeY>#LATITUDE#</LatitudeY>
  <Guid>#GUID#</Guid>
</AutoVu>
```

Configuring the SharpV HTTP extension

You can configure the SharpV to send LPR data to an HTTP server instead of to Security Center. LPR data that is sent to an HTTP server can then be integrated by third-party applications.

To configure the SharpV for HTTP:

- 1 [Log on to the SharpV web portal.](#)
- 2 From the **Configuration** menu, select the **Extension** page.
- 3 From the **Active extension** section, select **HTTP** from the **Extension type** drop-down menu.
- 4 Configure the following:
 - **Server:** Enter the URL of the server that receives the LPR data. For example, *https://address:port/path/*. Both *http://* and *https://* are supported.
 - **Format:** Select the format you want to send the LPR data in. You can select either **JSON** or **XML** format.
 - **Username:** Enter the username for the HTTP server (basic authentication).
 - **Password:** Enter the password for the HTTP server (basic authentication).
 - **Export context images:** Export the context image (in JPEG format).

NOTE: Information on context images is not applicable to SharpV ITS cameras.

- **Export LPR images:** Export the plate image (in JPEG format).
- **Retain data when the connection is lost:** If the check box is selected, plate reads are saved locally in the SharpV's database if the connection with the HTTP server is lost. The system will try to re-connect with the server every 30 seconds. Stored reads are pushed to the server when the connection is re-established. If the check box is cleared, the SharpV does not store reads locally if the connection with the HTTP server is lost. You can see how many reads are stored on the SharpV in the *Dashboard > Overview > Storage and usage* section.

NOTE: If there are any plate reads in the SharpV's database, clearing this check box and saving the configuration deletes the plate reads.

- **Use plate number privacy:** The camera *hashes* the license plate using the SHA-1 algorithm. When you add an alphanumeric *salt (cryptography)* to the license plate number, it increases the security of the hashed output. Adding the same salt on all of the cameras in a network means that the same license plate produces an identical hash on all cameras. This allows the external system to recognize the identical hashes as a the same vehicle while still maintaining privacy.
- IMPORTANT:** If the salt is changed after it is set, it must also be changed on all other cameras.
- **Ignore certificate errors:** Select this option when sending LPR data to an HTTPS server that does not have a trusted certificate. The SharpV will not send the LPR data to an HTTPS server that does not have a trusted certificate unless you select this option.

- 5 Click **Send sample** to send a test plate to verify that the system can connect to the server using these settings.
- 6 Click **Save**.

Examples of JSON and XML LPR events for the SharpV HTTP extension

When you send LPR data to an HTTP server, you can configure the SharpV system to send the data in XML or JSON format.

JSON format sample:

The following is an example of a license plate read event in JSON format.

NOTE: The binary image data has been removed from the example.


```
{
  "ContextCameraName" : "Context Camera",
  "ContextImage" : "",
  "Id" : "32cf870a-46aa-4cfd-914b-00062d98e93a",
  "Latitude" : 0.0,
  "Longitude" : 0.0,
  "LprCameraName" : "Lpr Camera",
  "PlateAnalytics" : [ { "Key" : "State Name",
    "Score" : -1.0,
    "Value" : "-"
  },
    { "Key" : "Vehicle Type",
    "Score" : 1.0,
    "Value" : "-"
  },
    { "Key" : "Relative Motion",
    "Score" : -1.0,
    "Value" : "-"
  },
    { "Key" : "Context",
    "Score" : 1.0,
    "Value" : "US"
  },
    { "Key" : "Characters Height",
    "Score" : 1.0,
    "Value" : "70"
  }
  ],
  "PlateImage" : "",
  "PlateRead" : "AA7D2",
  "SourceUrl" : "SHARPV12345",
  "Timestamp" : "2016-08-29T08:42:45.797"
}
```

XML format sample:

The following is an example of a license plate read event in XML format.

NOTE: The binary image data has been removed from the example.

```
<Plate>
  <ContextCameraName>Context Camera</ContextCameraName>
  <ContextImage/>
  <Id>32cf870a-46aa-4cfd-914b-00062d98e93a</Id>
  <Latitude>0.0</Latitude>
  <Longitude>0.0</Longitude>
  <LprCameraName>Lpr Camera</LprCameraName>
  <PlateAnalytics>
    <PlateAnalytics>
      <Key>State Name</Key>
      <Score>-1.0</Score>
      <Value>-</Value>
    </PlateAnalytics>
    <PlateAnalytics>
      <Key>Confidence Score</Key>
      <Score>1</Score>
      <Value>100</Value>
    </PlateAnalytics>
  </PlateAnalytics>
  <PlateImage/>
  <PlateRead>AA7D2</PlateRead>
  <SourceUrl>SHARPV12345</SourceUrl>
  <Timestamp>2016-10-21T21:35:04.8627622+00:00</Timestamp>
</Plate>
```

Plate read event parameters

The following parameters are included in JSON and XML files that are exported to the HTTP server:

Parameter	Value type	Description
ContextCameraName	String	Name of the color context camera that generated the read event. NOTE: Information on context cameras is not applicable to SharpV ITS cameras.
ContextImage	Binary	Color context image of the scene. Base64 encoded JPEG image. NOTE: Information on context images is not applicable to SharpV ITS cameras.
Id	Guid	Unique identifier for the read event.
Latitude	Double	Decimal latitude of the SharpV camera.
Longitude	Double	Decimal longitude of the SharpV camera.
LprCameraName	String	Name of the license plate recognition camera that generated the read event.
PlateAnalytics	Array of analytics	Each analytic object is composed of a data triplet. This array is of variable size. The amount of analytic objects received depends on the SharpV camera's configuration.
Key (analytic triplet)	String	Name of the analytic.
Score (analytic triplet)	Float (-1.0 or 1.0)	Indicates if the analytic value is reliable (1.0) or not (-1.0).
Value (analytic triplet)	String	Value of the analytic.
PlateImage	Binary	Black and white cropped license plate image. Base64 encoded JPEG image.
PlateRead	String	Detected license plate number.
SourceUrl	String	Unique name of the SharpV camera.
Timestamp	DateTime	Date and time of the read event (UTC) in the following format: yyyy-MM-ddTHH:mm:ss:fff.

Configuring Syslog for SharpV log files

For installations that include multiple SharpV cameras, the *Syslog* feature allows you to configure a central repository for all SharpV log entries.

Before you begin

- You will need a Syslog server that is accessible by the SharpV camera.

What you should know

- The SharpV syslog feature is compliant with the RFC 5424 protocol.
- Whether you use the syslog feature or not, SharpV logs will be available on SharpV web portal's *Diagnostics > Logs* page.

To configure a repository for SharpV log files:

- 1 [Log on to the SharpV web portal](#).
- 2 Click the *Configuration > Maintenance* page.
- 3 Select the **Use syslog** checkbox.
- 4 In the **Server** field, enter the address of the server.
- 5 In the **Port** field, enter the port.
- 6 From the **Network Protocol** drop-down, select UDP or TCP.
- 7 Click **Test connection** to test the connection.
- 8 Click **Save**.

Upgrade

This section includes the following topics:

- ["Updating the SharpV from the Sharp Portal"](#) on page 52
- ["Updating the SharpV from Security Center"](#) on page 53

Updating the SharpV from the Sharp Portal

The Web Updater tool allows you to update your SharpOS using the Sharp Portal. The Web Updater is accessed from the **Update** option available on the *Maintenance* page of the portal.

Before you begin

Update packages are available from [GTAP](#). Save the self extracting *SharpOS_12.x.x.x.zip* file on the local machine you are using to log on to the Sharp Portal.

IMPORTANT: You must select the correct upgrade file depending on the current SharpOS version running on the SharpV.

What you should know

The Web Updater does not check which version is currently installed before performing the update. Therefore, you must check your current SharpOS version and ensure that you are installing the most recent one. The current version of the SharpOS is displayed in the portal on the *Overview* page under **Version**.

To update the SharpV using the Web Updater:

- 1 Log on to the SharpV web portal.
- 2 Click **Configuration > Maintenance**.
- 3 Under **Version**, click **Update**.
- 4 In the **Software Update** dialog box, browse to the location of the folder that contains the update .zip file, and then click **Open**.
- 5 Click **Update**.
The files are transferred to the SharpV.
- 6 When the transfer is complete, click **OK**.
The *Sharp updater* page opens.
- 7 Click **Update now** to start updating the SharpV.
The *Progress* window allows you to monitor the update. When the upgrade is complete, a message indicates whether the upgrade was completed successfully. If the update fails, you receive a message and an automatic rollback occurs.

IMPORTANT: Do not close or navigate away from the *Sharp Updater* page while the update is being installed.

After you finish

After the SharpV is updated, you can click **Back to Portal** to verify that your SharpV has been upgraded. You can check the SharpV file versions on the *Overview* page by clicking **Details** under **Version**.

Updating the SharpV from Security Center

If your SharpV camera is connected to Security Center wirelessly or through a network, you can use the Security Center updater service to push the updates to the SharpV.

What you should know

The updates to the SharpV are automatically installed after you push the updates from Security Center.

To update the SharpV using the updater service:

- 1 (First time update only) Turn on the updater service and specify the listening port in Security Center Config Tool:
 - a) Log on to Security Center Config Tool.
 - b) From the Security Center Config Tool *Home* page, go to **LPR > Roles and units**, select the LPR Manager that controls the units you want to update, and then click **Properties**.
 - c) Turn on the **Update provider** and specify the listening port.
This port number must match the **Update provider port** specified on the *Extension* page of the SharpV web portal.

Security Center creates the *Updates* folder under the *LPR Root Folder* on your computer. This folder is usually located at *C:\Genetec\AutoVu\RootFolder\Updates*.
- 2 Copy the SharpV updates to the *Upgrade* folder. For example, *C:\Genetec\AutoVu\RootFolder2\Updates\SharpOS\Upgrade* folder:
 - a) From the Security Center Config Tool *Home* page, go to **LPR > General settings > Updates** to display the SharpV units on your system.
 - b) Click the **Genetec Patroller™ and SharpV units** tab.
 - c) Move the mouse pointer to the **Drop folder** of the component you want to update.
A tool tip appears with the drop folder's location. If you're on the computer hosting the LPR Manager role, you can click the **Drop folder** icon to automatically open the folder.
 - d) Copy the update to the **Drop folder**.
After copying the zip file into the folder, the file name changes from *.zip* to *.processed*. This means that the LPR Manager has unzipped the update, and is ready to send the update to the AutoVu™ components.
- 3 Push the updates to AutoVu™ components:
 - a) From the Security Center Config Tool *Home* page, go to **LPR > General settings > Updates**.
The Patrollers and Sharp units tab displays the SharpV cameras that are eligible for an update.
 - b) Click **Update** to update a single camera, or click **Update all** to update all eligible cameras in the list.
When the status changes from **Waiting for connection...** to **Synchronized**, it means the camera has successfully downloaded the update.

NOTE: The time it takes to transfer the updates depends on the connection bandwidth and the size of the update.

The update is automatically installed on the associated SharpV.

Sharp Portal reference

This section includes the following topics:

- ["Sharp Portal - Overview page "](#) on page 55
- ["Sharp Portal - Camera feeds page "](#) on page 57
- ["Sharp Portal - Network page "](#) on page 58
- ["Sharp Portal - Security page "](#) on page 59
- ["Sharp Portal - Zoom and focus page "](#) on page 60
- ["Sharp Portal - Cameras page "](#) on page 62
- ["Sharp Portal - Analytics page "](#) on page 63
- ["Sharp Portal - Extension page "](#) on page 65
- ["Sharp Portal - Date and time page "](#) on page 67
- ["Sharp Portal - Power options page "](#) on page 68
- ["Sharp Portal - Maintenance page "](#) on page 69
- ["Sharp Portal - Logs page "](#) on page 70

Sharp Portal - Overview page

The *Overview* page is available from the **Dashboard** menu. Use the **Overview** page to view general information about the SharpV, such as serial number, license, IP address, input and output status, and so on.

SharpV (XYZ)

Use the section with the name of your SharpV to view general information about it.

- **Serial number:** Displays the SharpV hardware serial number.
 - **License:** Displays if the SharpV license is valid, invalid, or missing.
 - **Inputs:** Shows the inputs on the SharpV and whether the input is in a high or low state. When the input is in a high state, it is detecting a voltage of 5.75 V or higher. When the input is in an “low” state, it is detecting a voltage of 4.80 V or lower.
 - **Outputs:** Shows the SharpV outputs (two dry type, solid-state (transistor) polarized outputs) and whether the output is in a high or low state. When the output is in a high state, the output is open. When the input is in an low state, it is closed. SharpV.
 - **Test outputs:** Click to toggle your configured output between low and high to validate the configuration.
 - **Mac address:** Displays the MAC address of the SharpV. This information might be requested if you contact technical support.
 - **Type:** Displays the type of SharpV unit.
 - **Illuminator:** Displays the illuminator information on the SharpV.
 - **Image:** Displays the software image installed on the SharpV. If you contact technical support, you will be asked to provide this number.
 - **Version:** Displays the SharpOS package version. Click **Details** for more information about the versions of the services included in the package. You can use this information to confirm that your SharpV is up to date.
 - **Location:** Displays the coordinates of the SharpV camera (the camera's position must be configured in Security Center). **Locate on map** displays the camera's position on a map.
 - **Camera:** Displays the resolution and the lens focal range available for context camera images and LPR camera images.
- NOTE:** Information on context cameras is not applicable to SharpV ITS cameras.
- **Blink LED:** Click to blink the LED on the SharpV for ten seconds. This is useful when you have multiple Sharps and you want to physically identify the one you are configuring.

Connectivity

Use the **Connectivity** section to view information about the internet connectivity and whether or not the SharpV is connected to Security Center.

- **IP address:** Displays the IP address of the SharpV.
- **Security Center:** Displays whether the SharpV is connected to Security Center or not.

NOTE: This field is only displayed if you choose to send your LPR data to Security Center on the **Extension** page.

- **Internet:** Displays whether the SharpV is connected to the Internet or not.

- **Video streams:** If the SharpV has been added to the Security Center Archiver and is being used to monitor video, then the camera name, client IP address, frame rate, and encoding format are listed for each stream.

Storage and usage

Use the **Storage and usage** section to view information about reads stored on the SharpV, CPU usage, and memory usage. Indicator lines are provided so you can see the status. Indicator lines are usually green or orange. A red indicator line either indicates that there is a problem, or indicates high CPU activity.

- **Reads stored:** Indicates the reads stored in the database of the SharpV (in bytes). The number of reads is also displayed.
- **Memory:** Displays the memory drives, and indicates each drive's memory usage in gibibytes (GiB).
- **CPU (Total):** Indicates the total CPU usage of the SharpV. Click **Show details** to see the usage for each CPU.

Last activities

- **Unit rebooted:** Indicates the last time the unit was restarted.
- **Software restarted:** Indicates the last time the PlateReader software was restarted.

Sharp Portal - Camera feeds page

The *Camera feeds* page is available from the **Dashboard** menu. Use the **Camera feeds** page to view the live feeds of the Context camera and LPR camera.

Camera feeds

The **Camera feeds** section displays the live video feeds for both the Context camera and the LPR camera. You can also view information about the live video feed such as the **FPS**, **Resolution**, **Exposure time**, and so on.

NOTE: Information on context cameras is not applicable to SharpV ITS cameras.

- **Record:** Click the **Record** button to capture a series of context and LPR images directly from the **Camera feeds** window and save them to your computer as a .zip file for debugging purposes.

NOTE: Using the **Record** option increases CPU usage.

- **Camera selection:** You can select either the **1st camera group** (LPR and Context camera) or **No camera**. The **No camera** option is useful when you want to conserve CPU usage and network bandwidth while monitoring reads.
- **Show the crosshairs:** Select this option to display crosshairs in the LPR or Context camera window.
- **Show the bounding box:** Select this option to display the yellow bounding box around detected plates in the **LPR camera** window.
- **Show the region of interest:** Select this option to display the region of interest in the **LPR camera** window. The region of interest must be configured on the **Cameras** page. There is no region of interest by default.
- **FPS (actual/average):** Displays the FPS of the context camera. This is the framerate processed by the LPR engine.
- **Resolution:** Displays the resolution of the camera's video feed.
- **Exposure time:** Displays the **Exposure** time of the video feed.
- **Gain:** Displays the **Gain** of the video feed.
- **Iris:** Displays the **Iris** aperture of the video feed as a percentage.
- **Illuminator:** (Context camera only) Displays the intensity of light of the illuminator (as a percentage) on the Context camera.

Last read

- **Plate number:** Displays the plate number of the last read.
- **State:** Displays the plate state or province if the Sharp was able to read it from the license plate. You must enable this feature in the **Analytics** page of the **Configuration** menu.
- **Number of reads:** Displays the number of reads that have been taken with the Sharp since the Plate Reader service was started. You can reset this value to zero by clicking **Reset**.
- **Candidate:** Every read detected is displayed in this field as a potential read candidate. The SharpV can read up to 30 frames (reads) per second. The **Read strategy** configured on the **Analytics** page determines which read candidate that will be used as the final read.

Sharp Portal - Network page

The *Network* page is available from the **Configuration** menu. Use the *Network* page to configure the SharpV to use Dynamic Host Configuration Protocol (DHCP) or a static IP address.

IPv4 network settings

NOTE: DHCP is used by default if no option is selected.

- **Use DHCP:** Select this option to connect the SharpV to a DHCP server, which assigns the required IP address. On a network with DHCP and DNS servers, you can connect to the SharpV using the SharpV name (for example, SharpV 1234) rather than the IP address (for example, 192.186.10.100).
- **Use static IP address:** Select this option to use a static address for the SharpV.

IMPORTANT: You must use a static IP address if you want to stream video to the Security Center Archiver role.

You can modify the following:

- **IP address:** Type the new IP address you want to assign to the SharpV. The default is 10.0.0.1.
- **Subnet mask:** Type the new **Subnet mask** if applicable. The default is 255.255.0.0.
- **Gateway:** Type the new **Gateway** if applicable. The default is 10.0.0.0.
- **DNS:** Type the new **DNS** if applicable. The default is 10.0.0.0.

Sharp Portal - Security page

The *Security* page is available from the **Configuration** menu. Use the *Security* page to modify the password, to manage certificates and permissions, and to configure the unit's LED.

Access

- **Modify password:** Click **Modify password** to change the password for the SharpV.

NOTE: If you forget your password, [you can reset it from the logon page](#).

HTTPS connection policy

- **HTTPS status:** Displays whether an installed and activated certificate has enabled HTTPS.

Certificate

Displays the signed and self-signed certificates that have been installed in your trusted root store. You can install multiple certificates and select which certificate to activate.

To activate a certificate, select the **Active** check box for the certificate and click **Save**.

To delete a certificate click **X** and click **Save**.

- **+ Self-signed:** Click to create a self-signed certificate. In the *Create a self-signed certificate* dialog box, you must enter a two-letter **Country** code, the **Server name**, the **IP address**, and you must define the **Validity (in years)**. The other fields are optional.

NOTE: If you use a self-signed certificate, you must also install the certificate on your client machine. For example, the machine used to log on to the SharpV web portal.

- **+ Signing request:** Click to create a certificate signing request. A certificate signing request must be created for your server before you can order a signed certificate from a trusted Certificate Authority. You must enter a two letter **Country** code, the **Server name**, and the **IP address** in the *Create a certificate signing request* dialog box. The other fields are optional.

IMPORTANT: If the SharpV has been added to the Security Center Archiver and is being used to monitor video, you must enter the IP address of the SharpV and not the SharpV name.

NOTE: The signing request is deleted when the certificate is signed.

Permissions

- **Accept remote reboot requests:** Select this option so that the SharpV can be rebooted from other applications.
- **Remote assistance:** Click **Enable for 1 hour** to grant remote access for technical support. The time and date when access expires is displayed.

NOTE: After an hour, logged-in users are still authorized but new logins are denied.

Unit

- **Run in covert mode:** Select this option to turn off the LED on the Sharp unit, making it less noticeable.

IMPORTANT: Selecting this option does not mean that the LED will never be illuminated. For example, if there is a serious error with the SharpV, the LED will blink to indicate that there is a problem.

Sharp Portal - Zoom and focus page

The *Zoom and focus* page is available from the **Configuration** menu. Use the *Zoom and focus* page to adjust the images from the LPR camera and Context camera so that they are clear, and vehicles associated with plate reads can be easily identified.

Normally the zoom and focus is adjusted once, and only needs to be adjusted if the location of the SharpV changes.

NOTE: Information on context cameras is not applicable to SharpV ITS cameras.

To properly adjust the zoom and focus for the SharpV:

- The camera must be pointed at a stationary license plate or target so that you can evaluate the appearance of the plate reads.
- **Select your camera:** Select which camera you want to adjust (LPR or Context).
- **Temporarily adjust the exposure:** Use the slider to adjust the exposure for the best plate image.

NOTE: This temporary setting is only used while adjusting the zoom and focus. Auto-exposure is temporarily suspended and the iris is fully open. After adjustment is complete, this setting is ignored and the camera uses the **Exposure** setting that is configured on the **Configuration > Cameras** page.

- **Enable Flash:** (Context camera only) If you need to calibrate the zoom and focus of the context camera in low light conditions, select this option to enable the IR illuminator.
- **Set the zoom level:** Use the labeled screws on the bottom of the SharpV to adjust the zoom on the camera's LPR lens or context camera. Use the **Show ruler** option in the portal to help you adjust the zoom so that the plate characters are 25 - 60 pixels, where 30 pixels is ideal. You can visually monitor when the optimal setting is reached, using the **Best score** graph. The zoom screws are labeled as follows:
 - **CTX:** Context camera
 - **LPR:** LPR camera
 - **T:** Telephoto
 - **W:** Wide
 - **(Context camera only) SR:** Standard range
 - **(Context camera only) LR:** Long range

IMPORTANT: The zoom level impacts the focus. Always adjust the zoom level before setting the focus.

- **Set the focus:** Use the labeled screws on the bottom of the SharpV to adjust the focus on the camera's LPR lens or context camera. Focus the camera on a stationary plate located at the mid-point of the vehicle's expected trajectory. You can visually monitor when the optimal setting is reached, using the **Best score** graph. The focus screws are labeled depending on the camera type and model:
 - **CTX:** Context camera
 - **LPR:** LPR camera
 - **F:** Far
 - **N:** Near
 - **(Context camera only) SR:** Standard range
 - **(Context camera only) LR:** Long range
- **Best score:** Use the **Best score** graph to visually monitor when the optimal setting is reached for the zoom and focus while you are adjusting the screws on the bottom of the SharpV. The bold orange line in the graph indicates the current focus value. The dim orange line indicates the best focus that has been achieved. You have reached the optimal point when the bold orange line separates from the dim orange

line and begins to descend. At this point, you must reverse the direction that you are turning the screw so that the bold orange line returns upwards to meet the dim orange line. When the two lines intersect again, this is the optimal setting.

- **Reset:** Click to reset the **Best score** graph.
- **Show ruler:** Select this option to have the ruler display on the camera image. Drag the ruler next to the license plate and enter a pixel (px) value to change the size of the ruler on the screen. The height of the plate characters in the image should be between 25 - 60 pixels, where 30 pixels is ideal.

TIP: Click the license plate to use digital zoom to help you evaluate the best zoom level. There are three zoom levels: 1:1, 2:1, and 4:1. A preview of the zoomed area is displayed in the top right corner of the image.

- **Done:** Click when you are finished calibrating the zoom and focus for your LPR and Context cameras.

Sharp Portal - Cameras page

The *Cameras* page is available from the **Configuration** menu. Use the *Cameras* page to define a region of interest and adjust the exposure.

- **Select your camera:** Select the camera to configure.
- **(Context camera only) Lighting type:** Select a lighting type from the drop-down menu.
NOTE: Information on context cameras is not applicable to SharpV ITS cameras.
- **Exposure:** Select the **Exposure** type. You can choose from the following:
 - **Default:** Select this option to have the SharpV automatically adjust the exposure settings.
 - **Fixed (indoor):** Select this option when constant lighting conditions are available. Use the sliders to adjust the **Gain** and **Shutter time**, until the overall brightness and clarity you want for the image is achieved.
 - **Range (outdoor):** Select this option for variable lighting conditions outdoors. Use the sliders to adjust the **Gain** and **Shutter time**, until the overall brightness and clarity you want for the image is achieved.
- **(LPR camera only) Click the picture to define region of interest:** Defining a region of interest restrict the readable area to a portion of the field of view as configured by the user. Define a region of interest by clicking points on the image to create a perimeter. Click **Clear the region of interest** to delete the region.
- **(Context camera only) Enable illuminator:** Select this to enable the IR illuminator in low light conditions. If **Exposure** is set to **Fixed (indoor)**, the IR illuminator is fixed to On or Off depending on **Enable illuminator** check box. If **Exposure** is set to **Range (outdoor)**, the illuminator is automatically turned On or Off depending on light conditions. However, the IR illuminator can be completely turned off by clearing the **Enable illuminator** check box.

NOTE: Information on context cameras is not applicable to SharpV ITS cameras.

Sharp Portal - Analytics page

The *Analytics* page is available from the **Configuration** menu. Use the *Analytics* page to configure the analytics used for the license plates read by the SharpV.

- **Context:** Select which plate origin the SharpV is reading.
- **Reading mode:** Select one of the following reading modes:
 - **Continuous:** Select this for plates to be captured continuously. This is the default setting.
 - **Conditional:** When this option is selected, the SharpV captures plate reads continuously as long as the selected input signal meets the condition defined (high/low). You must select an input and specify whether the state is high or low.
 - **Single read on trigger:** Select this option so the SharpV captures a plate read after a signal is received from an electrical trigger, or after a Security Center event-to-action or hot action. This configuration is useful for controlling vehicle access to gated parking lots. You can configure the plate read capture to occur before or after the trigger is activated.
 - **Add trigger:** Select to add a trigger. You must configure the following:
 - **When.** Select which input receives the trigger signal and indicate the state of the input (**Low** or **High**). You can also select an **External** input (Security Center event to-action or hot action).
 - **Capture Window.**
 - **Start X ms before/after trigger.** The capture can occur up to X ms before or after the trigger is activated.
 - **Duration X ms.** The system attempts to capture a plate read for up to 30000 ms. 4000 ms is the default value.
 - **IMPORTANT:** The capture window cannot end before the time the trigger is activated.
 - **If no plates.**
 - **Capture image X ms after trigger.** If no plate is read during the time specified in the **Capture window**, a *no plate* read is logged and the system captures a context image of the vehicle so the read can be manually edited.
 - **Use LPR image as context image.** An image from the LPR camera is used to replace the context image for the *no plate* read.
 - **Capture image X ms after trigger.** If no plate is read during the time specified in the **Capture window**, a "no plate" read is logged and the system captures a context image of the vehicle so the read can be manually edited.
 - **Use LPR image as context image.** An image from the LPR camera is used to replace the context image for the "no plate" read.
 - **NOTE:** Information on context images is not applicable to SharpV ITS cameras.
- **Read strategy:** Select one of the following read strategies:
 - **Slow-moving vehicles:** Select this when vehicles are traveling slowly when their license plates are captured. For example, use this for parking lot gates or toll stations.
 - **Fast-moving vehicles:** Select this when vehicles are traveling at moderate to high speeds when their license plates are captured. For example, select this option for a Sharp overlooking a highway.
 - **Gate control:** Select this when vehicles are stopped when their license plates are captured. For example, use this for a Sharp that is monitoring a gated parking lot or toll booth.
- **Options:** Select **Optimize for fixed installation** to create a smart region of interest to decrease false positives.

- **Read contents:** Select what you would like the SharpV to attempt to read:

NOTE: You can add the state, vehicle make, and confidence score as annotation fields in Security Center to query for this information in Security Desk reports.

- **State:** Select this option if you want the Sharp unit to attempt read the license plate origin (issuing state, province, or country).

NOTE: Plate state recognition might not be available for all states.

- **Vehicle make:** Select this option if you want the Sharp unit to attempt to read the vehicle's make from the brand or logo (Honda, Toyota, and so on).
- **Confidence score:** Assigns a numerical value (from 0 to 100) to each license plate read. This value indicates how confident the SharpV is in the accuracy of the read.

Sharp Portal - Extension page

The *Extension* page is available from the **Configuration** menu. Use the *Extension* page to configure where the SharpV sends LPR data.

- **Extension type:** Select an extension type from the drop-down list.
 - **None:** The default state.
 - **FTP:** Sends LPR data to an FTP server. Configure the following:
 - **Server:** Enter the server name and location for the LPR data.
 - **Username:** Enter the username for the server.
 - **Password:** Enter the password for the server.
 - **Test connection:** Click to determine if the server address can be reached by the SharpV.
 - **Content template:** LPR data is sent in XML format, using the template shown. You can change certain elements if you choose.
 - **Export context images:** Export the context images (in JPEG format).
NOTE: Information on context images is not applicable to SharpV ITS cameras.
 - **Export LPR images:** Send the plate images (in JPEG format).
 - **Retain data when the connection is lost:** Select this option for plate reads to be saved locally in the SharpV database if the connection with the server is lost. The system attempts to reconnect with the server every 30 seconds. Stored reads are pushed to the server when the connection is re-established.
 - **Send sample:** Click **Send a test plate** to verify that the system can connect to the server using the configured settings.
 - **HTTP:** Sends LPR data to an HTTP server. Configure the following:
 - **Server:** Enter the server name and location for the LPR data.
 - **Username:** Enter the username for the server.
 - **Password:** Enter the password for the server.
 - **Ignore certificate errors:** Select this option when sending LPR data to an HTTPS server that does not have a trusted certificate. The SharpV will not send the LPR data to an HTTPS server that does not have a trusted certificate, unless this option is selected.
 - **Format:** Select the format for the LPR data. You can select either **JSON** or **XML** format.
 - **Export context images:** Export the context images (in JPEG format).
NOTE: Information on context images is not applicable to SharpV ITS cameras.
 - **Export LPR images:** Send the plate images (in JPEG format).
 - **Retain data when the connection is lost:** Select this option for plate reads to be saved locally in the SharpV database if the connection with the server is lost. The system attempts to reconnect with the server every 30 seconds. Stored reads are pushed to the server when the connection is re-established.
 - **Send sample:** Click **Send a test plate** to verify that the system can connect to the server using the configured settings.
 - **Send sample:** Click **Send a test plate** to verify that the system can connect to the server using the configured settings.
 - **Use plate number privacy:** The camera *hashes* the license plate using the SHA-1 algorithm. When you add an alphanumeric *salt (cryptography)* to the license plate number, it increases the

security of the hashed output. Adding the same salt on all of the cameras in a network means that the same license plate produces an identical hash on all cameras. This allows the external system to recognize the identical hashes as a the same vehicle while still maintaining privacy.

IMPORTANT: If the salt is changed after it is set, it must also be changed on all other cameras.

- **Security Center:** Send LPR data to Security Center. Configure the following options:
 - **This unit manages the connection to Security Center:** Select this option if you want the SharpV you are currently configuring to manage the connection to Security Center. You must enter the following:
 - **Server:** The address of the Security Center server.
 - **Port:** Enter the Live - Listening Port of the LPR Manager role on the Security Center server.
 - **Discovery port:** Port on which the SharpV listens for discovery requests. If you chose Security Center, the port must match the discovery port entered on the LPR Manager *Properties* page.
 - **Control port:** Port used in Security Center Config Tool when creating a new LPR unit (Sharp) manually.
 - **Update provider port:** The Sharp receives updates from Security Center on this port. To update the Sharp, you need to enable the Update provider on the LPR Manager *Properties* page, and the port numbers must match.
 - **Test connection:** Click to determine if the server address can be reached by the SharpV.

Sharp Portal - Date and time page

The *Date and time* page is available from the **Configuration** menu. Use the *Date and time* page to configure how you want to configure the internal clock of the SharpV.

- **Settings:** Select one of the following settings.
 - **No synchronization:** The default state. The SharpV uses its own clock.
 - **NTP server:** Enter the URL of a known time server (for example, *time.windows.com*). The SharpV clock synchronizes with this server on startup and then every hour. You can test the connection at any time by clicking **Test connection**.
 - **Active extension (Security Center):** Click to synchronize the SharpV clock with the clock on the Security Center server it is connected to. The SharpV clock synchronizes with the Security Center server clock upon connection, then every 24 hours.
IMPORTANT: Selecting this option has no effect if you are using any of the other extension types (FTP, HTTP, and so on). It can only be used when the active extension type is configured as Security Center. The active extension is configured on the *Extension* page.
 - **Synchronize with client browser now:** Click to synchronize the date and time with the client machine you are using to connect to the Sharp portal. The camera performs a one-time synchronization.
IMPORTANT: Do not synchronize the SharpV clock with the client browser unless you are connecting to the SharpV web portal from the server hosting the LPR Manager role. If you synchronize clocks with a computer other than the Security Center server, the camera's reads and hits might not have accurate timestamps.
- **Date and time format:** Select one of the following date and time formats.
 - **International:** Selecting the International option displays the date and time in the format: YYYY-MM-DD HH:MM:SS
 - **Imperial:** Selecting the Imperial option displays the date and time in the format: DD/MM/YYYY H:MM:SS AM/PM

Sharp Portal - Power options page

The *Power options* page is available from the **Configuration > General settings** menu. Use the *Power options* page to configure the camera based on the power grid of the installation location.

- **Power line frequency:** Select the power line frequency that corresponds to the installation location.
 - **60 Hz:** Generally used in North America and South America
 - **50 Hz:** Generally used in Africa, Australia, Asia, and Europe

NOTE: For more information on the power line frequency used in your installation location, [click here](#).

Sharp Portal - Maintenance page

The *Maintenance* page is available from the **Configuration** menu. Use the **Maintenance** page to free up disk space, import and export settings, and restart the SharpV.

- **Version:**
 - **Image:** Displays the current image/firmware installed.
 - **Version:** Displays the SharpOS version installed.
 - **Reclaim disk space:** Displays the amount of disk space that can be freed up by deleting log files, cache files, and stored reads. Click **Free up space** to reclaim the space displayed.
IMPORTANT: Do not click **Free up space** if you think there are any untransmitted reads stored on the SharpV that you want to keep.
 - **Update:** Click to update the SharpOS.

Settings

- **Export settings:** Click to export configuration and diagnostic settings as a .zip file. You can use the .zip file for technical support, or you can import the settings to another Sharp unit for quick configuration
- **Import settings:** Imports configuration settings from a .zip file exported from another Sharp. You can use this .zip file to quickly configure your Sharp. After you import the settings, the Plate Reader service restarts automatically.
IMPORTANT: You can only import settings from a similar Sharp (same model and SharpOS version).
- **Reset to factory default:** Click to reset the SharpV to use the factory default settings.

Syslog

- **Use Syslog server:** Select this option to configure a central repository for all SharpV log entries.
 - **Server:** Enter the name of the server.
 - **Port:** Enter the name of the port.
 - **Network protocol:** Select UDP or TCP.

Reboot unit: Click to restart the SharpV.

Sharp Portal - Logs page

The *Logs* page is available from the **Diagnostics** menu. Use the *Logs* page to run reports and generate logs about the status of the SharpV. You can filter by a specific source, message, and so on. Log reports can also be exported to a .zip file by selecting **Export settings** on the *Maintenance* page.

- **Severity:** Click the icons to choose which severity types you want to include in the report query. You can choose from the following:
 - Error
 - Warning
 - Information
 - Debug
 - Performance
- **Source:** Select the source that you want to include in the report query.
- **Message:** Enter a message. Only logs containing the message string entered are displayed on the query.
- **Distinct entries only:** Logs with identical messages are displayed only once.
- **Time:** Select a time range.
- **Search:** Click to run the query.
- **Pause:** Click to pause the auto-refresh on the query. This is useful when you want to stop new entries from coming in so you can focus on a particular entry. Click **Resume** to activate the auto-refresh on the query.
- **Download all logs in XML file:** Click to download an XML log file.

NOTE: The filters on this page apply only to the visual report. The XML log file always contains a full, unfiltered list of events.
- **Sources to log:** Select the sources from which to generate a log. For example, if you only want to generate log events related to Plate Reader, select **Plate Reader** from the list.

NOTE: A source that contains **(Verbose)** in its name might generate a lot of disk activity.

Troubleshooting for SharpV fixed installation

This section includes the following topics:

- ["LED status on the SharpV camera unit"](#) on page 72
- ["Resetting a lost password for the SharpV web portal"](#) on page 74

LED status on the SharpV camera unit

The status LED on the SharpV camera unit responds according to the status of the system.

The following table describes how the SharpV camera's LED behaves in response to the SharpV system's status:



State	Description	LED (red or green)
Off	Unit is powered-off.	Off
Covert mode	The camera is configured in covert mode. Following camera startup, the LED is deactivated.	Off
Catastrophic failure	The camera is shut down due to a critical error, for example, an over-temperature alarm. In this state, you cannot connect to the camera.	Slow red blinking (0.5 seconds off – 0.5 seconds on)
Major failure	Plate Reader is down. You might be able to connect to the camera and you might be able to see the logs.	Three red blinks per second
Performance issues or minor failure	Plate Reader is running with important performance issues, for example, failure of the illuminator .	One short red blink per second
PoE+ failure	The PoE power supply has failed to negotiate IEEE 802.3at (POE+, or 25.5 W). PlateReader will not run, but the SharpV web portal might be accessible. Check the SharpV logs. For more information, see the network cable requirements for SharpV cameras.	One long red blink and one short green blink per second
Camera update	Plate Reader is down during the camera update, but is expected to come back online after the update is complete.	Five green blinks per second

State	Description	LED (red or green)
Locate camera	After clicking Blink LED in the SharpV web portal, the LED blinks for 10 seconds.	Slow red and green alternating (0.5 seconds each)
Focus mode	The camera's focus and zoom are being adjusted in the SharpV web portal.	Fast red and green alternating (0.25 seconds each)
Normal mode	The camera is running normally.	Solid green
Camera startup	The camera is booting up.	One green blink per second

Resetting a lost password for the SharpV web portal

If you forget your password to the SharpV web portal, you can reset the password using the **I forgot my password** button on the SharpV web portal logon screen.

Before you begin

To reset a lost password, you need the yellow *Important information* sticker that was shipped with the SharpV camera. If you do not have the sticker, you must contact your representative from Genetec Inc.

What you should know

- As a step in the password reset procedure, you must press the reset button on the SharpV camera. Alternatively, if you do not have physical access to the camera, you are given the option to present a known license plate to the camera.
- You can use this procedure for SharpV cameras running SharpOS 12.3 SR1 or later.

To reset a lost password for the SharpV web portal:

- From the SharpV web portal logon screen, click **I forgot my password**.
- Enter the 32-character unit access code. You can find the unit access code on the yellow sticker that was provided with the SharpV camera.

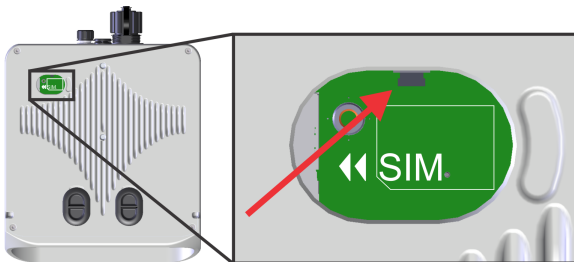


If you do not know the unit access password, contact the Genetec™ Technical Assistance Center (GTAC) at <https://gtap.genetec.com>.

- Click **Next**.
- For added security, and to ensure that the password cannot be reset remotely, you must select one of the following validation methods:
 - Press the reset button:** To use this validation method, you must have physical access to the camera.
 - Read a plate number:** To use this validation method, you are prompted to enter a plate number, and then have the camera read the plate.

To validate by pressing the reset button:

- Select **Use the reset button** and click **Next**.
The message *Press and hold the Sharp reset button for 2 seconds* is displayed.
- Press and hold the reset button for 2 seconds.
The reset button is located behind the rubber plug as indicated in the following image:



NOTE: If you do not press the reset button within two hours, the password recovery operation is canceled.

- The message *Reset button pressed. Please wait.* is displayed.
- 3 When prompted, enter and confirm the new Sharp web portal password.
 - 4 Click **Apply**.
The message *The portal password has been changed* is displayed.
 - 5 Log on to the web portal using your new password.
 - 6 Store your password safely for future use.

To validate by reading a plate number:

- 1 Select **Read a plate number**.
- 2 Enter the number of a license plate that you can use to generate a plate read on the camera.
- 3 Click **Next**.
- 4 The message *Waiting for the Sharp to read plate ABC123* is displayed.
- 5 Use the plate to generate a read on the camera.
NOTE: If the camera does not read the plate within two hours, the password recovery operation is canceled.
- 6 When the camera reads the plate, the message *Plate number read. Please wait* is displayed.
- 7 When prompted, enter and confirm the new Sharp web portal password.
- 8 Click **Apply**.
The message *The portal password has been changed* is displayed.
- 9 Log on to the web portal using your new password.
- 10 Store your password safely for future use.

Glossary

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

authorized user	An authorized user is a user who can see (has the right to access) the entities contained in a partition. Users can only exercise their privileges on entities they can see.
action	An action is a user-programmable function that can be triggered as an automatic response to an event, such as door held open for too long or object left unattended, or that can be executed according to a specific time table.
Activity trails	Activity trails is a type of maintenance task that reports on the user activity related to video, access control, and LPR functionality. This task can provide information such as who played back which video recordings, who used the Hotlist and permit editor, who enabled hotlist filtering, and much more.
area	An area is a type of entity that represents a concept or a physical location (room, floor, building, site, and so on) used for grouping other entities in the system.
automatic enrollment	Automatic enrollment is when new IP units on a network are automatically discovered by and added to Security Center. The role that is responsible for the units <i>broadcasts</i> a discovery request on a specific port, and the units listening on that port respond with a message that contains the connection information about themselves. The role then uses the information to configure the connection to the unit and enable communication.
AutoVu™	AutoVu™ is the automatic license plate recognition (ALPR) system of a Security Center system that automates license plate reading and identification. Deployed in both fixed and mobile installations, it lets you extend your physical security into your parking lots and perimeter, so you are always aware of vehicles moving in and out of your facilities.
AutoVu™ LPR Processing Unit	AutoVu™ LPR Processing Unit is the processing component of the SharpX system. The LPR Processing Unit is available with two or four camera ports, with one dedicated processor per camera (if using SharpX) or per two cameras (if using SharpX VGA). This ensures maximum, per-camera, processing performance. The LPR Processing Unit is sometimes referred to as the <i>trunk unit</i> because it is typically installed in a vehicle's trunk.

B

Breakout box	The breakout box is the proprietary connector box of Genetec Inc. for AutoVu™ mobile solutions that use Sharp cameras. The breakout box provides power and network connectivity to the Sharp units and the in-vehicle computer.
broadcast	Broadcast is the communication between a single sender and all receivers on a network.

C

canvas	Canvas is one of the panes found in the Security Desk's task workspace. The canvas is used to display multimedia information, such as videos, maps, and pictures. It is further divided into three panels: the tiles, the dashboard, and the properties.
capture rate	The capture rate measures the speed at which a license plate recognition system can take a photo of a passing vehicle and detect the license plate in the image.
certificate	Designates one of the following: (1) <i>digital certificate</i> ; (2) <i>SDK certificate</i> .
City Parking Enforcement	City Parking Enforcement is a Patroller software installation that is configured for the enforcement of parking permit and overtime restrictions.
City Parking Enforcement with Wheel Imaging	City Parking Enforcement with Wheel Imaging is a <i>City Parking Enforcement</i> installation of a Patroller application that also includes wheel imaging. The use of maps and of the Navigator is mandatory.
Config Tool	Config Tool is a Security Center administrative application used to manage all Security Center users, and configure all Security Center entities such as areas, cameras, doors, schedules, cardholders, Patroller/LPR units, and hardware devices.
context camera	A context camera is a camera connected to an LPR unit that produces a wider angle color image of the vehicle whose license plate was read by the LPR camera.
Copy configuration tool	The Copy configuration tool helps you save configuration time by copying the settings of one entity to many others that partially share the same settings.
covert hit	A covert hit is a read (captured license plate) that is matched to a covert hotlist. Covert hits are not displayed on the Patroller screen, but can be displayed in Security Desk by a user with proper privileges.

covert hotlist	A covert hotlist is a hotlist hidden from the AutoVu™ Patroller users. Reads matching a covert hotlist generate covert hits.
custom event	A custom event is an event added after the initial system installation. Events defined at system installation are called system events. Custom events can be user-defined or automatically added through plugin installations. Unlike system events, custom events can be renamed and deleted.
custom field	A custom field is a user defined property that is associated to an entity type and is used to store additional information that is useful to your particular organization.
D	
Daily usage per Patroller	Daily usage per Patroller is a type of investigation task that reports on the daily usage statistics of a selected Patroller (operating time, longest stop, total number of stops, longest shutdown, and so on) for a given date range.
dashboard	A dashboard is one of the three panels that belong to the canvas in Security Desk. It contains the graphical commands (or widgets) pertaining to the entity displayed in the current tile.
database server	A database server is an application that manages databases and handles data requests made by client applications. Security Center uses Microsoft SQL Server as its database server.
Data Server	Data Server is the Plan Manager Server module that manages the Plan Manager database where the map configuration is stored.
Directory	Directory is the main role that identifies your system. It manages all entity configurations and system wide settings in Security Center. Only a single instance of this role is permitted on your system. The server hosting the Directory role is called the <i>main server</i> , and must be set up first. All other servers you add in Security Center are called <i>expansion servers</i> , and must connect to the main server to be part of the same system.
Directory Manager	Directory Manager is the role that manages the Directory failover and load balancing in order to produce the high availability characteristics in Security Center.
Directory server	A Directory server is any one of the multiple servers simultaneously running the Directory role in a high availability configuration.
discovery port	A discovery port is a port used by certain Security Center roles (Access Manager, Archiver, LPR Manager) to find the units they

are responsible for on the LAN. No two discovery ports can be the same on one system.

district

A district is a type of parking regulation characterizing an overtime rule. A district is a geographical area within a city. A vehicle is in violation if it is seen within the boundaries of the district over a specified period of time.

E

enforce

To enforce is to take action following a confirmed hit. For example, a parking officer can enforce a scofflaw violation (unpaid parking tickets) by placing a wheel boot on the vehicle.

entity

Entities are the basic building blocks of Security Center. Everything that requires configuration is represented by an entity. An entity can represent a physical device, such as a camera or a door, or an abstract concept, such as an alarm, a schedule, a user, a role, a plugin, or an add-on.

entity tree

An entity tree is the graphical representation of Security Center entities in a tree structure, illustrating the hierarchical nature of their relationships.

event

An event indicates the occurrence of an activity or incident, such as access denied to a cardholder or motion detected on a camera. Events are automatically logged in Security Center, and can be programmed to trigger actions. Every event mainly focuses on one entity, called the event source.

event-to-action

An event-to-action links an action to an event. For example, you can configure Security Center to trigger an alarm when a door is forced open.

expansion server

An expansion server is any server machine in a Security Center system that does not host the Directory role. The purpose of the expansion server is to add to the processing power of the system.

F

failover

Failover is a backup operational mode in which a role (system function) is automatically transferred from its primary server to a secondary server that is on standby. This transfer between servers occurs only if the primary server becomes unavailable, either through failure or through scheduled downtime.

false positive read

False positive plate reads can occur when a license plate recognition system mistakes other objects in an image for license plates. For example, lettering on a vehicle or street signs can sometimes create false positive plate reads.

federated entity	A federated entity is any entity that is imported from an independent system through one of the Federation™ roles.
federated system	A federated system is a independent system (Omnicast™ or Security Center) that is unified under your local Security Center via a Federation™ role, so that the local users can view and control its entities, as if they belong to the local system.
Federation™	The Federation™ feature joins multiple, independent Genetec™ IP security 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.
G	
Genetec Motoscan™	Designed to help increase parking enforcement efficiency in cities with narrow streets, Genetec Motoscan™ is a lightweight, low-power, yet fully-featured license plate recognition unit that is designed to be easily mounted on a smaller vehicle such as a scooter or small motorcycle.
Genetec™ Server	Genetec™ Server is the Windows service that is at the core of Security Center architecture, and that must be installed on every computer that is part of the Security Center's pool of servers. Every such server is a generic computing resource capable of taking on any role (set of functions) you assign to it.
geocoding	Geocoding is the process of finding associated geographic coordinates (latitude and longitude) from a street address.
georeferencing	Georeferencing is the process of using an object's geographic coordinates (latitude and longitude) to determine its position on a map.
ghost Patroller	A ghost Patroller is an entity automatically created by the LPR Manager when the AutoVu™ license includes the XML Import module. In Security Center, all LPR data must be associated to a Patroller entity or an LPR unit corresponding to a fixed Sharp camera. When you import LPR data from an external source via a specific LPR Manager using the XML Import module, the system uses the ghost entity to represent the LPR data source. You can formulate queries using the ghost entity as you would with a normal entity.
Geographic Information System	Geographic Information System (GIS) is a system that captures spatial geographical data. Map Manager can connect to third-party vendors that provide GIS services in order to bring maps and all types of geographically referenced data to Security Center.

H

Hardware inventory	Hardware inventory is a type of maintenance task that reports on the characteristics (unit model, firmware version, IP address, time zone, and so on) of access control, video, intrusion detection, and LPR units in your system.
hash function	In cryptography, a hash function uses a mathematical algorithm to take input data and return a fixed-size alphanumeric string. A hash function is designed to be a one-way function, that is, a function which is infeasible to revert.
hit	A hit is a license plate read that matches a hit rule, such as a hotlist, overtime rule, permit, or permit restriction. A Patroller user can choose to reject or accept a hit. An accepted hit can subsequently be enforced.
hit rule	Hit rule is a type of LPR rule used to identify vehicles of interest (called "hits") using license plate reads. The hit rules include the following types: hotlist, overtime rule, permit, and permit restriction.
Hits	Hits is a type of investigation task that reports on hits reported within a selected time range and geographic area.
hot action	A hot action is an action mapped to a PC keyboard function key (Ctrl+F1 through Ctrl+F12) in Security Desk for quick access.
hotlist	A hotlist is a type of entity that defines a list of wanted vehicles, where each vehicle is identified by a license plate number, the issuing state, and the reason why the vehicle is wanted (stolen, wanted felon, Amber alert, VIP, and so on). Optional vehicle information might include the model, the color, and the vehicle identification number (VIN).
Hotlist and permit editor	Hotlist and permit editor is a type of operation task used to edit an existing hotlist or permit list. A new list cannot be created with this task, but after an existing list has been added to Security Center, users can edit, add, or delete items from the list, and the original text file is updated with the changes.

I

illuminator	An illuminator is a light in the Sharp unit that illuminates the plate, thereby improving the accuracy of the images produced by the LPR camera.
inactive entity	An inactive entity is an entity that is shaded in red in the entity browser. It signals that the real world entity it represents is either not working, offline, or incorrectly configured.
incident	An incident is an unexpected event reported by a Security Desk user. Incident reports can use formatted text and include events and entities as support material.

Incidents	Incidents is a type of investigation task that allows you to search, review, and modify incident reports.
Inventory report	Inventory report is a type of investigation task that allows you to view a specific inventory (vehicle location, vehicle length of stay, and so on) or compare two inventories of a selected parking facility (vehicles added, vehicles removed, and so on).
I/O linking	I/O (input/output) linking is controlling an output relay based on the combined state (normal, active, or trouble) of a group of monitored inputs. A standard application is to sound a buzzer (through an output relay) when any window on the ground floor of a building is shattered (assuming that each window is monitored by a "glass break" sensor connected to an input).
IPv4	IPv4 is the first generation Internet protocol using a 32-bit address space.
IPv6	IPv6 is a 128-bit Internet protocol that uses eight groups of four hexadecimal digits for address space.
L	
Law Enforcement	Law Enforcement is a Patroller software installation that is configured for law enforcement: the matching of license plate reads against lists of wanted license plates (hotlists). The use of maps is optional.
license key	A license key is the software key used to unlock the Security Center software. The license key is specifically generated for each computer where the Directory role is installed. To obtain your license key, you need the <i>System ID</i> (which identifies your system) and the <i>Validation key</i> (which identifies your computer).
license plate inventory	A license plate inventory is a list of license plate numbers of vehicles found in a parking facility within a given time period, showing where each vehicle is parked (sector and row).
license plate read	A license plate read is a license plate number captured from a video image using LPR technology.
License Plate Recognition	License Plate Recognition (LPR) is an image processing technology used to read license plate numbers. License Plate Recognition (LPR) converts license plate numbers cropped from camera images into a database searchable format.
live hit	A live hit is a hit matched by the Patroller and immediately sent to the Security Center over a wireless network.
live read	A live read is a license plate captured by the Patroller and immediately sent to the Security Center over a wireless network.

load balancing	Load balancing is the distribution of workload across multiple computers.
logical ID	Logical ID is a unique ID assigned to each entity in the system for ease of reference. Logical IDs are only unique within a particular entity type.
Logons per Patroller	Logons is a type of investigation task that reports on the logon records of a selected Patroller.
long term	Long term is a type of parking regulation characterizing an overtime rule. The <i>long term</i> regulation uses the same principle as the <i>same position</i> regulation, but the parking period is over 24 hours. No more than one overtime rule may use the long term regulation in the entire system.
LPR camera	A LPR camera is a camera connected to an LPR unit that produces high resolution close-up images of license plates.
LPR Manager	LPR Manager is a role that manages and controls Patrollers, Sharp units, and parking zones. The LPR Manager stores the LPR data (reads, hits, timestamps, GPS coordinates, and so on) collected by the devices and generated by the system in a database for reporting. Images, however, are stored and managed by a separate Archiver role. The LPR Manager is also responsible for updating fixed Sharps and Patrollers in the field with hotfixes, hotlist updates, and so on.
LPR rule	LPR rule is a method used by Security Center and AutoVu™ for processing a license plate read. An LPR rule can be a hit rule or a parking facility.
LPR unit	A LPR unit is a type of entity that represents a hardware device dedicated to the capture of license plate numbers. An LPR unit is typically connected to an LPR camera and a context camera. These cameras can be incorporated to the unit or external to the unit.
M	
macro	A macro is a type of entity that encapsulates a C# program that adds custom functionalities to Security Center.
main server	Main server is the only server in a Security Center system hosting the Directory role. All other servers on the system must connect to the main server in order to be part of the same system. In an high availability configuration where multiple servers host the Directory role, it is the only server that can write to the Directory database.
manual capture	Manual capture is when license plate information is entered into the system by the user and not by the LPR.

Map Generator	Map Generator is a Map Server module that imports raster and vector maps to Plan Manager database.
map link	A map link is a map object that brings you to another map with a single click.
map mode	Map mode is a Security Desk canvas operating mode where the main area of the canvas is used to display a geographical map, with all the active, georeferenced events in your system.
map object	Map objects are graphical representations of Security Center entities or any geographical feature (cities, highways, rivers, and so on) on your maps. With map objects, you can interact with your system without leaving your map.
Map Server	Map Server is a Plan Manager Server module that manages the private maps imported by the Plan Manager administrator. Map Server includes two modules: Map Generator and Tile Server.
map view	A map view is a defined section of a map.
Mobile Admin	Mobile Admin is a web-based administration tool used to configure the Mobile Server.
Mobile app	Mobile app is the client component of Security Center Mobile installed on mobile devices. Mobile app users connect to Mobile Server to receive alarms, view live video streams, view the status of doors, and more, from Security Center.
Mobile Data Computer	Mobile Data Computer is a tablet computer or ruggedized laptop used in patrol vehicles to run the AutoVu™ Patroller application. The MDC is typically equipped with a touch-screen with a minimum resolution of 800 x 600 pixels and wireless networking capability.
Mobile License Plate Inventory	Mobile License Plate Inventory is the Patroller software installation that is configured for collecting license plates and other vehicle information for creating and maintaining a license plate inventory for a large parking area or parking garage.
Mobile Server	Mobile Server is the server component of Security Center Mobile that connects Mobile apps and Web Clients to Security Center, and synchronizes the data and video between Security Center and supported Mobile client components.
Monitoring	The <i>Monitoring</i> task is a type of operation task that you can use to monitor and respond to real-time events that relate to selected entities. Using the <i>Monitoring</i> task, you can also monitor and respond to alarms.

Move unit Move unit tool is used to move units from one manager role to another. The move preserves all unit configurations and data. After the move, the new manager immediately takes on the command and control function of the unit, while the old manager continues to manage the unit data collected before the move.

N

Navigator box The Navigator box is a proprietary in-vehicle device of Genetec Inc. that provides GPS coordinates and odometer readings to Patroller. Because it taps into the vehicle's odometry signal, it is more accurate than a standard GPS device. The Navigator box can be used with any type of AutoVu™ mobile deployment that requires positioning information, but it is required for City Parking Enforcement with Wheel Imaging.

network The network entity is used to capture the characteristics of the networks used by your system so that proper stream routing decisions can be made.

network address translation Network address translation is the process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device, for the purpose of remapping one IP address space into another.

network view The network view is a browser view that illustrates your network environment by showing each server under the network they belong to.

new wanted A new wanted is a manually entered hotlist item in Patroller. When you are looking for a plate that does not appear in the hotlists loaded in the Patroller, you can enter the plate in order to raise a hit if the plate is captured.

notification tray The notification tray contains icons that allow quick access to certain system features, and also displays indicators for system events and status information. The notification tray display settings are saved as part of your user profile and apply to both Security Desk and Config Tool.

O

OCR equivalence OCR equivalence is the interpretation of OCR (Optical Character Recognition) equivalent characters performed during license plate recognition. OCR equivalent characters are visually similar, depending on the plate's font. For example, the letter "O" and the number "0", or the number "5" and the letter "S". There are several pre-defined OCR equivalent characters for different languages.

output behavior	An output behavior is a type of entity that defines a custom output signal format, such as a pulse with a delay and duration.
overtime rule	An overtime rule is a type of entity that defines a parking time limit and the maximum number of violations enforceable within a single day. Overtime rules are used in city and university parking enforcement. For university parking, an overtime rule also defines the parking area where these restrictions apply.
P	
parking facility	A parking facility is a type of entity that defines a large parking area as a number of sectors and rows for the purpose of inventory tracking.
parking lot	A parking lot is a polygon that defines the location and shape of a parking area on a map. By defining the number of parking spaces inside the parking lot, Security Center can calculate its percentage of occupancy during a given time period.
parking zone	The parking zones that you define in Security Center represent off-street parking lots where the entrances and exits are monitored by Sharp cameras.
partition	A partition is a type of entity that defines a set of entities that are only visible to a specific group of users. For example, a partition could include all areas, doors, cameras, and zones in one building.
partition administrator	(Obsolete) Beginning in Security Center 5.7 GA, privileges that used to be exclusive to administrators can now be granted individually, making the concept of <i>partition administrator</i> obsolete.
Patroller	<ol style="list-style-type: none"> 1 Patroller is the AutoVu™ software application installed on an in-vehicle computer. Patroller connects to Security Center and is controlled by the LPR Manager. Patroller verifies license plates read from LPR cameras against lists of vehicles of interest (hotlists) and vehicles with permits (permit lists). It also collects data for time-limited parking enforcement. Patroller alerts you of hotlist or permit hits so that you can take immediate action. 2 Type of entity that represents a patrol vehicle equipped with the Patroller software.
Patroller Config Tool	Patroller Config Tool is the Patroller administrative application used to configure Patroller-specific settings, such as adding Sharp cameras to the in-vehicle LAN, enabling features such

	as Manual Capture or New Wanted, and specifying that a username and password are needed to log on to Patroller.
Patroller tracking	Patroller tracking is a type of investigation task that allows you to replay the route followed by a patrol vehicle on a given date on a map, or view the current location of patrol vehicles on a map.
permit	A permit is a type of entity that defines a single parking permit holder list. Each permit holder is characterized by a category (permit zone), a license plate number, a license issuing state, and optionally, a permit validity range (effective date and expiry date). Permits are used in both city and university parking enforcement.
permit hit	A permit hit is a hit that is generated when a read (license plate number) does not match any entry in a permit or when it matches an invalid permit.
permit restriction	A permit restriction is a type of entity that applies time restrictions to a series of parking permits for a given parking area. Permit restrictions are only used by AutoVu™ Patrollers configured for University Parking Enforcement.
Plate Reader	Plate Reader is the software component of the Sharp unit that processes the images captured by the LPR camera to produce license plate reads, and associates each license plate read with a context image captured by the context camera. The Plate Reader also handles the communications with the Patroller and the LPR Manager. If an external wheel imaging camera is connected to the Sharp unit, the Plate Reader also captures wheel images from this camera.
plugin	A plugin is a software module that adds a specific feature or service to a larger system.
Plugin	Plugin is a role template that serves to create specific plugin roles.
primary server	Primary server is the default server chosen to perform a specific function (or role) in the system. To increase the system's fault-tolerance, the primary server can be protected by a secondary server on standby. When the primary server becomes unavailable, the secondary server automatically takes over.
private IP address	A private IP address is an IP address chosen from a range of addresses that are only valid for use on a LAN. The ranges for a private IP address are: 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.16.255.255, and 192.168.0.0 to 192.168.255.255. Routers on the Internet are normally configured to discard any traffic using private IP addresses.

private task	A private task is a saved task that is only visible to the user who created it.
privilege	Privileges define what users can do, such as arming zones, blocking cameras, and unlocking doors, over the part of the system they have access rights to.
public task	A public task is a saved task that can be shared and reused among multiple Security Center users.
R	
read rate	The read rate measures the speed at which a license plate recognition system can correctly detect and read all of the characters in an image of a license plate.
Reads	Reads is a type of investigation task that reports on license plate reads performed within a selected time range and geographic area.
Reads/hits per day	Reads/hits per day is a type of investigation task that reports on license plate reads performed within a selected time range and geographic area.
Reads/hits per zone	Reads/hits per zone is a type of investigation task that reports on the number of reads and hits per parking area for a selected date range.
Report Manager	Report Manager is a type of role that automates report emailing and printing based on schedules.
report pane	Report pane is one of the panes found in the Security Desk task workspace. It displays query results or real-time events in a tabular form.
reverse geocoding	Reverse geocoding is an AutoVu™ feature that translates a pair of latitude and longitude into a readable street address.
role	A role is a software module that performs a specific job within Security Center. To execute a role, you must assign one or more servers to host it.
S	
salt (cryptography)	In cryptography, a salt is data that is used as an additional input to the information you want to encrypt or protect with a hash function, so that the original information is nearly impossible to guess, even when the attacker knows what algorithm is being used.
same position	Same position is a type of parking regulation characterizing an overtime rule. A vehicle is in violation if it is seen parked at the exact same spot over a specified period of time. Patroller must

be equipped with GPS capability in order to enforce this type of regulation.

schedule	A schedule is a type of entity that defines a set of time constraints that can be applied to a multitude of situations in the system. Each time constraint is defined by a date coverage (daily, weekly, ordinal, or specific) and a time coverage (all day, fixed range, daytime, and nighttime).
scheduled task	A scheduled task is a type of entity that defines an action that executes automatically on a specific date and time, or according to a recurring schedule.
Software Development Kit	The Software Development Kit (SDK) allows end-users to develop custom applications or custom application extensions for Security Center.
secondary server	A secondary server is any alternate server on standby intended to replace the primary server in the case the latter becomes unavailable.
Security Center	Security Center is a truly unified platform that blends IP video surveillance, access control, license plate recognition, intrusion detection, and communications within one intuitive and modular solution. By taking advantage of a unified approach to security, your organization becomes more efficient, makes better decisions, and responds to situations and threats with greater confidence.
Security Center Federation™	The Security Center Federation™ role connects a remote, independent Security Center system to your local Security Center. That way, the remote system's entities and events can be used in your local system.
Security Center Mobile	Security Center Mobile is a feature of the Genetec Inc. unified platform that you can use to remotely connect to your Security Center system over a wireless IP network. Supported Mobile client components include a unified Web Client that is platform-independent, as well as various Mobile apps for smartphones and tablets.
Security Desk	Security Desk is the unified user interface of Security Center. It provides consistent operator flow across all of the Security Center's main systems, Omnicast™, Synergis™, and AutoVu™. Security Desk's unique task-based design lets operators efficiently control and monitor multiple security and public safety applications.
server	A server is a type of entity that represents a server machine on which the Genetec™ Server service is installed.
Server Admin	Server Admin is the web application running on every server machine in Security Center that allows you to configure the

settings of Genetec Server. Server Admin also allows you to configure the Directory role on the main server.

Sharp EX

Sharp EX is the Sharp unit that includes an integrated image processor and supports two standard definition NTSC or PAL inputs for external cameras (LPR and context cameras).

SharpOS

SharpOS is the software component of a Sharp or SharpX unit. SharpOS is responsible for everything related to plate capture, collection, processing, and analytics. For example, a SharpOS update can include new LPR contexts, new firmware, Sharp Portal updates, and updates to the Sharp's Windows services (Plate Reader, HAL, updater service, and so on).

Sharp Portal

Sharp Portal is a web-based administration tool used to configure Sharp cameras for fixed or mobile AutoVu™ systems. From a web browser, you log on to a specific IP address (or the Sharp name in certain cases) that corresponds to the Sharp you want to configure. When you log on, you can configure options such as selecting the LPR context (e.g. Alabama, Oregon, Quebec, etc), selecting the read strategy (e.g. fast moving or slow moving vehicles), viewing the Sharp's live video feed, and more.

Sharp unit

The Sharp unit is a proprietary LPR unit of Genetec Inc. that integrates license plate capturing and processing components, as well as digital video processing functions, inside a ruggedized casing.

Sharp VGA

Sharp VGA is a Sharp unit that integrates the following components: an infrared illuminator; a standard definition (640 x 480) LPR camera for plate capture; an integrated image processor; an NTSC or PAL color context camera with video streaming capabilities.

SharpX

SharpX is the camera component of the SharpX system. The SharpX camera unit integrates a pulsed LED illuminator that works in total darkness (0 lux), a monochrome LPR camera (1024 x 946 @ 30 fps), and a color context camera (640 x 480 @ 30 fps). The LPR data captured by the SharpX camera unit is processed by a separate hardware component called the AutoVu™ LPR Processing Unit.

Sharp XGA

Sharp XGA is a Sharp unit that integrates the following components: an infrared illuminator; a high-definition (1024 x 768) LPR camera for plate capture; an integrated image processor; an NTSC or PAL color context camera with video streaming capabilities and optional internal GPS.

SharpX VGA

SharpX VGA is the camera component of the SharpX system. The SharpX VGA camera unit integrates a pulsed LED illuminator that works in total darkness (0 lux), a monochrome

LPR camera (640 x 480 @ 30 fps), and a color context camera (640 x 480 @ 30 fps). The LPR data captured by the SharpX VGA camera unit is processed by a separate hardware component called the AutoVu™ LPR Processing Unit.

standard schedule

A standard schedule is a type of schedule entity that may be used in all situations. Its only limitation is that it does not support daytime or nighttime coverage.

system event

A system event is a predefined event that indicates the occurrence of an activity or incident. System events are defined by the system and cannot be renamed or deleted.

System status

System status is a type of maintenance task that monitors the status of all entities of a given type in real time, and allows you to interact with them.

T

task

A task is the central concept on which the entire Security Center user interface is built. Each task corresponds to one aspect of your work as a security professional. For example, use a monitoring task to monitor system events in real-time, use an investigation task to discover suspicious activity patterns, or use an administration task to configure your system. All tasks can be customized and multiple tasks can be carried out simultaneously.

taskbar

A taskbar is a user interface element of the Security Center client application window, composed of the Home tab and the active task list. The taskbar can be configured to appear on any edge of the application window.

task workspace

A task workspace is an area in the Security Center client application window reserved for the current task. The workspace is typically divided into the following panes: canvas, report pane, dashboard, and Logical view.

tile

A tile is an individual window within the canvas, used to display a single entity. The entity displayed is typically the video from a camera, a map, or anything of a graphical nature. The look and feel of the tile depends on the displayed entity.

tile ID

The tile ID is the number displayed at the upper left corner of the tile. This number uniquely identifies each tile within the canvas.

tile mode

Tile mode is the Security Desk canvas operating mode where the main area of the canvas is used to display the tiles and the dashboard.

tile pattern

The tile pattern is the arrangement of tiles within the canvas.

tile plugin	A tile plugin is a type of entity that represents an application that runs inside a Security Desk tile.
Tile Server	Tile Server is the Map Server module that answers the map requests issued from Plan Manager Client.
timeline	A timeline is a graphic illustration of a video sequence, showing where in time, motion, and bookmarks are found. Thumbnails can also be added to the timeline to help the user select the segment of interest.
U	
unit	<p>A unit is a hardware device that communicates over an IP network that can be directly controlled by a Security Center role. We distinguish four types of units in Security Center:</p> <ul style="list-style-type: none"> • Access control units, managed by the Access Manager role • Video units, managed by the Archiver role • LPR units, managed by the LPR Manager role • Intrusion detection units, managed by the Intrusion Manager role
Unit discovery tool	Starting with Security Center 5.4 GA the Unit discovery tool has been replaced by the Unit enrollment tool.
Unit replacement	Unit replacement is a tool that is used to replace a failed hardware device with a compatible one, while ensuring that the data associated to the old unit gets transferred to the new one. For an access control unit, the configuration of the old unit is copied to the new unit. For a video unit, the video archive associated to the old unit is now associated to the new unit, but the unit configuration is not copied.
University Parking Enforcement	University Parking Enforcement is a Patroller software installation that is configured for university parking enforcement: the enforcement of scheduled parking permits or overtime restrictions. The use of maps is mandatory. Hotlist functionality is also included.
unreconciled read	A unreconciled read is a MLPI license plate read that has not been committed to an inventory.
user	A user is a type of entity that identifies a person who uses Security Center applications and defines the rights and privileges that person has on the system. Users can be created manually or imported from an Active Directory.
user group	A user group is a type of entity that defines a group of users who share common properties and privileges. By becoming member of a group, a user automatically inherits all the

properties of the group. A user can be a member of multiple user groups. User groups can also be nested.

user level

A user level is a numeric value assigned to users to restrict their ability to perform certain operations, such as controlling a camera PTZ, viewing the video feed from a camera, or staying logged on when a threat level is set. Level 1 is the highest user level, with the most privileges.

V

validation key

A validation key is a serial number uniquely identifying a computer that must be provided to obtain the license key.

vehicle identification number

A vehicle identification number (VIN) is an identification number that a manufacturer assigns to vehicles. This is usually visible from outside the vehicle as a small plate on the dashboard. A VIN can be included as additional information with license plate entries in a hotlist or permit list, to further validate a hit and ensure that it is the correct vehicle.

W

Web Client

You can log on to Security Center Web Client from your Internet browser to monitor video, investigate events related to door activity, search for and investigate active and past alarms, view and manage cardholders, visitors, cardholder groups, and credentials. Your system administrator must create a Web Client Server role in Security Center, which defines the Web Client's address (URL).

Web Map Service

Web Map Service (WMS) is a standard protocol for serving georeferenced map images over the Internet that are generated by a map server using data from a GIS database.

wheel imaging

Wheel imaging is a virtual tire-chalking technology that takes images of the wheels of vehicles to prove whether they have moved between two license plate reads.

widget

A widget is a component of the graphical user interface (GUI) with which the user interacts.

Windows Communication Foundation

Windows Communication Foundation (WCF) is a communication architecture used to enable applications, in one machine or across multiple machines connected by a network, to communicate. AutoVu™ Patroller uses WCF to communicate wirelessly with Security Center.

Z

Zone occupancy

Zone occupancy is a type of investigation task that reports on the number of vehicles parked in a selected parking area, and the percentage of occupancy.

Where to find product information

You can find our product documentation in the following locations:

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

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

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

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

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

Additional resources

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

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

Licensing

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

Hardware product issues and defects

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