AutoVu Handbook 5.2 SR10

Click here for the most recent version of this guide.

Genetec

Copyright notice

Document information

Document title: AutoVu Handbook 5.2 SR10

Document number: EN.400.003-V5.2.C10(1)

Document update date: February 27, 2015

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 how to install and configure an AutoVu system.

You'll still need to refer to the *Security Center Administrator Guide* from time to time. For example, this guide does not explain how to manage partitions or databases, since these topics are also required for the other Security Center products (video and access control).

This guide assumes you are familiar with Security Center 5.2 systems.

This guide is organized into the following sections:

- Part I, "About AutoVu" on page 1

  This part includes overviews of the hardware and software components that make up an AutoVu system, and explains the key concepts required to understand how AutoVu works. This part also includes user interface overviews of the different software applications required to configure AutoVu.

- Part II, "Deployment overviews" on page 42

  This part includes process overviews (roadmaps) for fixed and mobile AutoVu systems. The roadmaps guide you through the different tasks you need to perform to successfully deploy an AutoVu system.

- Part III, "Hardware installation" on page 51

  This part explains how to install AutoVu Sharp cameras and their related components in a fixed or mobile configuration.

- Part IV, "Software installation and upgrade" on page 85

  This part explains how to install and upgrade the different AutoVu software components: Security Center, Patroller, and Sharp camera firmware.

- Part V, "Software configuration" on page 115

  This part explains the software-related procedures required to configure a fixed or mobile AutoVu system. It includes general configuration tasks that apply to all types of AutoVu systems, as well as the additional tasks you'll need to configure for your specific AutoVu installation type (e.g. Law Enforcement, City Parking Enforcement, etc).

- Part VI, "Interface references" on page 266

  This part describes the buttons and options in the three applications you use to configure an AutoVu system: Security Center Config Tool, Patroller Config Tool, and the Sharp Portal.

- Part VII, "Appendices" on page 387

  This part provides additional information which is not directly related to AutoVu installation or configuration, but that can be useful in AutoVu system maintenance.

Notes and notices

The following notes and notices might appear in this guide:

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

Contents

Chapter 2: AutoVu software interface tours

Part II: Deployment overviews

Chapter 3: Deploying fixed AutoVu systems

Chapter 4: Deploying mobile AutoVu systems

Part IV: Software installation and upgrade

Chapter 9: Installing Security Center

Chapter 10: Installing AutoVu Patroller

Chapter 11: Upgrading AutoVu

Part V: Software configuration

Chapter 12: General AutoVu configuration

Chapter 13: Additional configuration for AutoVu fixed systems

Chapter 14: General AutoVu mobile configuration

Chapter 15: Additional configuration for AutoVu Law Enforcement systems

Chapter 16: Additional configuration for AutoVu City and University Parking Enforcement systems

Chapter 17: Additional configuration for Mobile License Plate Inventory (MLPI) systems

Part VI: Interface references

Chapter 18: Security Center Config Tool reference

Chapter 19: Patroller Config Tool reference

Chapter 20: Sharp Portal reference

Part I

About AutoVu

This part includes overviews of the hardware and software components that make up an AutoVu system, and explains the key concepts required to understand how AutoVu works. This part also includes user interface overviews of the different software applications required to configure AutoVu.

This part includes the following chapters:

1

Introducing AutoVu

This section describes the main features and components of AutoVu, the IP license plate recognition (LPR) solution of Security Center.

This section includes the following topics:

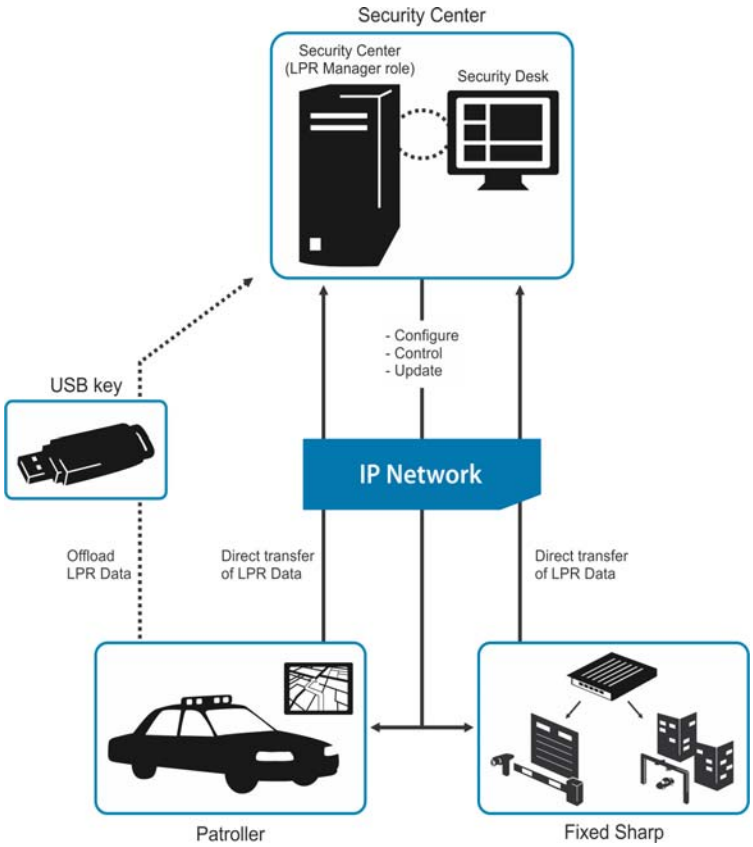
What is AutoVu?

AutoVu™ is the IP license plate recognition (LPR) system of Security Center that automates the reading and verification of vehicle license plates.

AutoVu Sharp cameras capture license plate images, and send the data to 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 (e.g. on a pole in a parking lot), or in a mobile configuration (e.g. on a police car).

Depending on the license purchased, you can use AutoVu for scofflaw and wanted vehicle identification, city-wide surveillance, time-limited parking enforcement, parking permit control, vehicle inventory, security, and access control.

The following diagram shows how a typical AutoVu system works.



AutoVu hardware components

The AutoVu Sharp and SharpX are the IP-based license plate recognition cameras that capture vehicle plates.

This section includes the following topics:

AutoVu Sharp components

The AutoVu Sharp is typically used for fixed installations, but it can also be used for mobile installations. It comes in the following models:

- **Sharp XGA.** Sharp unit that integrates a pulsed LED illuminator for effective use in 0 lux (total darkness) environments, 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.
- **Sharp VGA.** Same as the Sharp XGA, except with a standard definition (640 x 480) LPR camera for plate capture and no internal GPS.

For more information, see the AutoVu Sharp specification sheet available on the Genetec website.

AutoVu SharpX components

The AutoVu SharpX is typically used for mobile installations, but it can also be used for fixed installations. Unlike the Sharp, the SharpX system separates the capture and processing functionality into two components:

- **SharpX camera unit.** Camera component of the SharpX system (sometimes referred to as the "SharpX XGA"). 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.
- **SharpX VGA camera unit.** Same as the SharpX, except with a standard definition (640 x 480) LPR camera for plate capture.

- **AutoVu LPR Processing Unit.** Processing component of the SharpX system. The LPR Processing Unit is available with two or four camera ports. In mobile installations, the LPR Processing Unit is sometimes referred to as the "trunk unit" because it is typically installed in the vehicle's trunk.

  For more information, see the AutoVu SharpX specification sheet available on the Genetec website.

Ruggedized touchscreen PC

The in-vehicle computer used in AutoVu mobile systems to run the Patroller application. The model currently used for typical AutoVu installations is the Panasonic Toughbook. You can use another computer if you choose, but it must have touchscreen capability.

AutoVu software components

There are several software components you'll need to install, upgrade, and configure to deploy an AutoVu system.

- **Security Center.** The "parent" application that you use to configure and manage an AutoVu system. Security Center also stores all the LPR data collected from Patrollers or fixed Sharp units. You configure Security Center using Security Center Config Tool (Config Tool).

  For more information, see "What is Security Center?" on page 6.
- **Patroller.** The software application installed on an in-vehicle computer that sends LPR data to Security Center.

  For more information, see "What is Patroller?" on page 6.
- **Patroller Config Tool.** The administrative application used to configure Patroller-specific settings.

  For more information, see "What is Patroller Config Tool?" on page 7.
- **Sharp Portal.** The web-based administrative application used to configure Sharp units.

  For more information, see "What is the Sharp Portal?" on page 7.

What is Security Center?

Security Center is the unified security platform that seamlessly blends Genetec's IP security and safety systems within a single innovative solution. The systems unified under Security Center include Genetec's Omnicast IP video surveillance system, Synergis IP access control system, and AutoVu IP license plate recognition (LPR) system.

AutoVu Sharp and Patroller components are integrated with Security Center to provide advanced data mining and reporting through the Security Desk user interface. You can use Security Desk to generate a variety of LPR reports. You filter query results based on date, time, patrolling unit, hotlist, type of hit, area, and much more.

With GPS correlation, a GPS location is marked in Security Desk for each Patroller in the field, and each license plate read. Therefore, when you monitor live incoming reads and hits in Security Desk, you'll have precise information on where the read or hit took place. With the supported mapping display, Security Desk displays a map with symbols for each read, hit, and vehicle position.

What is Patroller?

Patroller is the AutoVu software application installed on an in-vehicle computer. Patroller connects to Security Center and is controlled by the LPR Manager.

Depending on your AutoVu solution, Patroller can be used to do the following:

- Verify license plates read from LPR cameras against lists of vehicles of interest (hotlists) and vehicles with permits (permit lists).
- Alert you of hotlist or permit hits so that you can take immediate action.
- Collect data for time-limited parking enforcement.
- Collect license plate reads to create and maintain a license plate inventory for a parking facility.

What is Patroller Config Tool?

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.

What is the Sharp Portal?

The web-based administrative application 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.

NOTE To use the Sharp Portal, your Web browser must have the Microsoft Silverlight plugin installed.

How do AutoVu hardware and software components work together?

How the AutoVu hardware and software work together depends on what type of installation you have: fixed or mobile.

This section includes the following topics:

How AutoVu fixed installations work

AutoVu fixed systems have Sharp cameras installed in a stationary position, such as on a pole, or on a gantry overlooking a highway. These Sharp cameras are connected through a network to Security Center for configuration, monitoring, and reporting activities.

Security operators use Security Desk to monitor license plate reads from the Sharp cameras and any associated video from various co-located CCTV cameras. The Sharp cameras send each read to Security Desk in real-time. Reads can optionally be compared to the applicable hotlists and an alarm is triggered if a hit occurs.

How AutoVu mobile installations work

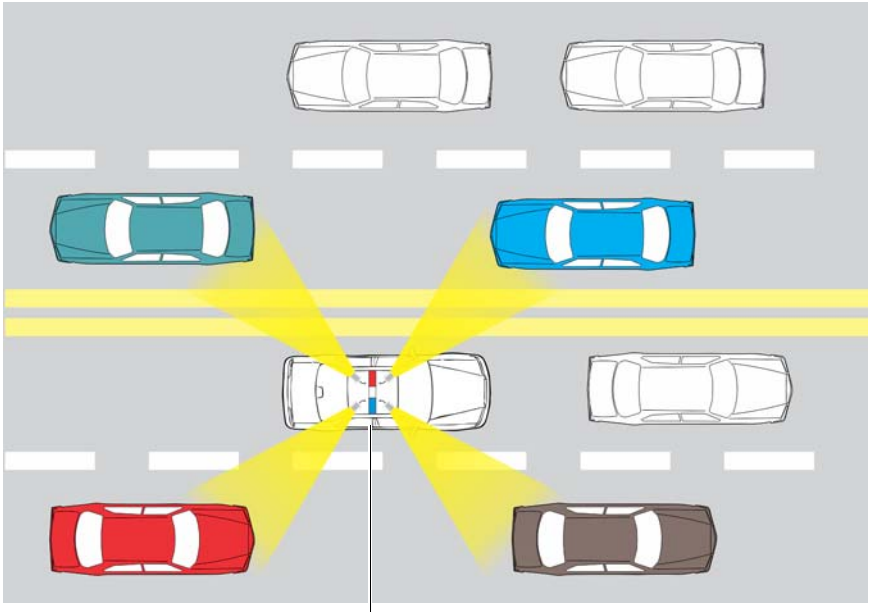
AutoVu mobile systems have Sharp cameras installed on a vehicle, such as on a police cruiser. The Sharp cameras send reads to the Patroller application that is installed on the in-vehicle computer. Patroller compares the reads to loaded hotlists or permit lists and an alarm is triggered if a hit occurs. The Patroller operator (e.g. police officer or parking enforcement officer) can then choose whether or not to enforce the hit.

Patroller data can be offloaded to Security Center in real-time, if the vehicle is equipped with a wireless connection, or at the end of a shift (e.g. using a USB key, or local wireless connection). Security Desk can also display the reads and hits from patrolling units.

Understanding Law Enforcement

In a Law Enforcement installation, Patroller matches license plates against lists of vehicles of interest (hotlists). As you patrol, the Sharp cameras installed on the vehicle automatically read plates and send the information to Patroller. If a plate is on a loaded hotlist, Patroller alerts you, and you can take immediate action. Hotlists typically contain information on stolen vehicles, scofflaw suspects, amber alerts, and so on. The use of in-vehicle mapping with a Law Enforcement installation is optional.

EXAMPLE You can have up to six Sharp cameras installed on a Patroller vehicle. This allows you to capture the maximum number of plates on vehicles in different lanes and even those travelling in the opposite direction. The following diagram shows a Patroller law enforcement vehicle outfitted with four cameras:



Patroller law enforcement vehicle capturing plates on multiple vehicles travelling in different directions.

Understanding City and University Parking Enforcement

This section includes the following topics:

About parking enforcement

In AutoVu parking enforcement, Patroller matches plates on parked vehicles to enforcement rules (overtime rules, permit lists, or permit lists with permit restrictions) created in Security Center. Overtime rules specify *when* and for *how long* vehicles are allowed to park, and permit lists specify *which* vehicles are allowed to park.

Which rules you use, and how you configure them, depends on the type of AutoVu parking enforcement system you have: *City Parking Enforcement* or *University Parking Enforcement*.

NOTE Both City Parking Enforcement and University Parking Enforcement systems support hotlists, which contain information on vehicles of interest (e.g. scofflaw, and stolen vehicles).

This section includes the following topics:

City Parking Enforcement

In City Parking Enforcement, you can use overtime rules alone, permit lists alone, or both together. You can also use wheel imaging to provide additional evidence of whether or not a vehicle has moved. For more information on wheel imaging, see "About wheel imaging" on page 19.

EXAMPLE Here are some examples of when you would use each type of enforcement rule:

- **Overtime rule alone.** To maximise turnover, and avoid free parking abuse in a commercial area, vehicles are allowed to park for only two hours on main streets between 8:00 a.m and 6:00 P.M. Any vehicles parked for more than two hours are in violation of the overtime rule.

This results in an overtime hit in Patroller. In this example, you don't need a permit list because there are no exceptions to the rule.

- **Permit list alone.** Some residential areas allow only permit holders to park on neighborhood streets. Any vehicle parked in the area without a permit is in violation of the permit list. This results in a permit hit in Patroller. In this example, you don't need an overtime rule because there are no time limits. *Any* vehicle parked without a valid permit (e.g. expired permit, no permit at all, etc) is in violation, regardless of the day or time.
- **Overtime rule and permit list together.** Some residential areas allow permit holders to park indefinitely, and non-permit holders to park for a limited time. Any vehicle without a permit, that is parked in the area longer than the limit allows, is in violation of the overtime rule. This results in an overtime hit. In this example, you need both an overtime rule, and a permit list to determine if a parked vehicle is in violation.

University Parking Enforcement

University Parking Enforcement is very similar to City Parking Enforcement in that both use overtime rules and permit lists, but there are some important differences with University Parking Enforcement:

- You apply a permit restriction to one or more permit lists. It is the permit restriction that specifies when and where permits apply.
- You define a parking lot for each overtime rule or permit restriction you create. The parking lot and its associated enforcement rule (overtime rule or permit restriction) is called a "zone". The zone is what appears in Patroller.
- You can enforce overtime rules or permit restrictions for a selected parking lot, but not both at the same time.
- Wheel imaging is not supported.
- You have GPS-assisted parking lot selection in Patroller.

EXAMPLE The following examples show when you would use an overtime rule, and when you would use a permit restriction:

- **Overtime rule.** A university campus has several parking lots reserved for students and faculty, but also has conveniently located parking areas that are used by delivery vehicles for the loading or unloading of equipment.

  Using an overtime rule, you can allow any vehicle to park in the loading area at any time of day, but only for a limited time (e.g. 20 minutes). A vehicle parked over that time is in violation of the overtime rule. This results in an overtime hit in Patroller. In this example, you don't need a permit restriction because *any* vehicle can park, but only for a limited time.
- **Permit restriction.** A university parking lot can be used by both faculty and students, but at different times. Faculty can park on weekdays from 8:00 A.M. to 6:00 P.M., while students can park from 10:00 A.M. to 4:00 P.M. This reserves the prime parking spaces for the university's faculty, but still allows students convenient parking during peak class hours.

You wouldn't be able to create this parking scenario with an overtime rule. You need a permit restriction and associated permit lists. Vehicles without a permit, with an expired permit, or parked at the wrong time, are in violation of the permit restriction. This results in a permit hit in Patroller.

NOTE There is another type of permit hit that is unique to University Parking Enforcement, called a shared permit hit. For more information, see "About shared permits" on page 22.

Types of overtime rules

This section describes the different types of overtime rules (*Same position*, *District*, and *Block face*) and when to use them.

If you have the wheel imaging option installed, it can be used to provide additional evidence of the violation by showing whether or not the vehicle has moved even a small distance. Wheel imaging can be used with any type of overtime rule, but it is most commonly used for *Same position* enforcement. For more information about how wheel imaging works, see "About wheel imaging" on page 19.

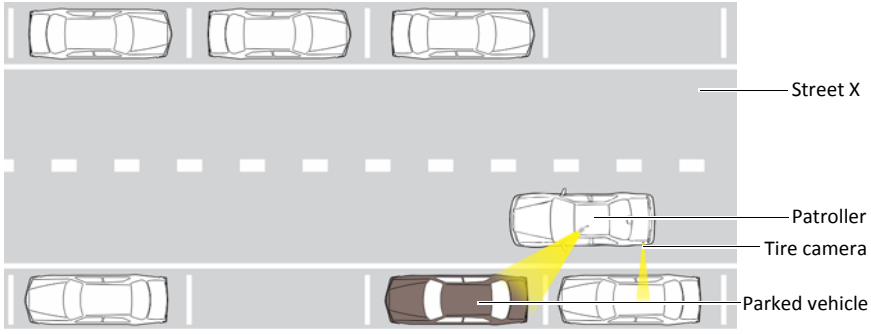
This section includes the following topics:

About Same position overtime rules

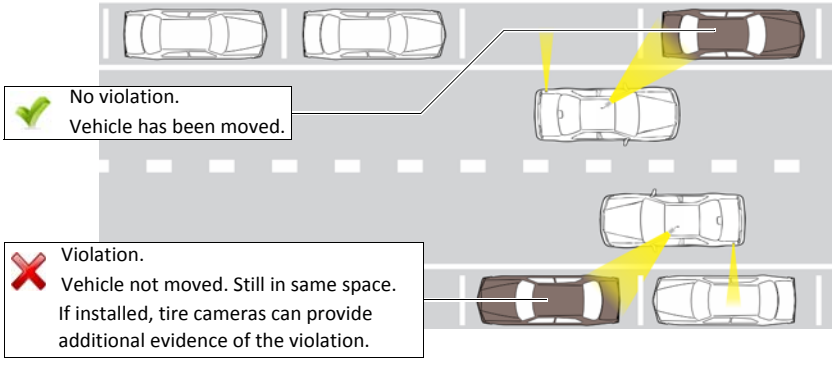
Same position overtime rules specify how long a vehicle is allowed to park in a *single parking space* on a particular street.

EXAMPLE The overtime rule states that vehicles can park for one hour in any parking space on Street X. You do a first pass at 9:00 A.M. collecting license plate reads. You then do a second pass at 10:05 A.M. If Patroller reads the same plate in the same parking space, Patroller generates an overtime hit.

① First pass at 9:00 A.M.
Patroller logs vehicle's position.



② Second pass at 10:05 A.M.
One hour has expired.

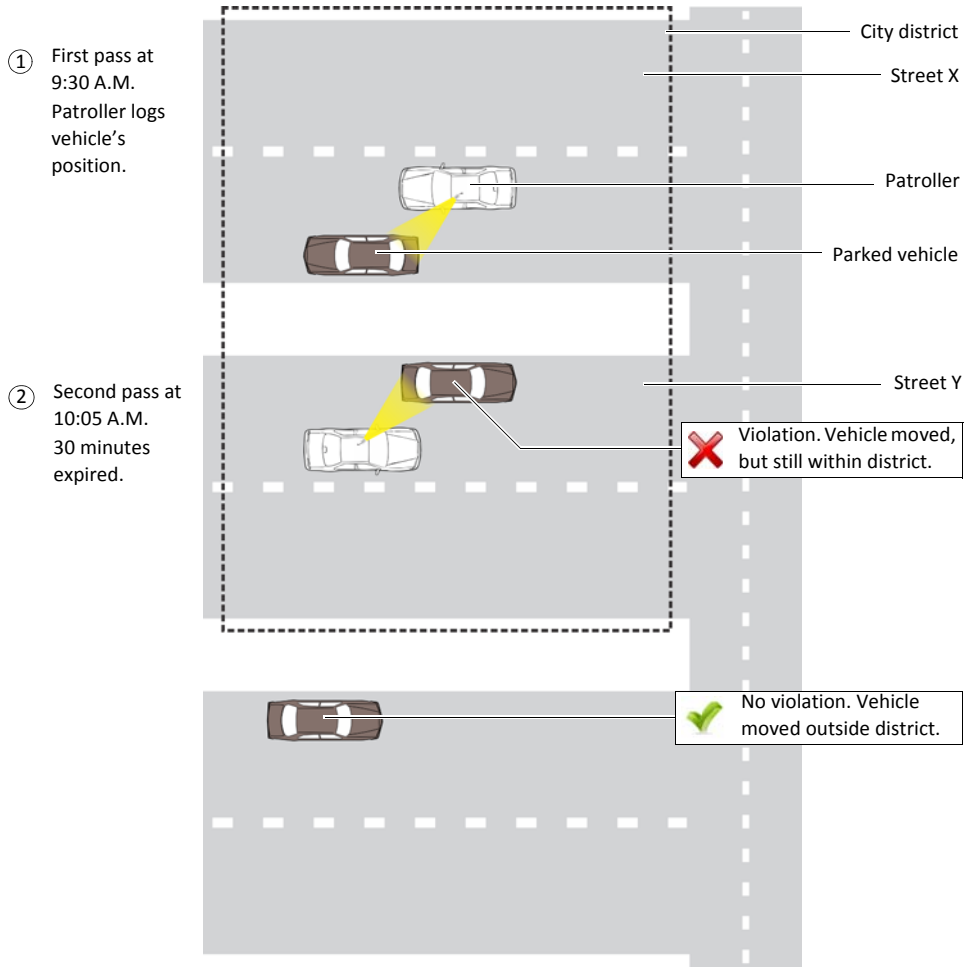


About District overtime rules

District parking enforcement is a type of overtime rule that specifies when a vehicle is allowed to park *within a specific geographic location* (e.g. city district).

The borders of a "district" are not defined in Security Center Config Tool (e.g. by drawing a polygon on a map), and there is no correlation with a city's formal boroughs or municipalities. A district exists whereever the Patroller user chooses to enforce it.

EXAMPLE The overtime rule states that between 9:00 A.M. and 5:00 P.M. on weekdays, vehicles can park for only 30 minutes within the district defined by Street X and Street Y. You do a first pass through the district at 9:30 A.M. collecting license plate reads. You then do a second pass through the district at 10:05 A.M. If Patroller reads the same plate within the same district (regardless if the vehicle has moved or not), the vehicle is in violation of the overtime rule, and you get an overtime hit.

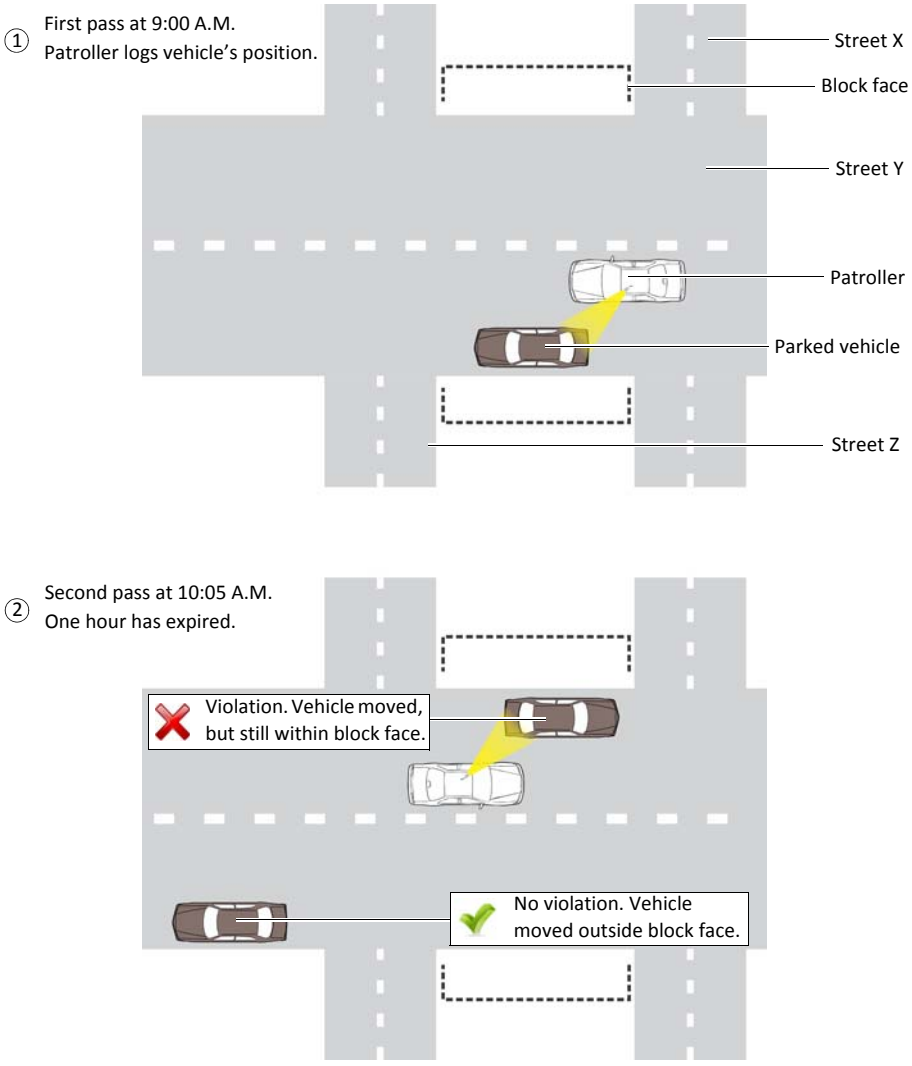


About Block face overtime rules

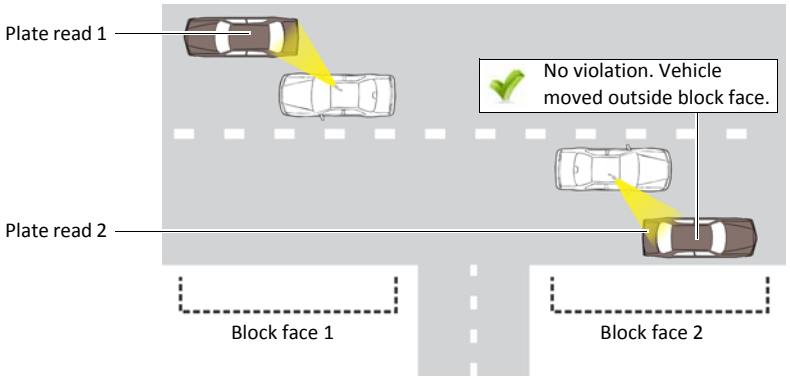
Block face parking enforcement is a type of overtime rule that specifies when a vehicle is allowed to park *on both sides of a street, between intersecting cross-streets*.

The borders of a "block face" are not defined in Security Center Config Tool (e.g. by drawing a polygon on a map). They are defined on the spot for each individual plate read. For example, when a Patroller user selects a block face overtime rule, and then reads a license plate, Patroller uses GPS to determine the block face for that particular plate read based on the intersecting cross-streets closest to the parked vehicle's position.

EXAMPLE The overtime rule states that vehicles can park for one hour on either side of Street Y, between Street X and Street Z. You do a first pass through the block face at 9:00 A.M. collecting license plate reads. You then do a second pass down the block face at 10:05 A.M. If Patroller reads the same plate within the same block face, the vehicle is in violation of the overtime rule, and you get an overtime hit.



NOTE Patroller considers "T intersections" to be valid borders of a block face. For example, in the following scenario, Patroller would **not** raise an overtime hit because the T intersection is seen as the end of *Block face 1*, and the beginning of *Block face 2*.



About multiple violations

You can add multiple violations to any of the three types of overtime rules. This specifies the maximum number of citations that can be issued to the same vehicle for the same overtime offence.

EXAMPLE Here are two examples to explain the difference between having an overtime rule with one violation, and an overtime rule with multiple violations:

- **Overtime rule with one violation.** Your overtime rule allows vehicles to park for one hour on a specific street. If a vehicle is parked in that area longer than an hour, it is in violation of the overtime rule. This results in an overtime hit in Patroller. However, because the overtime rule allows only one violation for the offense, even if the vehicle is parked in the same place all day, you'll only get one overtime hit for it. In this scenario, you would issue one ticket for the offense.
- **Overtime rule with multiple violations.** Your overtime rule allows vehicles to park for one hour on a specific street, but your system is configured to allow multiple violations (e.g. three) of that one hour rule. If a vehicle is parked in that area all day, and you patrol the area three times during your shift, you'll get *three* violations of the overtime rule, and three separate overtime hits in Patroller. In this scenario, you would issue three tickets for the same offense.

Best practice: Multiple violations must be configured so that they overlap. The start time of a violation should be greater than or equal to the start time of the previous violation and the end

time of the violation should be less than or equal to the end time of the previous violation. For example:

Violation #1 = 8:00 - 16:00

Violation #2 = 10:00 - 16:00

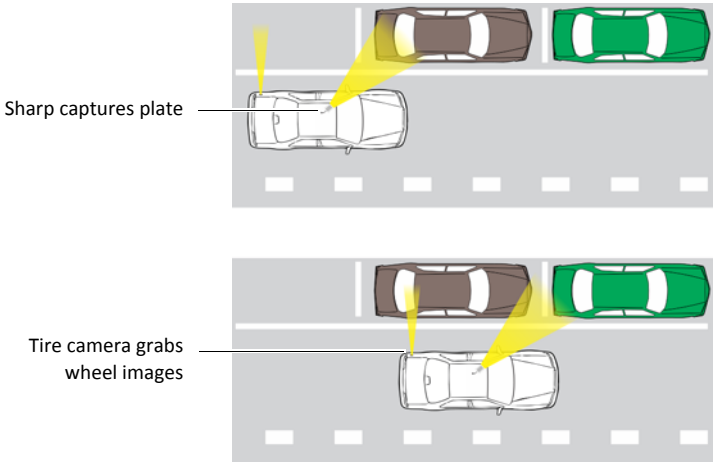
Violation #3 = 10:00 - 13:00

About wheel imaging

In a City Parking Enforcement with Wheel Imaging system, Patroller uses wheel images taken by "tire cameras" as additional evidence of whether or not a parked vehicle has moved even a small distance.

For example, when you get an overtime hit, you can look at the vehicle's wheels and see by the valve stem or other reference point (e.g. crack in the hubcap), that the vehicle hasn't moved. This photographic evidence can help prove the overtime offense if the driver claims to have moved the vehicle, and then parked again in the same area.

EXAMPLE Here is a Patroller vehicle with a Sharp camera and a single tire camera.



NOTE You cannot do wheel imaging on both sides of a street at the same time.

For wheel imaging to be effective, you also need the AutoVu Navigator box. The Navigator box comes with a GPS receiver that receives satellite positioning information, but it also taps into the vehicle's odometer readings and has an internal gyroscope. This provides greater accuracy than GPS alone.

For example, drive through a long tunnel and you'll lose the GPS satellite signal, but the Navigator box still knows how far and how fast you're driving (odometry signal), and if you change direction (gyroscope). The Navigator box is installed in the vehicle, and is connected to the vehicle's odometry signal and in-vehicle computer. Some calibration is required.

About long term overtime

Long term overtime is used for long term parking; that is, where vehicles can park in the same space for over 24 hours. With long term overtime, you can specify a time limit between 2 to 5 days. This option automatically sets the overtime rule category to *same position*, which means that the vehicle is in violation if it is parked in the same parking space beyond the time limit specified.

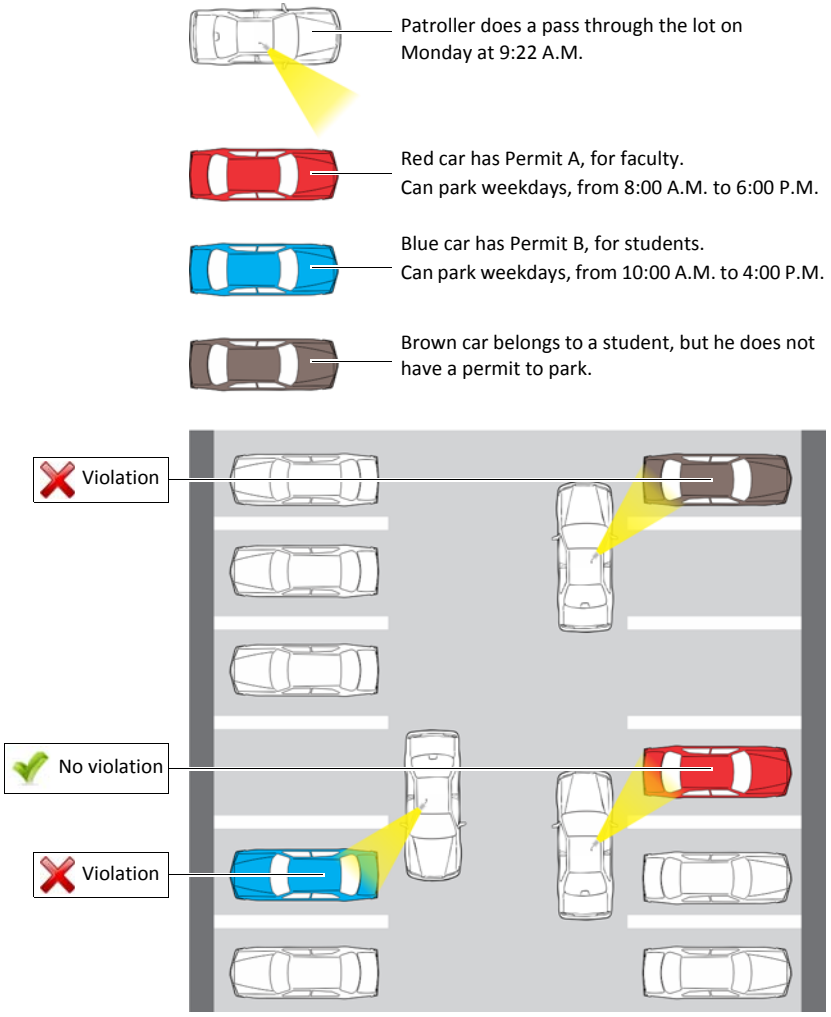
About permit lists and permit restrictions

Permit lists are lists of vehicles that are allowed to park in a certain place at a certain time. They are used in both City Parking Enforcement, and in University Parking Enforcement (with permit restrictions and parking lots).

In City Parking Enforcement, you create the permit list and configure its basic properties, but you don't need to define a parking lot or permit restriction. It is the city or municipality that decides when and where the permit is applicable. When you're patrolling, you choose which permit to enforce in Patroller based on where you are in the city (e.g. street signs).

In University Parking Enforcement, you create and configure a permit list the same way you would in City Parking Enforcement, but you also need to assign permit restrictions and parking lots to create an enforcement "zone" that is downloaded to Patroller. This additional configuration is needed because you're patrolling individual parking lots, not city streets with specific regulations already in place.

EXAMPLE In this example, you use a permit restriction to specify different time limits for different permit holders.



About shared permits

A permit list includes a field called *Permit ID*, which allows different vehicles to share the same permit by having the same *Permit ID* value in the permit list's source file. For example, a car pool permit could be shared amongst several vehicles (usually up to four). Each member of the car pool takes a turn driving the other members to work or school, therefore each member needs to share the same permit to park.

However, the permit still applies to *one vehicle at a time*. For example, if all four members of the car pool decide to take their own vehicles one day, they can't all use that car pool permit to park at the same time. Patroller will allow one vehicle with the car pool permit to park (the first one it sees), but will raise a *Shared permit* hit for every other vehicle seen with the same permit.

About parking lots and zones in Patroller

In City and University Parking Enforcement, when you create an enforcement rule (overtime rule or permit restriction), you have to apply that enforcement rule to a particular parking lot (zone). You do this in Security Center Config Tool by drawing a polygon around the parking lot's geographical location on the map.

Patroller downloads the zones at startup, then uses GPS to display them in order of proximity to its current location (closest zone is displayed at the top). The Patroller operator chooses the zone to enforce, rather than the enforcement rule.

If you don't configure a parking lot when creating your enforcement rule, there won't be any zones for the Patroller to enforce.

Differences between City and University Parking Enforcement

The following table shows you which parking enforcement concepts/features are used with each type of system.

	City Parking Enforcement	University Parking Enforcement	Learn more
Enforce permits and overtime simultaneously?	Yes	No	"About parking enforcement" on page 10
District overtime	Yes	Yes	"About District overtime rules" on page 14
Block face overtime	Yes	Yes[a]	"About Block face overtime rules" on page 15
Same position overtime	Yes	Yes[a]	"About Same position overtime rules" on page 13
Permits	Yes	Yes[b]	"About permit lists and permit restrictions" on page 20
Permit restrictions	No	Yes	"About permit lists and permit restrictions" on page 20
Shared permits	No	Yes	"About shared permits" on page 22
Multiple violations	Yes	Yes	"About multiple violations" on page 17
Parking lots ("zones")	No	Yes	"About parking lots and zones in Patroller" on page 22
Wheel imaging	Yes[c]	No	"About wheel imaging" on page 19
Long term overtime	Yes	No	"About long term overtime" on page 20

a. Supported but not typically used in University Parking Enforcement.
b. Permits must have permit restrictions applied to them in University Parking Enforcement.
c. Used to provide additional evidence of whether or not a vehicle has moved.

Understanding Mobile License Plate Inventory

This section includes the following topics:

About Mobile License Plate Inventory

Mobile License Plate Inventory (MLPI) is the AutoVu solution for vehicle license plate inventory. In MLPI, Patroller collects license plate reads to create and maintain a license plate inventory for a parking facility. The inventory can be used to report the following:

- The number of days a vehicle has been parked in the facility.
- The location (sector and row) of the vehicle in the facility.
- All vehicles parked in the facility.
- All vehicles that have left or entered the facility.

License plate reads can be collected in three ways:

- Automatic reading using the Patroller application and a Sharp camera (or cameras).
- Manual entry using the *Manual capture* feature of the Patroller application.
- (Optional) Manual capture using the Genetec approved handheld computer that is running the Patroller MLPI application.

About parking facilities

The parking facility entity represents the parking facility you wish to create an inventory for. Before AutoVu MLPI Patrollers can collect license plate reads for a parking facility inventory, the *Parking facility* entity needs to be configured into sectors and rows using Security Center Config Tool. The sector and row where a license plate is read represents the location of the vehicle in the parking facility. The sectors and rows of the parking facility entity can also be configured to create a specific route for the patroller to follow.

For more information, see "Additional configuration for Mobile License Plate Inventory (MLPI) systems" on page 256.

About license plate inventory

The license plate inventory includes license plate reads of all vehicles parked in the parking facility. It is created from the license plate collection offload data of the patroller application and the Genetec approved handheld computer (if applicable). The inventory can be used to monitor vehicle activity of the parking facility for a specific time period. For example, a patroller may collect license plate reads early in the morning and then do another collection in the evening to see how many vehicles have left the facility. The Security Desk *Inventory management* task is used to create the inventory from the offload data, and the Security Desk *Inventory Report* task is used to query any changes to an inventory.

For more information, see the *Inventory management* and *Inventory report* topics in the *Security Desk User Guide*.

About reconciling reads

Most reads from the offload data of a license plate collection are automatically reconciled (validated and added) to the license plate inventory by Security Center. However, some of them may require manual reconciliation if a conflict is detected. For example, a vehicle may have the same license plate numbers as another vehicle, but be from a different state. If this is the case, the Security Desk *Inventory Management* task will display a dialog box asking you to reconcile the read (confirm the plate number and state of the vehicle).

For more information, see the *Inventory management* topic in the *Security Desk User Guide*.

2

AutoVu software interface tours

This chapter provides an overview of the various applications you'll use to configure a fixed or mobile AutoVu system. You'll learn how to log on and log off the different applications, and how to navigate the applications' user interfaces.

This section includes the following topics:

What is an interface tour?

An interface tour provides an overview of a particular software application. It explains how to log on and log off, how to navigate through the different parts of the application, and other key concepts and tasks related to the application. For example, in the Patroller Config Tool interface tour, one of the topics describes how to restore the default settings for any individual option in the interface.

An interface tour does not describe the functionality of each button or option in the interface. That information is contained in an interface reference. For more information on interface references, see Part VI, "Interface references" on page 266

Security Center Config Tool interface tour

Security Center Config Tool (Config Tool) is the 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.

NOTE This interface tour is an abridged version of the main Security Center interface tour found in the *Security Center Administrator Guide*. For more information, see the Config Tool help.

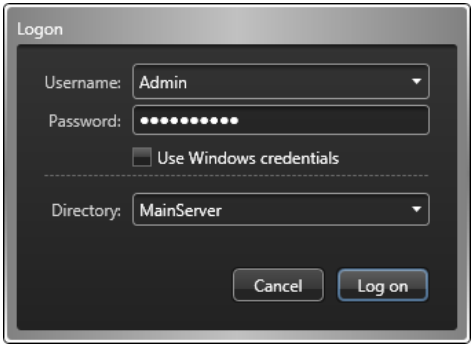
This section includes the following topics:

Log on to Security Center Config Tool

Before you begin: You need a username, password, and Directory name.

1 Click **Start**, then select **All Programs** > **Genetec Security Center 5.2** > **Config Tool**.

The **Logon** dialog box appears.



2 Enter the required information.

If you have just installed Security Center, log on as **Admin**, and use a blank password. The Directory name is the name or IP address of your main server.

If you are running Config Tool on your main server, you may leave the Directory field blank.

3 Click **Log on**.

The Home page appears.

After you are done: Change the **Admin** user's password if it hasn't been changed yet.

IMPORTANT If *active directory integration* has been set up by your system administrator, and you are connecting over a VPN connection, you must clear the **Use Windows credentials** check box and type your username in the format *DOMAIN\Username*.

Log off Security Center Config Tool

To log off Config Tool:

- Click the **Home** button and select **Log off** in the Home menu.

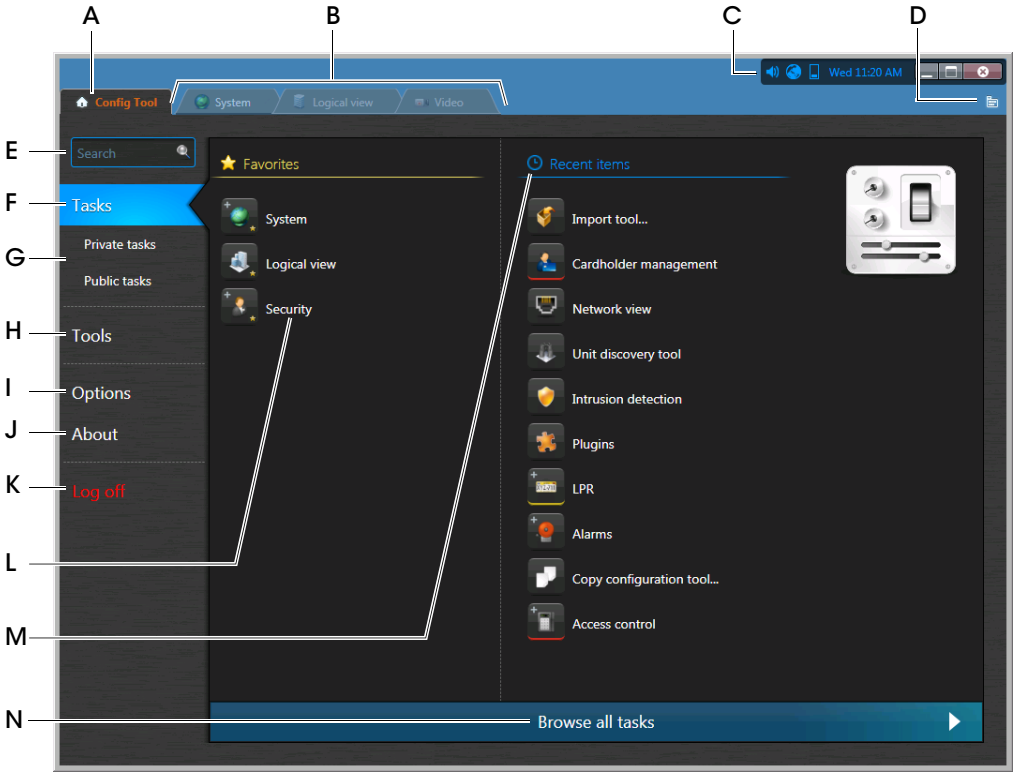
This disconnects you from the Directory, but does not close the application.

Close the Security Center Config Tool application

1. Click the **Exit** button in the upper-right corner of the Config Tool window.
2. If you have unsaved tasks in your workspace, you will be prompted to save them.
   Click **Save** to automatically load the same task list the next time you open Config Tool.

Security Center Config Tool Home page

This section describes the *Home page*, and key components of the Config Tool user interface. The *Home page* is the main page in Config Tool. You can open the Home page by clicking the *Home* ( ) tab. It is also shown if the task list is empty.



A	**Home tab**	• Click to show or hide the Home page. Right-click for a list of commands (for example, save the workspace, close tasks, and so on).
B	**Current tasks**	Lists the tasks you currently have open and are working on. • Click a task tab to switch to that task. • Right-click a tab for a list of commands.
C	**Notification tray**	Displays important information about your system. Hold your mouse pointer over an icon to view system information, or double-click the icon to perform an action. You can choose which icons to show in the notification bar from the Options dialog box.
D	**List all tasks**	Click to view a list of all open tasks. This button only appears if the task tabs take up the width of the taskbar.

E	**Search box**	Type the name of the task, tool, or entity you are looking for. All tasks, tools or entities containing that text in their category, name, or description, are shown.
F	**Tasks**	Lists your recent items, favorites, and all the task types that are available to you. Select a task to open from this tab.
G	**Private/ public tasks**	Click to view the saved tasks that are available to you. • **Private tasks**. Tasks that you saved that are only available to you. • **Public tasks**. Tasks that you or someone else saved that are available to the general public.
H	**Tools**	Click to view the tools that you can start directly from your Home page. The Tools page is divided into two sections: • **Tools**. This section shows the standard Security Center tools. • **External tools**. This section shows the shortcuts to external tools and applications.
I	**Options**	Click to configure Config Tool options.
J	**About**	Click to view information regarding your Security Center software, such as your license, SMA, and software version. From the About page, you can also view the following: • **Help.** Click to open the online help. • **Change password.** Click to change your password. • **Contact us.** Click to visit GTAP or the GTAP forum. You need an Internet connection to visit these Web sites. See "Technical support" on page 436. • **Installed components.** Click to view the name and version of all installed software components (DLLs). • **Copyright.** Click to display software copyright information. For information about your software license, see the section “License options” in the *Security Center Administrator Guide*.
K	**Log off**	Click to log off without exiting the application.
L	**Favorites**	Right-click any task or tool to add or remove it from your *Favorites* list. You can also drag a task into your favorites list. Tasks listed in favorites no longer appear in the *Recent items* list.
M	**Recent items**	Lists your recently opened tasks and tools.
N	**Browse tasks**	Click to view all the tasks available to you. Click a task icon to open the task. If it is a single-instance task, it will open. If you can have multiple instances of the task, you are required to type a name for the task. If the task has multiple entity views, you need to select an entity.

Patroller Config Tool interface tour

Patroller Config Tool is the 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.

This section includes the following topics:

Open Patroller Config Tool

By default, Patroller Config Tool is installed on your C drive, along with Patroller. However, it does not appear in your Windows Start menu. You have to navigate to the proper folder on your computer.

- On the in-vehicle computer, navigate to *C:\Program Files\Genetec AutoVu x.y\MobileClient*, then double-click *PatrollerConfigTool.exe*.

Patroller Config Tool opens.

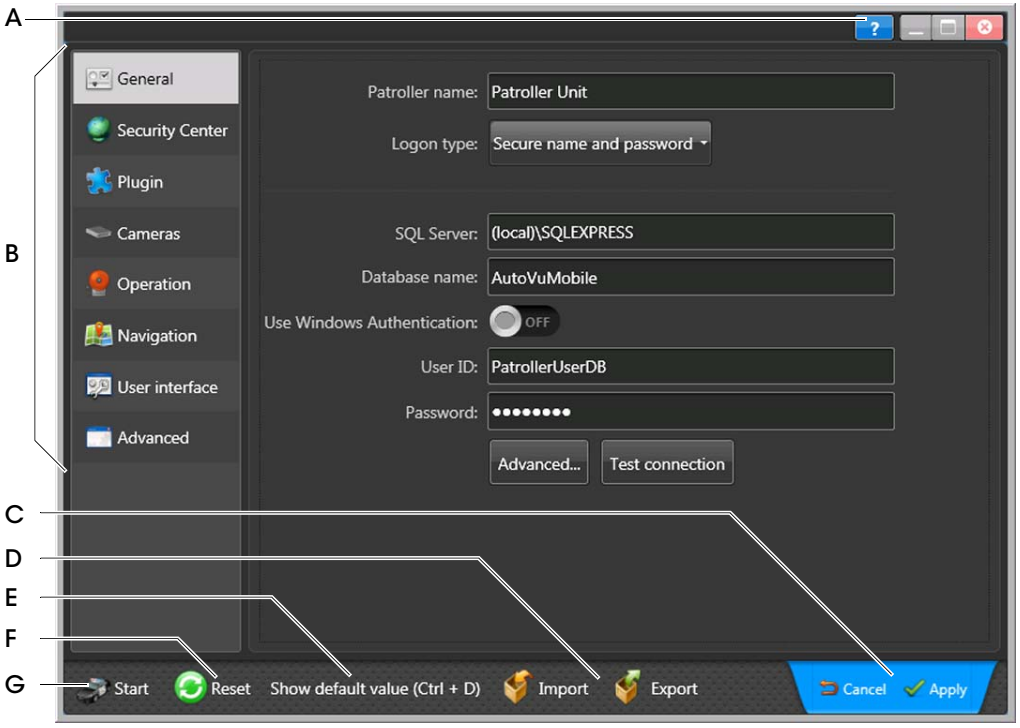
Close Patroller Config Tool

- Close the Patroller Config Tool window.

If you haven't applied your changes, you are prompted to do so. You need to restart Patroller for your changes to take effect.

Patroller Config Tool interface overview

This section takes you on a tour of the main areas in the Patroller Config Tool user interface. For more information on all the settings in Patroller Config Tool, see Chapter 19, "Patroller Config Tool reference" on page 344.



A	Contextual help	Click to open the product help. You can also press **F1** on your keyboard.
B	Main menu	List of the different configuration pages in the Patroller Config Tool. Each page contains the related settings for that category. For example, the Security Center page includes settings for connecting and offloading to Security Center.
C	Apply/Cancel changes	This tab only appears after you have changed a setting. Click **Apply** to save changes. Click **Cancel** to undo your changes.
D	Import/Export settings	Import or export the configuration settings from one Patroller to another. This simplifies the deployment of multiple Patroller vehicles. For example, if you have a fleet of Patroller vehicles, you can configure one and then export the settings to the others.

E	Show default settings	Display the default settings on the current page. The Default values appear as an orange tag next to the option. Click the orange tag to reset the option to the default value. For more information, see "Restoring a default setting" on page 34.
F	Reset to default settings	Reset all settings to the default state.
G	Start Patroller	Click to start Patroller.

Using Patroller Config Tool on a touchscreen

Since Patroller is typically used on an in-vehicle computer that is equipped with touchscreen capabilities, Patroller Config Tool is optimized to work with touch screen commands. This means you can tap buttons instead of clicking, and swipe the screen instead of scrolling. If you tap on a text box, you will see an on-screen keyboard that allows you to enter text.

Restoring a default setting

1 To see the default values for each setting on the current page, tap the **Show default value** button, or press **Ctrl** + **D** on your keyboard.

An orange button displaying the default value appears next to each setting that has been modified.

2 To reset a default value, tap the orange button next to the setting.

3 Tap **Apply**.

4 Tap **Show default value** or press **Ctrl** + **D** on your keyboard to return to normal view.

Importing and exporting Patroller settings

You can import or export the configuration settings from one Patroller to another, simplifying the deployment of multiple Patroller vehicles. For example, if you have a fleet of Patroller vehicles, you can configure one and then export the settings to the others.

NOTES

- Before you import settings, your current settings are saved to a zip file on the Patroller computer's desktop to be used as a backup if necessary.
- The imported Patroller settings will overwrite all current Patroller settings.
- If an error occurs during import, Patroller Config Tool will abort the import process and restore the old settings.

To export and import settings:

1 Open Patroller Config Tool on the Patroller computer that is ready to export settings.

2 Click **Export**.

A zip file is created on the Patroller computer's desktop.

3 Copy the zip file to the Patroller computer you want to configure.

NOTE You can keep the file on a USB key or network drive if you choose, but it must be accessible by the Patroller computer you want to configure.

4 Open Patroller Config Tool on the Patroller computer you want to configure.

5 Click **Import**.

6 Browse to the zip file with the Patroller settings you want to import.

7 Follow the on-screen instructions to proceed.

After importing the new settings, Patroller Config Tool closes. When you re-open it, the new settings are applied.

Sharp Portal interface tour

The Sharp Portal is the web-based administrative application 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.

This section includes the following topics:

Log on to the Sharp Portal

Before you begin: You need to know the IP address or name of the Sharp camera you want to connect to:

- **Sharp IP address.** The default IP address is 192.168.10.100.
- **SharpX IP addresses.** The default IP addresses are 192.168.10.1 for SBC1, and 192.168.10.2 for SBC2 (if applicable).

  NOTE SBC2 only applies if you have a *SharpX – Multi* system with four camera ports. For more information, see "Using the Sharp Portal with SharpX" on page 37.
- **Sharp name.** The Sharp name (e.g. Sharp1234) is on the label under the Sharp's visor.
- **SharpX name.** The SharpX name (e.g. SharpX1234) is on the LPR Processing Unit.

To log on to the Sharp Portal:

1 Open your Web browser, and go to *http://<Sharp name or IP address>/portal/*.

EXAMPLE

- If the Sharp camera's IP address is 192.168.10.1, enter *http://192.168.10.1/portal/*.
- If the Sharp camera's name is Sharp1234, enter *http://Sharp1234/portal/*.

2 Enter the default password "Genetec" (case-sensitive).

Best practice: After you log on, change the default password.

3 Select your language, then do one of the following:

- Click **OK** or press **Enter** on your keyboard to log on in regular mode.
- Press **Ctrl** + **Enter** on your keyboard to log on in *Advanced* mode, which gives you access to additional settings not found in regular mode. For more information, see Chapter 20, "Sharp Portal reference" on page 367.

The Sharp Portal opens to the **Status** page.

Log off the Sharp Portal

To log off the Sharp Portal, save your changes, and then close your Web browser.

Restart the Sharp unit

Certain configuration procedures require you to restart the Sharp camera. You can do this from the Sharp Portal.

1. Log on to the Sharp Portal.
2. Go to the **Status** page.
3. Click **Reboot unit**, then click **OK** to confirm.

   The connection to the Sharp Portal is momentarily lost.
4. Wait a few minutes to allow the Sharp to restart, then refresh the browser window.

Using the Sharp Portal with SharpX

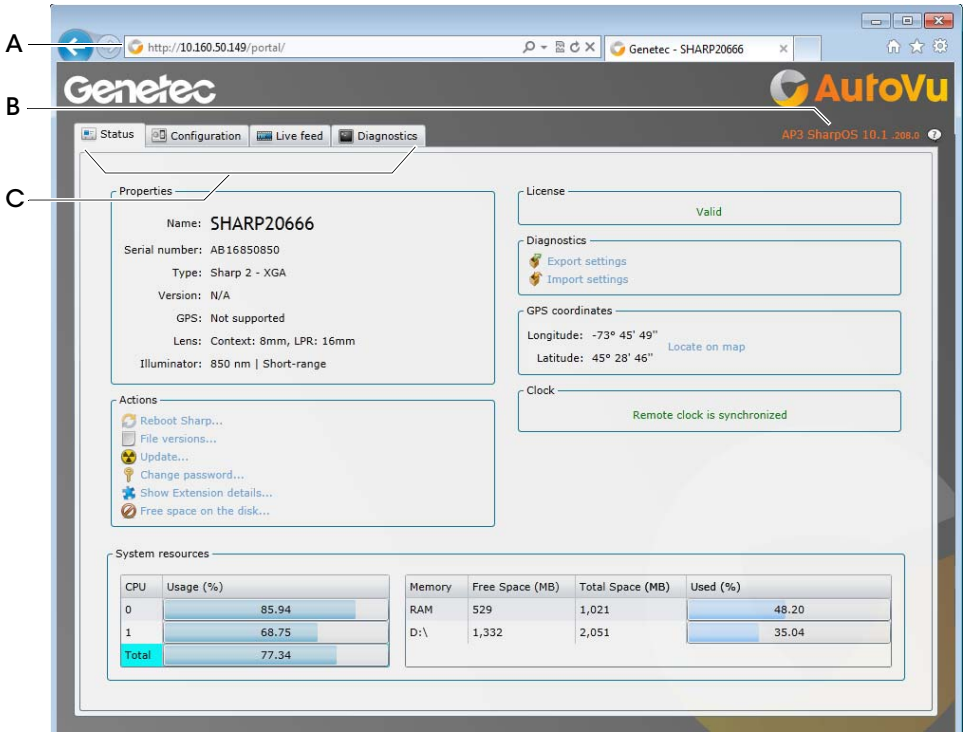
There is an important difference between connecting to a Sharp and connecting to a SharpX. For SharpX units, the Sharp Portal does not connect to the SharpX itself, but rather to the single board computer (SBC) inside the LPR Processing Unit that controls the SharpX camera. This is a crucial distinction if you are using a 4-port LPR Processing Unit, because it has two internal SBCs (one SBC can control two SharpX cameras). This means that you'll need to open a separate Sharp Portal web page for each SBC.

EXAMPLE You have an AutoVu mobile configuration that includes three SharpX cameras connected to a 4-port LPR Processing Unit. Two of the cameras are controlled by one of the SBCs, and the third camera is controlled by the other SBC. On the back of a 4-port LPR Processing Unit, there is a printed label has two Sharp names (e.g. Sharp1000 and Sharp1001). These are the names that correspond to the SBCs inside the unit. Therefore, to configure the SharpX cameras connected to ports 1 and 2, you must log on to *http://Sharp1000/portal/*, and to configure the SharpX camera connected to port 3, you must log on to *http://Sharp1001/portal/*.

For more information on how to configure a SharpX system using the Sharp Portal, see "Sharp Portal reference" on page 367.

Sharp Portal interface overview

This section takes you on a tour of the main areas of the Sharp Portal user interface. For more information on Sharp Portal settings, see "Sharp Portal reference" on page 367.



A	Sharp Portal address	Type the Sharp name or the IP address. The format is *http://Sharp1234/portal/*, or *http://10.1.0.176/portal/*. **NOTE** The IP address in the image is only an example.
B	Sharp details	Displays the Sharp image and the SharpOS version currently running on the Sharp unit you are connected to.
C	Main menu	Shows the different pages of the Sharp Portal. Each page contains the related settings for that category. For example, the *Configuration* page includes settings for configuring your Sharp camera.

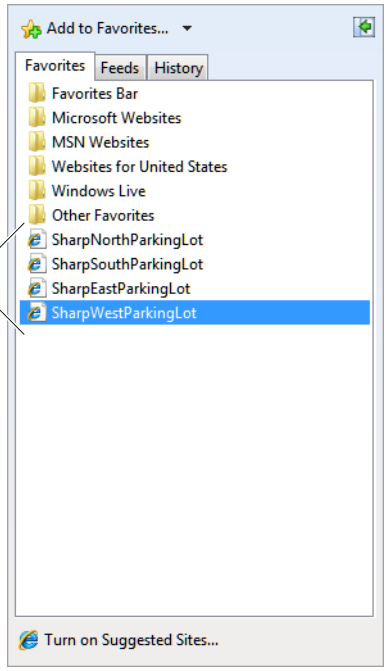
About the benefits of a web-based configuration tool

Some of the benefits of using a Web browser configuration tool are:

- **Open Sharp Portals in many tabs.** Web browsers use tab-based browsing, which provides you with a simple way to configure multiple Sharps. You can have many Sharp Portals open within the same Web browser.

- **Secure connection.** You can log on to the Sharp Portal securely using an HTTPS protocol with SSL encryption. For more information, see "Configuring Sharp Portal security" on page 148.

Add Sharp Portals to your Favorites for quick access to all the Sharps on your network.



- **Use Favorites.** A web-based tool allows you to easily monitor and configure all the Sharp units on your network. For example, if you have multiple fixed Sharps on your network, you can add them all to your Web browser's Favorites folder, and then rename them (e.g. SharpNorthParkingLot) for quick configuration and maintenance.

Where to find the most common tasks

Since you need to use several different applications to configure AutoVu, this section lists some of the common configuration-related tasks, and which application you use to configure them. In some cases, you'll need to use more than one application to configure a feature. For example, to encrypt communication between Patroller and Security Center, you need to configure settings in both Patroller Config Tool and Security Center Config Tool.

NOTE This table only lists a *few* of the common settings you can configure. For a complete list of all the settings in Security Center Config Tool, Patroller Config Tool, and the Sharp Portal, see Part VI, "Interface references" on page 266

Common tasks	Security Center Config Tool	Patroller Config Tool	Sharp Portal
Configuring users and user groups	**X**		
Configuring LPR root folder	**X**		
Connecting Patroller to Security Center	**X**	**X**	
Configuring/activating hotlists and permits	**X**		
Configuring Patroller sound management	**X**		
Configuring overtime rules	**X**		
Configuring parking facilities	**X**		
Configuring permit restrictions	**X**		
Configuring New Wanted attributes	**X**		
Configuring New Wanted categories	**X**		
Enabling New Wanted		**X**	
Enabling Manual Capture		X	
Configuring database and database retention	X		
Adding cameras to Patroller		X	

Common tasks	Security Center Config Tool	Patroller Config Tool	Sharp Portal
Choosing your read strategy (fast moving or slow moving vehicles)			X
Updating Patroller, Sharp firmware, or services	**X**		
Configuring hotlist privacy settings	X		
Configuring enforced hit attributes	X		
Configuring hit accept/reject survey	**X**		
Configuring annotation fields	**X**		
Configuring Patroller unit name		**X**	
Configuring Patroller to ask for username and password at logon		**X**	
Configure offload type		**X**	
Encrypting communication between Patroller and Security Center	**X**	**X**	
Disabling periodic transfer of hotlist data	**X**		
Configuring frequency of periodic transfer of hotlist data		**X**	
Turning LED on Sharp on/off			**X**
Selecting the LPR context			**X**
Viewing Sharp camera live video feeds			**X**
Restarting Sharp camera	**X**		**X**
Configuring Sharp extension (connect to Security Center, FTP server, or Patroller)			**X**

Part II

Deployment overviews

This part includes process overviews (roadmaps) for fixed and mobile AutoVu systems. The roadmaps guide you through the different tasks you need to perform to successfully deploy an AutoVu system.

This part includes the following chapters:

3

Deploying fixed AutoVu systems

This section includes a roadmap of the tasks needed to install and configure a fixed AutoVu system.

NOTE Because you can customize AutoVu in a number of ways, only the tasks for a *typical* deployment are provided.

This section includes the following topics:

Roadmap for fixed deployment

The table in this section summarizes a typical fixed AutoVu deployment.

NOTES

- The table includes the tasks required to get you up and running as soon as possible. For more information on all the configuration tasks you can use to customize AutoVu, see Part V, "Software configuration" on page 115
- The table does not include settings that are pre-configured. For example, when you install Security Center, the LPR Manager root folder is automatically created on your computer at the location *C:\Genetec\AutoVu\RootFolder*. Because this is done for you, it is not included in the table's list of configuration tasks.

Phase	Description	See
1	Read the related release notes. They contain information about the current release, as well as any known issues or limitations.	• Security Center Release Notes • AutoVu SharpOS Release Notes • AutoVu Patroller Release Notes
2	Have the information from your initial site survey on hand before you install the AutoVu hardware. For example, you should already know how high to install a fixed Sharp before you begin the installation.	• N/A
3	Read the hardware installation prerequisites, general guidelines, and safety precautions.	• Chapter 6, "Before you install AutoVu hardware" on page 52
4	Read the specific fixed installation guidelines, and then install the fixed Sharp hardware.	• Chapter 7, "Installing fixed AutoVu hardware" on page 55
5	Install Security Center. NOTE Security Center installation is explained in a separate document.	• *Security Center Installation and Upgrade Guide*
6	Upgrade Sharp units to the latest software and firmware. NOTE You can perform certain upgrades from Security Center Config Tool.	• "Updating AutoVu with hotfixes or service packs" on page 105
7	Log on to the Sharp Portal to configure the Sharp for a fixed AutoVu system.	• "Configure Sharp units for a fixed AutoVu system" on page 166
8	Specify the listening port that Security Center should use to communicate with fixed Sharp units.	• "Connect Security Center to fixed Sharp units" on page 167

Phase	Description	See
9	Specify which images to send to Security Center when a plate is read (LPR images and/or context images).	• "Configure which LPR images the Sharp sends to Security Center" on page 169
10	Specify the discovery port that Security Center should use to detect new fixed Sharps on the network.	• "Configure discovery port for fixed Sharp units" on page 168
11	Configure the LPR Manager server and database settings. NOTE You can also add additional servers to act as failover servers for the LPR Manager.	• "Configure LPR Manager server, database, and database retention periods" on page 118
12	(Optional) If you're using hotlists with your fixed deployment, you need to create and configure the hotlist entities, then turn on hotlist matching.	• "Configuring hotlists" on page 120 • "(Fixed Sharps only) Turn on hotlist matching" on page 128
13	Specify the Sharp's location and time zone.	• "Configure fixed Sharp time zone and location" on page 170

4

Deploying mobile AutoVu systems

This section includes a roadmap of the tasks needed to install and configure a mobile AutoVu system.

NOTE Because you can customize AutoVu in a number of ways, only the tasks for a typical deployment are provided.

This section includes the following topics:

Roadmap for mobile deployment

The table in this section summarizes a typical mobile AutoVu deployment, with the additional tasks and links for each type of mobile installation: Law Enforcement, City Parking Enforcement, University Parking Enforcement, and Mobile License Plate Inventory.

NOTES

- The table includes the tasks required to get you up and running as soon as possible. For more information on all the configuration tasks you can use to customize AutoVu, see Part V, "Software configuration" on page 115
- The table does not include settings that are pre-configured. For example, when you install Security Center, the LPR Manager root folder is automatically created on your computer at the location *C:\Genetec\AutoVu\RootFolder*. Because this is done for you, it is not included in the table's list of configuration tasks.

Phase	Description	See
1	Read the related release notes. They contain information about the current release, as well as any known issues or limitations.	• Security Center Release Notes • AutoVu SharpOS Release Notes • AutoVu Patroller Release Notes
2	Have the information from your initial site survey on hand before you install the AutoVu hardware. For example, you should already know how high to install a fixed Sharp before you begin the installation.	• N/A
3	Read the hardware installation prerequisites, general guidelines, and safety precautions.	• Chapter 6, "Before you install AutoVu hardware" on page 52
4	Read the specific mobile installation guidelines, and then install the mobile Sharp hardware.	• Chapter 8, "Installing mobile AutoVu hardware" on page 65
5	Install Security Center. NOTE Security Center installation is explained in a separate document.	• *Security Center Installation and Upgrade Guide*
6	Install Patroller and related hotfixes.	• "System requirements" on page 88 • "Before you install" on page 91 • "About the AutoVu Patroller installation package" on page 93 • "Installation overview" on page 94 • "Installing AutoVu Patroller" on page 95

Phase	Description	See
7	Upgrade AutoVu Patroller and Sharp units to the latest software and firmware. NOTE You can perform certain upgrades from Security Center Config Tool.	• "Updating AutoVu with hotfixes or service packs" on page 105 • "Upgrading Patroller to the latest version" on page 108
8	Log on to the Sharp Portal to configure the Sharp for a mobile AutoVu system.	• "Configure Sharp units for a mobile AutoVu system" on page 180
9	Connect Patroller to Security Center so that Patroller is discovered by the LPR Manager.	• "Connect Patroller to Security Center" on page 181
10	Connect SharpX units to Patroller.	• "Connect Sharp units to Patroller" on page 182 • "Using a SharpX – Multi system" on page 198
11	Configure the LPR Manager server and database settings. NOTE You can also add additional servers to act as failover servers for the LPR Manager and Patroller.	• "Configure LPR Manager server, database, and database retention periods" on page 118
12	Create and configure hotlists.	• "Configuring hotlists" on page 120
13	Configure Patroller.	• "Configure Patroller unit settings from Security Center" on page 185 • "Configure offload options" on page 187. • "Configure the Patroller unit name and logon options" on page 188 • "Configure Patroller hit options" on page 189 • "Configure the Patroller navigation and map settings" on page 190 • "Customize the Patroller user interface" on page 194
14	Configure the additional settings for your AutoVu mobile installation type.	• Chapter 15, "Additional configuration for AutoVu Law Enforcement systems" on page 205 • Chapter 16, "Additional configuration for AutoVu City and University Parking Enforcement systems" on page 209 • Chapter 17, "Additional configuration for Mobile License Plate Inventory (MLPI) systems" on page 256

5

Deploying Patroller Standalone systems

This section includes a roadmap of the tasks needed to install and configure a Patroller Standalone system.

NOTE Because you can customize AutoVu in a number of ways, only the tasks for a typical deployment are provided.

This section includes the following topics:

Roadmap for Patroller Standalone deployment

The table in this section summarizes a typical Patroller Standalone deployment.

Phase	Description	See
1	Read the related release notes. They contain information about the current release, as well as any known issues or limitations.	• AutoVu SharpOS Release Notes • AutoVu Patroller Release Notes
2	Read the hardware installation prerequisites, general guidelines, and safety precautions.	• Chapter 6, "Before you install AutoVu hardware" on page 52
3	Read the specific mobile installation guidelines, and then install the mobile Sharp hardware.	• Chapter 8, "Installing mobile AutoVu hardware" on page 65
4	Install Patroller.	• "System requirements" on page 88. • "About the AutoVu Patroller installation package" on page 93 • "Installing AutoVu Patroller" on page 95
5	Log on to the Sharp Portal to configure the Sharp for a mobile AutoVu system.	• "Configure Sharp units for a mobile AutoVu system" on page 180
6	Connect SharpX units to Patroller.	• "Connect Sharp units to Patroller" on page 182 • "Using a SharpX – Multi system" on page 198
7	Configure Patroller.	• "Patroller Config Tool reference" on page 344

Part III

Hardware installation

This part explains how to install AutoVu Sharp cameras and their related components in a fixed or mobile configuration.

This part includes the following chapters:

6

Before you install AutoVu hardware

This chapter provides links to the Sharp and SharpX hardware specifications, and the general safety precautions you should follow when installing the AutoVu fixed or mobile hardware.

This section includes the following topics:

Hardware specifications and system requirements

For more information about AutoVu hardware, including detailed specifications such as camera lens options, operating/storage temperatures, and more, click the links below to download the Sharp and SharpX specification sheets:

- Download the AutoVu Sharp spec sheet.
- Download the AutoVu SharpX spec sheet.

About the hardware installation procedures in this guide

The hardware installation procedures in this guide are based on typical AutoVu hardware installations. AutoVu's versatility allows you to customize an installation in a number of ways, and you may need to deviate slightly from the installation procedures depending on your individual setup (e.g. your installation site or type of vehicle). For questions about your specific installation, contact your Genetec representative.

Safety precautions

The following section describes the safety precautions regarding AutoVu installations. Read this section *before* beginning your fixed or mobile AutoVu installation.

WARNING Neglecting to observe the following safety precautions could result in physical harm, and/or severe damage to your hardware.

- It is extremely dangerous to allow the cables to become wound around the steering column or shift lever. Be sure to install this product, its cables, and wiring in such a way that they will not obstruct or hinder driving.
- Do not install this product or route any wires in the deployment area of your air bag. Equipment mounted or located in the air bag deployment area will damage or reduce the effectiveness of the air bag, or become a projectile that could cause serious personal injury or death. Refer to your vehicle's owner manual for the air bag deployment area. The User/Installer assumes full responsibility for determining proper mounting location, based on providing ultimate safety to all passengers inside the vehicle.
- Do not route wires where they will be exposed to high temperatures. If the insulation heats up, wires may become damaged, resulting in a short circuit or malfunction and permanent damage to the product.
- Only personnel who have special training and experience in automobile electronics, should set up and install this product. Installing or servicing this product and its connecting cables may expose you to the risk of electric shock or other hazards, and can cause damage to the system that is not covered by warranty.

CAUTION Neglecting to observe the following safety precautions could result in loss of data, damage to your product, and cause performance issues with your vehicle.

- Do not install this product where it may obstruct the driver's vision, impair the driver's ability to safely operate the vehicle, or impair the performance of any of the vehicle's safety features, including air bags, hazard lamp buttons, etc.
- When using screws, do not allow them to come into contact with any electrical lead. Vibration may damage wires or insulation, leading to a short circuit or other damage to the vehicle.
- Do not in any way cut or lengthen the GPS antenna cable. Altering the antenna cable could result in a short circuit or malfunction.

Best practice: Follow these basic safety requirements when installing your AutoVu hardware:

- Read this manual fully and carefully before installing your AutoVu product.
- Keep this manual handy for future reference.
- Consult your owner manual if you have any questions on your vehicle's wiring and/or operation.
- When drilling holes in your vehicle, make sure the drilling will not damage vehicle components.
- Deburr all drilled holes, and smooth any sharp edges.
- Install grommets into any holes you've drilled into your vehicle's sheet metal before passing wires or cables through them.
- Ensure that your installation will not affect vehicle operation or mandated safety functions or circuits. Always check the vehicle for proper operation after installation.
- The holding power of the magnetic mounting systems is dependant on surface finish, surface flatness, and thickness of the steel mounting surface.
- Keep your mounting surface and magnets clean, dry, and free of foreign particles that would prevent good surface contact.
- Installation should be done only by qualified personnel and conform to all local codes.
- To prevent damage from water leakage when installing a mount outdoors on a roof or wall, apply non-corrosive sealant around the bolt holes between the mount and mounting surface.
- As with any accessory in your vehicle's interior, the AutoVu system should not divert your attention from the safe operation of your vehicle. If you experience difficulty in operating the system or reading the display, please make adjustments while safely parked.
- Secure all wiring with cable clamps or electrical tape. Do not allow any bare wiring to remain exposed.
- Make sure cables and wires are routed and secured so they will not interfere with or become caught in any of the vehicle's moving parts, especially the steering wheel, shift lever, parking brake, sliding seat tracks, doors, or any of the vehicle's controls.

7

Installing fixed AutoVu hardware

This section explains how to install AutoVu in a fixed configuration, such as on a pole.

NOTE Instructions on how to install a fixed SharpX system were not available at the time of release. For more information, see the document *How to Power Up and Connect Your SharpX (fixed)* found on the GTAP Documents page.

This section includes the following topics:

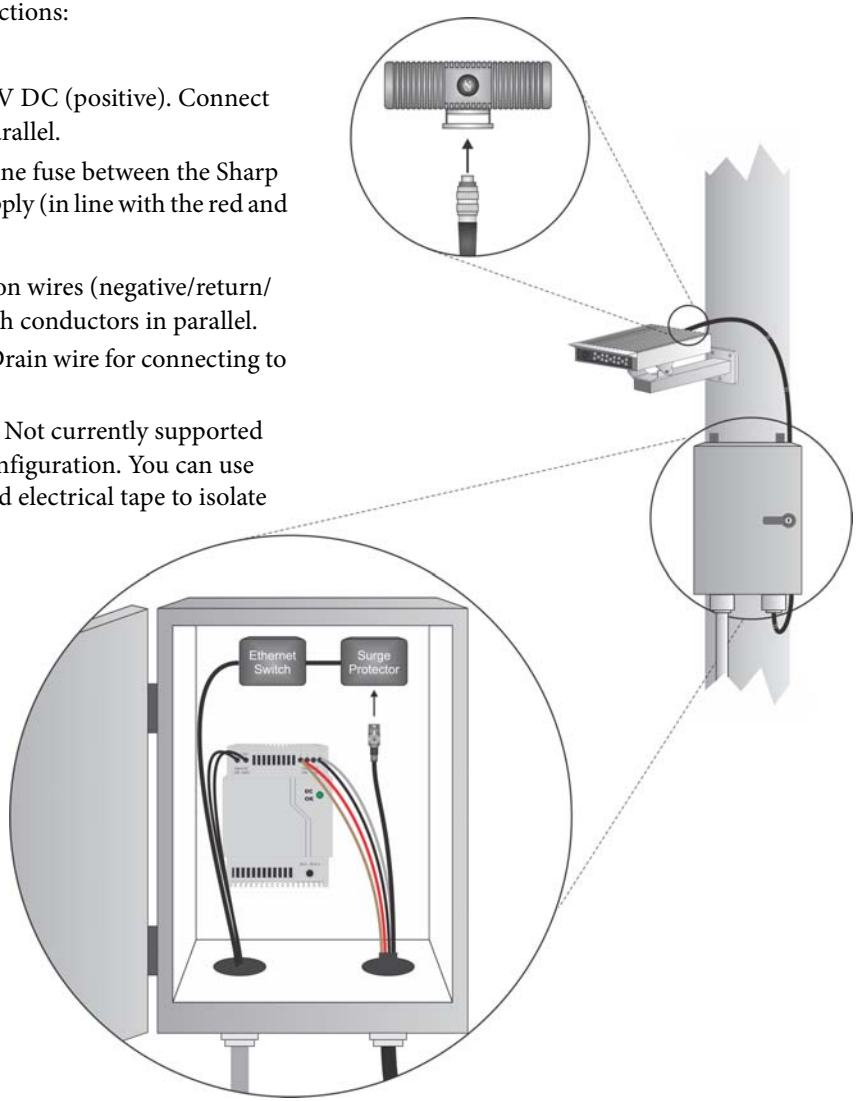
Fixed installation example

This section shows how a typical fixed AutoVu system is connected in the field. In this example, a Sharp XGA camera is mounted on a pole, with an electrical enclosure underneath. The enclosure contains the power supply and other components you'll need, such as a surge protector and Ethernet switch. This illustration gives you an idea of what a fixed installation should look like, but your specific installation may differ depending on the installation site and other factors.

Sharp power cable connections:

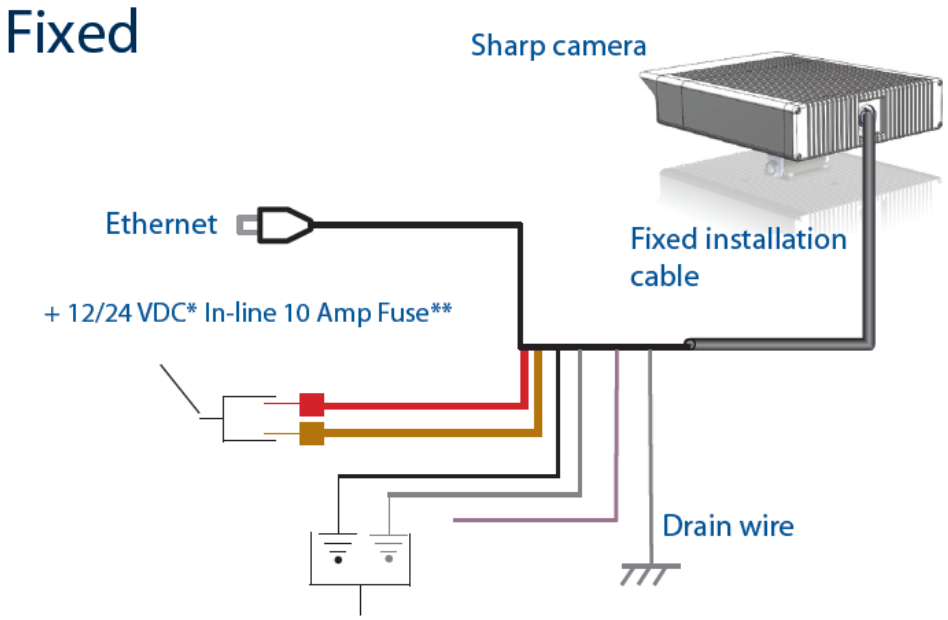
- Large black: Ethernet
- Red + Brown: +12/24V DC (positive). Connect both conductors in parallel.

  NOTE Install the in-line fuse between the Sharp camera and power supply (in line with the red and brown power wires).
- Black + Grey: Common wires (negative/return/ground). Connect both conductors in parallel.
- Tinned copper wire: Drain wire for connecting to earth/chassis ground.
- Violet: Micro-coaxial. Not currently supported for a fixed AutoVu configuration. You can use heat-shrink tubing and electrical tape to isolate the cut tip.



Sharp wiring diagram

The following illustration is taken from the printed document *Connecting the Sharp Camera* that is shipped in the box with the AutoVu hardware.



Specifications for pigtail end

- Large Black: Ethernet
- Red + Brown: +12/24VDC (positive). Connect both conductors in parallel.
- Black + Gray: Common. Connect both conductors in parallel.
- Tinned copper wire: Drain wire. Connect to earth/chassis ground.
- Violet: Micro-coaxial. Not used, do not connect.

* Genetec strongly recommends to use 24 VDC for fixed systems. For any cable longer than 5 meters, 24 VDC is mandatory.

* *Fuse not required if you use the power supply provided by Genetec. If you use a different power supply, install an inline 10 Amp Fuse (not included) between the power source and the Fixed installation cable.

Fixed installation guidelines

This section provides you with important tips that you should be aware of before you begin the installation, as well as the information you'll need to properly position the Sharps.

This section includes the following topics:

General guidelines

Best practice: Use the following best practices when installing a fixed AutoVu system.

- The AC connection to the Sharp's power supply should only be performed by a certified electrician. Make sure to follow all local laws and codes.
- The Sharp should be relatively accessible for cleaning. Although the Sharp lens is protected by a polycarbonate panel and a visor, you should regularly clean the panel for optimal results.
- You can order the AutoVu hardware with a Pelco universal mounting plate.
  The plate is compatible with the following Pelco mounts: EM22 / MM22 / EM2000 / EM1000U / EM1109.

Bottom of Sharp camera with Pelco mounting plate attached (part number AU-H-SHPPMPLT).

The Pelco mounting plate does not come with standard AutoVu hardware. You need to specify that you want a Pelco mounting plate when ordering.

NOTE Installation instructions for Pelco mounts and other third-party mounts are not provided in this document. For more information, you'll need to refer to the mount manufacturer's documentation.

- If you're connecting the Sharp fixed cable to an Ethernet switch (sold separately), make sure it's an industrial Ethernet switch that is capable of withstanding the environmental conditions of your area.
- It is recommended that you install surge protectors (sold separately) for your Ethernet connection and power supply, especially if you are installing the AutoVu system in an area with frequent lightning. For your Ethernet connection, a gigabit Ethernet (GigE) surge protector is required. Here are some guidelines to follow for Ethernet surge protection:

- You should use a bi-directional, in-line surge protector if available (e.g. protecting both sides of the surge protector). If you use a uni-directional surge protector, make sure the protected side is connected to the Sharp.
- Make sure to properly earth-ground the surge protector. For example, in a dry region, the ground should be of low-resistance at all times. Always keep the ground conductor as short as possible, and as large as possible for low-inductance.
- Install the surge protector so that it is no more than three meters away from the Sharp.

For more information on surge protection, contact your Genetec representative.

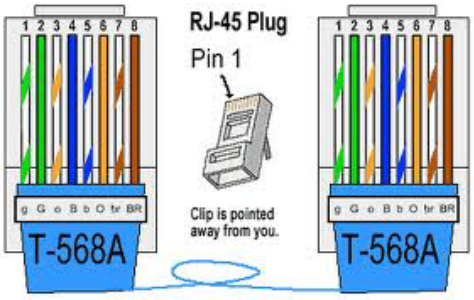
- You can connect the Sharp to an un-interruptible power supply (UPS) in order to provide emergency power in the event of a power failure in your area.
- The enclosure that will house the various components your Sharp requires should conform to NEMA standards.
- The enclosure you use should be installed close enough to the Sharp camera so the Sharp's cable can reach it. You should not attempt to extend the Sharp cable in any way. Various cable lengths are provided that can accommodate your specific situation.

If you need to shorten the Sharp cable

In some cases, you may want to cut the pigtail end of the Sharp cable in order to shorten it.

Best practice: Use the following best practices when shortening the Sharp cable:

- You'll need to re-crimp the CAT5e cable. The crimping procedure should follow the TIA/EIA-568-B.1-2001 telecommunications standard, and the T568A pin/pair assignment.

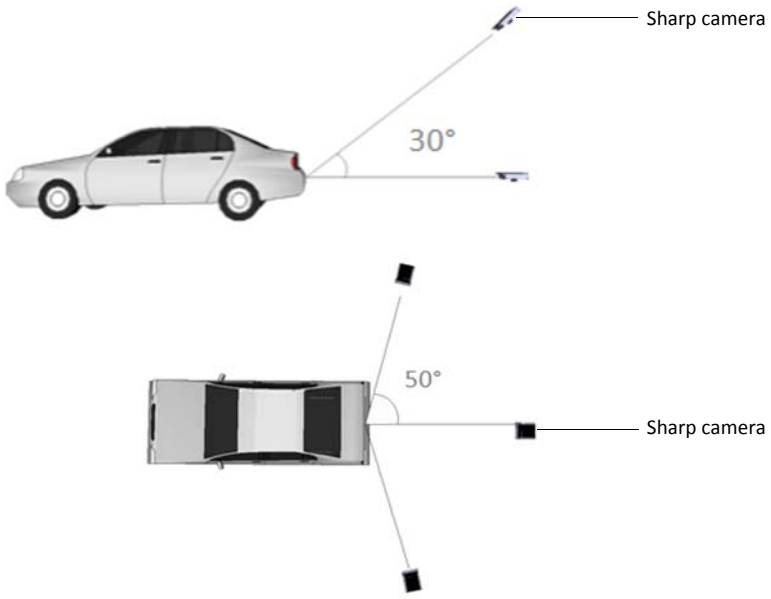


- A new RJ45 connector is provided to re-crimp the CAT5e cable. You cannot reuse the same RJ45 connector you cut off the Sharp cable.
- After cutting the Sharp cable, you'll need to strip the internal wires (CAT5e and power wires) before connecting them to the RJ45 and power supply. To determine the length of insulation to strip, refer to the instructions provided with your RJ45 connector and power supply.

Sharp positioning guidelines

Although these guidelines will help you properly position the Sharp camera, keep in mind that it is your specific installation site that determines the positioning requirements. This means that a certain degree of trial and error will be needed to correctly position the Sharp to read plates in your area.

- Make sure to install the Sharp at the proper angle for your target area. The angle of the camera can deviate from a straight-on view by up to 30 degrees vertically, and up to 50 degrees horizontally.

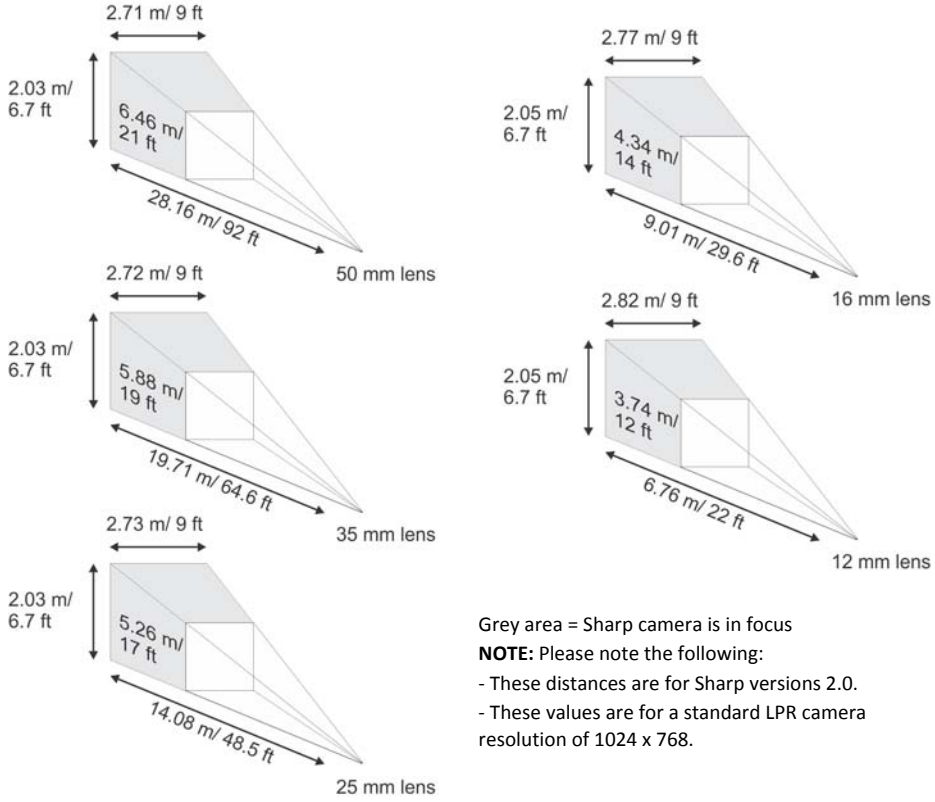


NOTE For optimal results, it is best practice to minimize the angles and avoid extreme angle positions.

IMPORTANT If you install the Sharp at zero degrees horizontally and vertically, you will receive multiple reads of the same plate.

- Install the Sharp at the proper distance from the target area. The proper distance is determined by the camera's resolution, lens, and the height of the characters on the license plates you want to capture. The illustration below shows the guidelines for North American and European plates. For more information on the proper distance for your location, contact your Genetec sales representative.

Sharp focal distances



Grey area = Sharp camera is in focus

NOTE: Please note the following:

- These distances are for Sharp versions 2.0.
- These values are for a standard LPR camera resolution of 1024 x 768.

- To capture plates on vehicles that are travelling at high speeds, such as on a highway, you should minimize the camera's horizontal and vertical angles. This will maximize the amount of time the vehicle is in the camera's field of view, and increase the chances of a successful plate read.

Fixed installation procedure

This section describes a typical installation procedure for a Sharp XGA. It also includes guidelines for the Sharp EX.

This section includes the following topics:

What you need

In addition to the AutoVu parts listed in the section "AutoVu hardware components" on page 4, you may also require the following third-party components:

- **Surge protector.** For ethernet (GigE required) and power.
- **Electrical enclosure.** Must conform to NEMA standards.
- **Flexible liquid-tight conduit.** For protecting the Sharp camera cable.
- **Weatherproof, non-corrosive sealant.** For protecting cable connections.

Install your Sharp XGA

WARNING Before you begin your installation, make sure that power to the installation site is not active. Power should only be activated when the installation is complete.

This section includes the following topics:

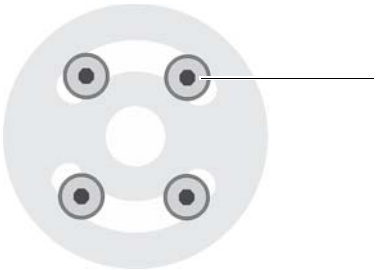
Step 1: Mount the Sharp

1. Attach the camera mount to the wall, pole, or other base that will support the Sharp camera. Refer to the camera mount's documentation for more information.
2. Locate the circular bracket underneath the Sharp, loosen the nut, slide the hex bolt out, and remove the bracket.

Loosen nut and remove hex bolt to detach circular bracket from Sharp.

NOTE If you're using the Pelco Mounting Plate to attach the Sharp camera to a compatible Pelco mount, see the Pelco mount's documentation for installation instructions. For a list of compatible Pelco mounts, see "Fixed installation guidelines" on page 58.

3 Attach the circular bracket you removed from the Sharp in Step 2 to the mount. The arc-shaped grooves allow you to position the screws as needed to align them to the threaded holes on different mounts.



4 Position and angle the Sharp camera according to the best practices described in "Fixed installation guidelines" on page 58.

Step 2: Connect the Sharp

1 Pass the Sharp cable through the flexible liquid-tight conduit (if you're using one).

2 Connect the Sharp cable to the connector at the rear of the Sharp camera.

IMPORTANT Note the following:

- Put dielectric grease on the cable connector threads.
- Tighten the cable connector by turning the connector ring clockwise. Do not tighten the cable by turning the cable cord.
- Do not turn the cable from behind the outer ring.
- Do not use any tools to tighten the cable. Tighten by hand only.

Step 3: Mount the electrical enclosure

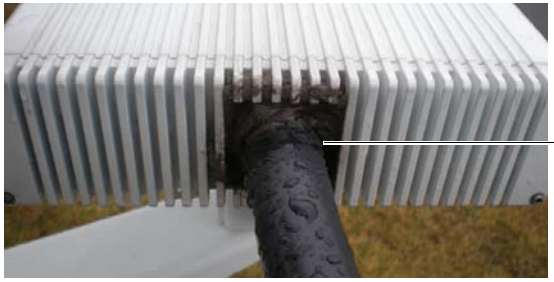
1 Attach the electrical enclosure that will house the power supply and surge protector to the base near the Sharp camera. For instructions on how to install the enclosure, see the enclosure manufacturer's documentation.

2 Make sure that the surge protector, power supply, and any other components you require are properly installed inside the electrical enclosure.

3 Connect the AutoVu cables to the power supply, surge protector, and any other components inside the electrical enclosure.

Step 4: Finishing up

- Power up the installation site. If everything is working properly, you can apply weatherproof sealant where the conduit cable meets the Sharp to help prevent damage from the elements or from possible vandalism.



8

Installing mobile AutoVu hardware

This section explains how to install AutoVu in a mobile configuration, such as in a vehicle.

This section includes the following topics:

Mobile installation examples for Sharp

This section provides examples of the most common mobile AutoVu installations. One is a basic installation with two Sharp cameras and a GPS antenna, and the other is an advanced installation with the additional Navigator unit and tire cameras added.

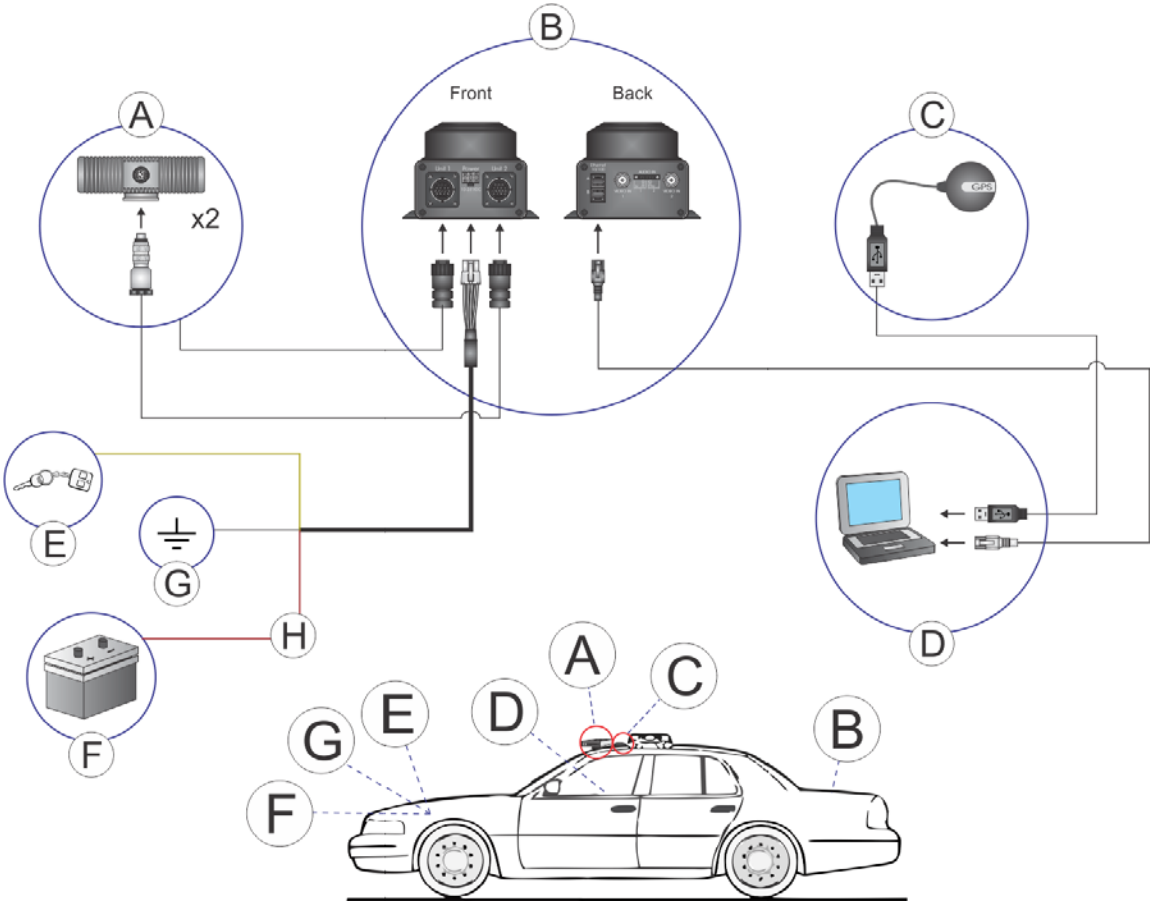
The examples in this section are intended to show you the relationship between all the AutoVu components, and where they belong in your vehicle. For information on wiring connections, see the printed document *How to Power Up and Connect Your Sharp* that is included in the box with your AutoVu hardware.

This section includes the following topics:

Basic mobile installation example

This section shows how a typical mobile AutoVu system is connected in the field. In this example, we're using two Sharp cameras and a GPS antenna. The breakout box is installed in the trunk, and the Sharp cameras are hardmounted.

The following illustration and table provide information on each required component:



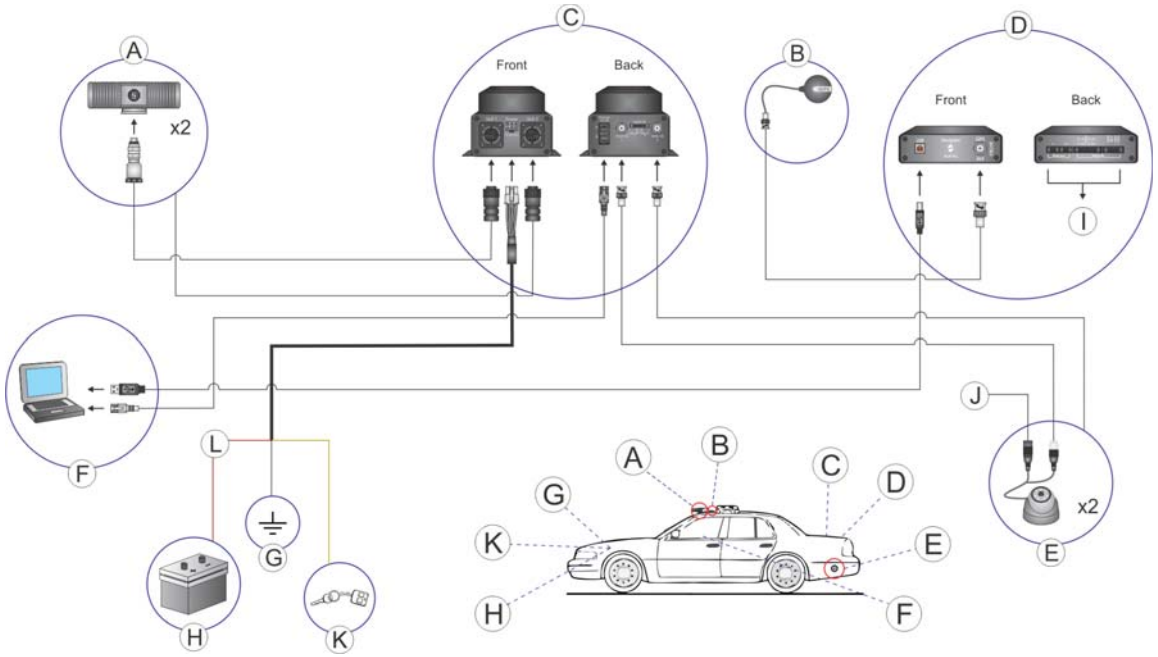
Component	What you should know
A: Sharp Camera	• Magnetic mount Sharps can also be used. For more information, see "Magnetic mount installation" on page 80. • Make sure to secure the Sharp cable to the Sharp by turning the outer connector ring clockwise. • Do not bring the camera through a mechanical car wash.
B: Breakout box	• The breakout box can be installed anywhere in the vehicle, but make sure that the heat sink fins are not blocked, and that the unit is protected from being jostled or moved by other objects in the vehicle. • It is best practice to install the breakout box where it will not be in direct sunlight for an extended period of time.

Component	What you should know
C: GPS antenna	• Try to install the GPS antenna as close to the Sharp cameras as possible for an accurate signal. • Must have an unobstructed view of the sky for best results.
D: Mobile data computer (MDC)	• For instructions on how to install the in-vehicle MDC mount, you'll need to refer to your mount manufacturer's documentation.
E: Vehicle's ignition	• Connect yellow wire from breakout box power cable to vehicle's ignition.
F: Vehicle's battery	• Connect red wire from breakout box power cable through a 15A in-line fuse to vehicle's battery.
G: Ground	• Connect black wire from breakout box power cable to ground (vehicle's frame, engine block, etc).
H: Power cable in-line fuse	• Connect to red wire going to vehicle's battery. Install as close to the battery as possible.

Advanced mobile installation example

This section shows how an advanced mobile AutoVu system is connected in the field. In this example, we're using two Sharp cameras, two tire cameras, a Navigator unit, and a GPS antenna. The breakout box and Navigator are installed in the trunk, and the Sharp cameras are hardmounted.

The following illustration and table provide information on each required the component:



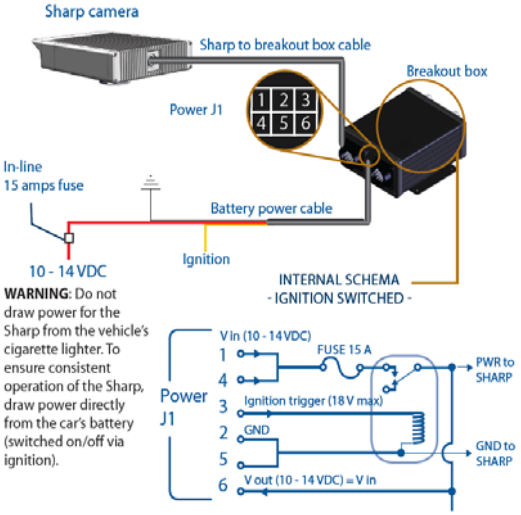
Component	What you should know
A: Sharp Camera	• Magnetic mount Sharps can also be used. For more information, see "Magnetic mount installation" on page 80. • Make sure to secure the Sharp cable to the Sharp by turning the outer connector ring clockwise. • Do not bring the camera through a mechanical car wash.
B: GPS antenna	• Connects to Navigator unit. • Try to install the GPS antenna on the roof as close to the Sharp cameras as possible for an accurate signal. • Must have an unobstructed view of the sky for best results.

Component	What you should know
C: Breakout box	• The breakout box can be installed anywhere in the vehicle, but make sure that the heat sink fins are not blocked, and that the unit is protected from being jostled or moved by other objects in the vehicle. • It is best practice to install the breakout box where it will not be in direct sunlight for an extended period of time.
D: Navigator unit	• The Navigator unit can be installed anywhere in the vehicle, but it **must** be installed on a flat, level surface, and should be protected from being jostled or moved by other objects in the vehicle. • A 15 ft USB cable is provided with the Navigator unit. If you need to use your own USB cable, you must use a type A to type B USB cable no longer than 15 ft. Longer cables may result in data loss. • Try not to install the Navigator unit where it will be in direct sunlight for an extended period of time. For more information, see "AutoVu hardware components" on page 4.
E & **J**: Tire Cameras	• Although this example shows the tire cameras installed behind the vehicle's bumper, you don't necessarily need to install them this way. The important thing is that the cameras are installed at an appropriate height, and the lenses are pointed in the right direction for capturing tire images. For more information, see "(Optional) Install tire cameras" on page 78. • The tire cameras require a 12V DC power source. However, you should **never** connect the cameras directly to the vehicle's battery, otherwise they will be receiving power even when the vehicle is turned off, which will drain your battery.
F: Mobile data computer (MDC)	• For instructions on how to install the in-vehicle MDC mount, you'll need to refer to your mount manufacturer's documentation.
G: Ground	• Connect black wire from breakout box power cable to ground (vehicle's frame, engine block, etc).
H: Vehicle's battery	• Connect red wire from breakout box power cable through a 15A in-line fuse to vehicle's battery.
I: Navigator unit	• Connect wires to vehicle's odometry, reverse signal, and ignition. For more information on the proper connections, see "Install your breakout box" on page 75.
K: Vehicle's ignition	• Connect yellow wire from breakout box power cable to vehicle's ignition.
L: Power cable in-line fuse	• Connect to red wire going to vehicle's battery. Install as close to the battery as possible.

Sharp wiring diagram

The following illustrations are from the printed document *Connecting the Sharp Camera* that is shipped in the box with your AutoVu hardware.

In vehicle • 12VDC

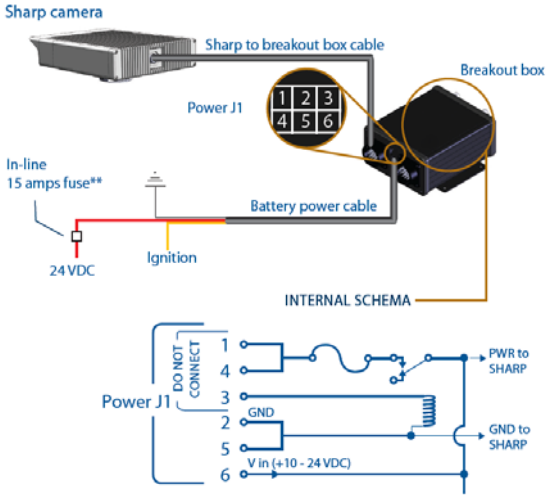


WARNING: Do not draw power for the Sharp from the vehicle's cigarette lighter. To ensure consistent operation of the Sharp, draw power directly from the car's battery (switched on/off via ignition).

Specifications for battery power cable
- Black: Ground
- Red: 10–14 VDC
- Yellow: Ignition

- Need to use ignition to enable main VDC power
- Fused circuit up to 14 VDC
- V out (pin6) needs crimped connector

In vehicle • 24VDC



Specifications for battery power cable
- Black: Ground
- Red: 24 VDC
- Yellow: Ignition

- Not ignition triggered
- Need to crimp 24V (pin6) on J1 connector
- Bypasses breakout unit fuse to directly power Sharp

Mobile installation guidelines for Sharp

This section provides you with important tips that you should be aware of before you begin the installation.

Best practice: Use the following best practices when you are choosing where to install your Sharp camera(s).

- Before removing any parts of your vehicle, such as the headliner or rear bumper, make sure that you have a good idea how you want to position your Sharp cameras and tire cameras, and where you want to install your breakout box and Navigator unit.
- If you are hardmounting your Sharp cameras, make sure that they do not obstruct any other devices on the vehicle's roof (such as a light bar), and that they do not overhang the door frame.
- Make sure that no part of the vehicle's roof obstructs the view of your Sharp camera(s).
- Always use a hardmount installation for your Sharp camera if you intend to drive your vehicle at moderate or high speed on regular city streets.
- The Navigator unit can be installed anywhere in the vehicle, but it **must** be installed on a flat, level surface.
- The breakout box can be installed anywhere in the vehicle, but you must make sure the heat sink fins are not blocked.
- The breakout box and Navigator unit should be protected from being jostled or moved by other objects in the vehicle. For example, if you install the components in the trunk, they should be placed in an enclosure or on an elevated tray.
- The connectors of the Navigator unit should not come into contact with other objects. It is recommended that you protect the Navigator unit's wires and connections accordingly.
- The USB cable used to connect the Navigator unit to the in-vehicle laptop can be no longer than 15 feet, otherwise data loss may occur.
- If you're using the GPS antenna, for best results, install it on your vehicle's roof where it has an unobstructed view of the sky.

Mobile installation procedure for Sharp

This section describes how to install your AutoVu hardware either in a hardmounted configuration (Sharp cameras permanently mounted on your vehicle), or in a portable configuration using the magnetic mount and cigarette lighter cable.

Before you begin: You'll need weatherproof, non-corrosive sealant to protect the cable connections after installation is complete.

This section includes the following topics:

Hardmount installation

This section describes how to install your mobile AutoVu system in a hardmounted configuration.

This section includes the following topics:

Before you begin: Read through the entire installation procedure first. This will help you decide where to install your AutoVu components, and how to route your wires and cables.

Prepare your vehicle

1. Remove your vehicle's headliner, and any other parts of your vehicle where you intend to route wires and/or cables.
2. Place one of the hardmount top plates on your vehicle's roof where you intend to attach your Sharp camera, place the plate at the desired position, and then use a pencil or other marker to trace the outline of the plate, as well as the plate's four corner drill holes. Repeat this step for your other Sharp.
3. Place the grommets on the section of your vehicle's roof where you intend to pass the Sharp cables (and GPS cable, if applicable), and then use a pencil or other marker to trace the outline of the grommets.

4 Verify that both sides of the roof are clear of anything that could be damaged, and then drill holes into the areas that you marked in Step 2 and Step 3.

NOTE Make sure that the holes you drill for the Sharp cables are slightly smaller than the outline of the grommets, otherwise the grommet collars won't grip your vehicle's roof.

5 Deburr the holes to remove any metal shards or remnants.

6 Install your grommets into the holes.

Install your Sharp camera

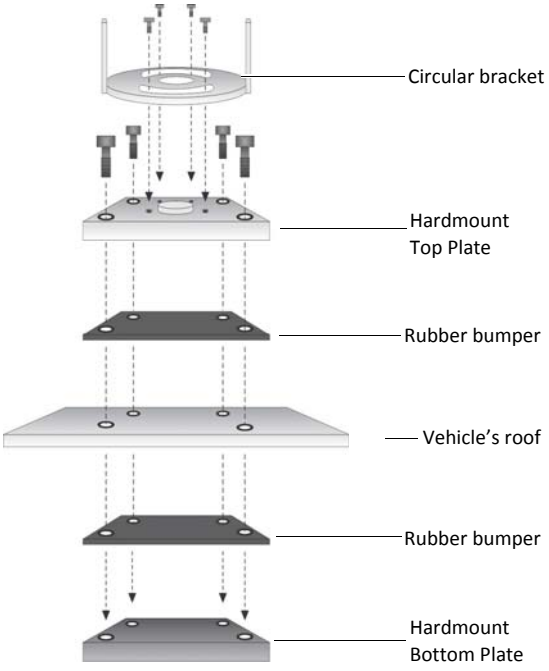
1 Locate the circular bracket underneath your Sharp camera, loosen the nut, slide the hex bolt out, and remove the bracket.

2 Place the hardmount top plate, along with the rubber bumper (poke holes in the bumper), on top of the vehicle's roof, and align the plate's drill holes with the holes you drilled in "Prepare your vehicle" on page 73.

3 Place the four provided screws inside the drill holes.

4 Position the hardmount bottom plate, along with its rubber bumper, under the roof, and then screw both plates together (sandwich the roof).

5 When the top and bottom plates are secure, attach the circular bracket that you removed in Step 1 to the top plate.



6 Re-attach the Sharp camera to the circular bracket.

Install your breakout box

The breakout box can be installed almost anywhere in your vehicle, but it is typically installed in the trunk.

Best practice: Use the following best practices to install the breakout box:

- The breakout box must be secure and protected from other equipment or moving parts. For example, if you install it in the trunk, you should place it in an enclosure or elevated tray to protect it from being damaged by other items in the trunk, or from water that may leak into the trunk floor.
- Do not block the heat sink fins on the top of the breakout box.
- Do not leave the breakout box in direct sunlight for an extended period of time, as it heats up considerably while in use.

(Optional) Install your Navigator box

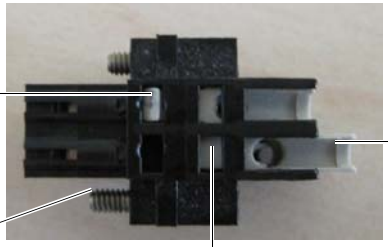
The AutoVu Navigator box provides Patroller with more accurate geographic coordinates than a standard GPS device. It can be used with any mobile installation, but is *required* for City Parking Enforcement with Wheel Imaging systems. The Navigator box is installed in the vehicle, and is connected to the vehicle's odometry signal (usually by tapping the vehicle speed sensor), and to the in-vehicle computer.

NOTES

- Wires are not included (12 VDC power is required). You'll need the following:
  - *Ignition and reverse signals.* Use stranded conductor copper wire AWG 16 to AWG 24.
  - *Odometry signal.* Use shielded, dual-conductor cable with stranded conductors AWG 16 to AWG 24.
- The Navigator box must be secure and protected from other equipment or moving parts. For example, if you install it in the trunk, you should place it in an enclosure or elevated tray to protect it from being damaged by other items in the trunk, or from water that may leak into the trunk floor.
- Install the Navigator box on a flat, level surface.
- Install the Navigator box as close to the breakout box as possible, as you may want to tap into the breakout box's power cable to provide power to the Navigator box.
- Do not connect the Navigator box directly to the vehicle's battery. It should only receive power when your vehicle's engine is running.
- The Navigator box uses Weidmuller tension clamp connectors. You need to push in the tension clamp, insert the wire, then release to secure the wire in the connector.

To use the included connectors:

2-pole connector (top view)



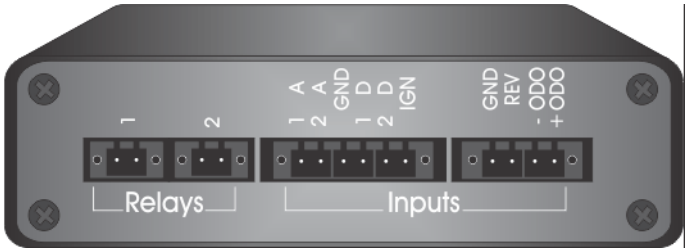
Use a 2.5 mm flat head screwdriver (0.4 mm blade width) to push here and open the pole's clamp

After inserting wire into pole, push here to close pole's clamp.

After connecting to the Navigator unit, make sure to tighten the securing screws.

Insert wire into open pole here. Do **not** strip the wire's insulation. if you do, the wire will be too small for the clamp to secure it.

To connect your wires:



Connection	What it's for
Relays 1 and 2	Not supported.
Inputs 1A and 2A	Analog inputs used to measure battery voltage, temperature, etc.
GND	Grounding
Inputs 1D and 2D	Digital inputs used for sensors handling events such as doors opening, etc.
IGN	Ignition input. State of the vehicle's power system.
GND	Grounding
REV	Reverse input. Connect to vehicle's reverse signal (required for inertial navigation). NOTE You can tap into the vehicle's reverse lights to get this signal.
- ODO and + ODO	Odometry inputs. Connect to the vehicle's odometry signal (required for inertial navigation).

After you are done: See "(Optional) Install USB GPS antenna" on page 77.

(Optional) Install USB GPS antenna

There are two different types of GPS antennas, depending on the AutoVu package you purchased. One type connects to the Navigator box (if you're using one). If you're not using a Navigator box, you'll have the other type which connects to the USB port on your in-vehicle computer.

1. Verify that the roof of your vehicle is clean, dry, and free of debris.
2. Place the magnetized end of the GPS antenna on your vehicle's roof so that it has an unobstructed view of the sky.
3. Pass the GPS antenna cable through one of the holes you drilled in the vehicle's roof for the Sharp cables.

4 If you are using the Navigator box, connect the GPS antenna to the designated connector on the unit (see "Advanced mobile installation example" on page 69).

5 If you are not using the Navigator box, connect the antenna to a free USB port on your in-vehicle computer.

(Optional) Install tire cameras

This section describes the typical tire camera installation in the vehicle's trunk.

NOTES

- Cables for powering the tire cameras are not included. 12V DC power is required.
- Do not connect the tire cameras directly to the vehicle's battery. They should only receive power when your vehicle's engine is running.
- You don't necessarily need to install the tire cameras as described in this section, but however you choose to install them, you must make sure that they are at an appropriate height and that the lenses are correctly positioned to capture tire images.
- The tire cameras included with your AutoVu kit are third-party cameras. Therefore, if you need more detailed information on the proper installation of your tire cameras, you'll need to refer to the cameras' documentation.

To install the tire cameras:

1 Open your vehicle's trunk.

2 Using the screws provided with your tire cameras, attach the cameras to the rear wall of your vehicle's trunk.

NOTE Never install the cameras directly on the vehicle's bumper, as even a slight collision could damage the cameras.

3 Make sure the tire cameras are facing outward to properly capture parked vehicles' wheels.

Finishing up

1 Connect all cables and wires.

2 Start your vehicle to verify that your AutoVu hardware, as well as your vehicle's other electrical devices, are working properly.

3 Seal the holes in the vehicle's roof with a weatherproof sealant, such as RTV silicone.

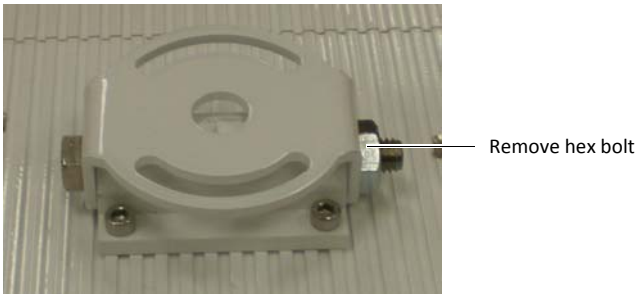
4 Replace the vehicle's headliner and any other parts you removed to install your AutoVu hardware.

Magnetic mount installation

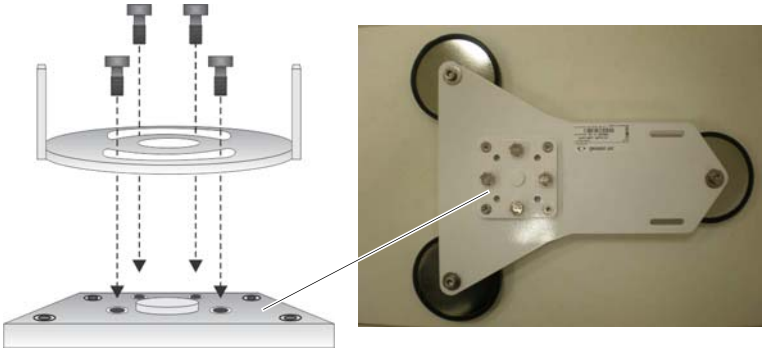
Your AutoVu hardware can be used as a portable LPR solution with a single Sharp camera on a magnetic mount (mag-mount), connected to a breakout box that is plugged into your vehicle's cigarette lighter.

NOTE The mount's magnets are extremely strong, and may be difficult to remove once attached to your vehicle's roof. If you need to adjust your Sharp's position after it is attached, you may find it easier to loosen the bolts rather than attempt to move the entire mount.

1 Locate the circular bracket underneath your Sharp camera, loosen the nut, slide the hex bolt out, and remove the bracket.



2 Remove the four hex bolts from the mag-mount base, and then use them to attach the circular bracket to the mag-mount.



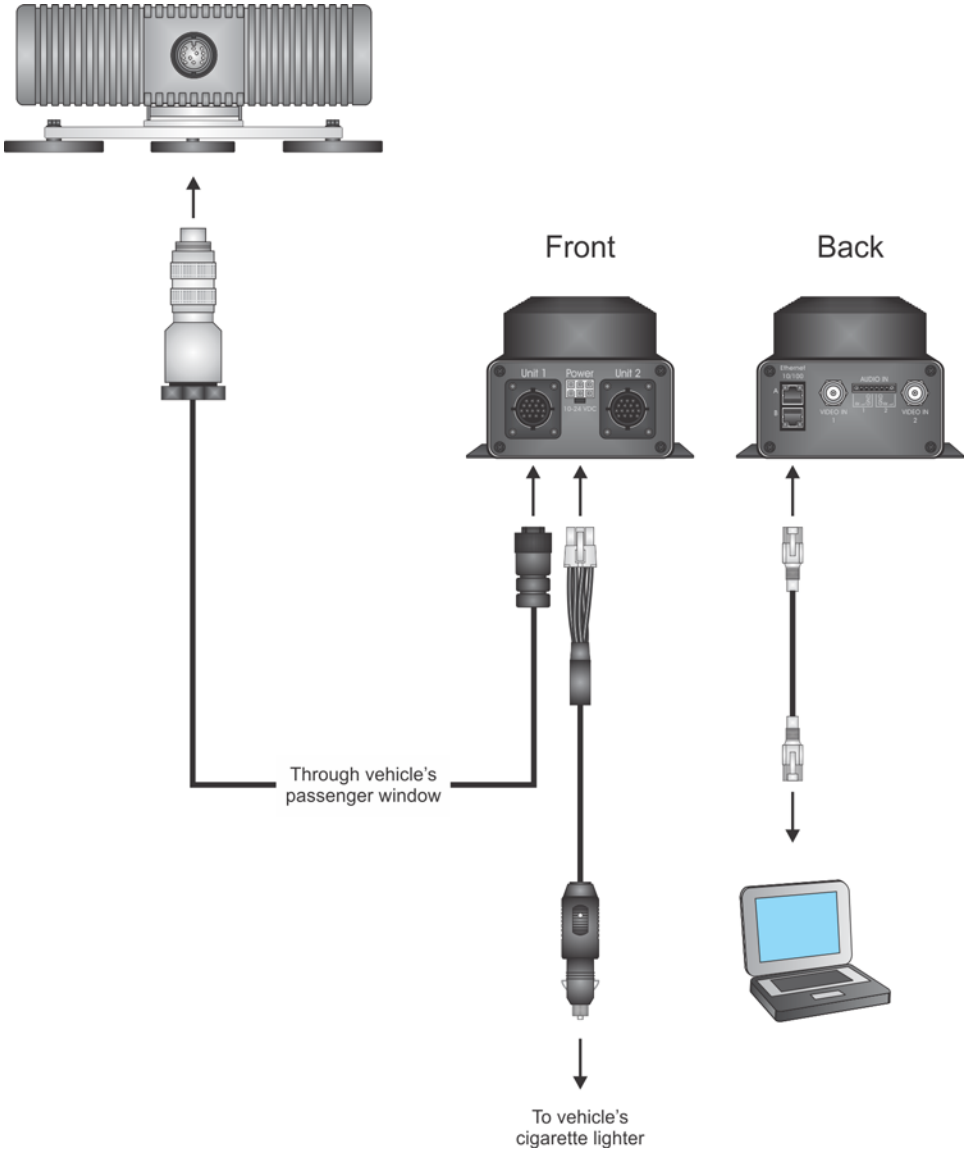
3 Re-attach the Sharp camera to the circular bracket. Don't tighten the bolts until after you have properly positioned the camera.

4 Verify that the roof of your vehicle is clean, dry, and free of debris, and then place the mag-mounted Sharp in the desired position on your roof.

5 Attach the grooved end of the universal window seal to your vehicle's passenger window. You can cut the seal as needed to fit your window.

6 Connect your devices as follows.

IMPORTANT Make sure to tighten the cable connector to the Sharp by turning the connector ring clockwise. Tighten the connector by hand only (no tools).



7 Start your vehicle to verify that your AutoVu hardware, as well as your vehicle's other electrical devices, are working properly.

Mobile installation guidelines for SharpX

Best practice: Observe the following best practices and general warnings when you are choosing where to install the Sharp camera(s).

- Use dielectric gel on the SharpX camera connector.
- Don't bring the SharpX through a mechanical car wash.
- The SharpX camera is IP67 compliant only when the plastic protector cap is on, or when the cable is secured to the camera.
- You can install the LPR Processing Unit on its side, but make sure the heat sink's fins are exposed to as much air as possible (contact your Genetec representative for available mounting brackets).
- You will void the warranty if you open or drill holes in AutoVu equipment, or if you paint, or add decals to a SharpX camera.

Mobile installation procedure for SharpX

For mobile installation procedures for the SharpX, see the printed document *How to Power up and Connect your SharpX (mobile)* that is shipped in the box. This document is also available from the GTAP Documents page.

Part IV

Software installation and upgrade

This part explains how to install and upgrade the different AutoVu software components: Security Center, Patroller, and Sharp camera firmware.

This part includes the following chapters:

9

Installing Security Center

Security Center installation is explained in the *Security Center Installation and Upgrade guide*, available on the GTAP Documents page.

The *Security Center Installation and Upgrade guide* describes the prerequisites for installing Security Center, and provides instructions for installing and upgrading Security Center on your system.

10

Installing AutoVu Patroller

This section explains how to install AutoVu Patroller on the in-vehicle computer.

NOTE See *Patroller 6.1 Administrator guide* for Patroller 6.1 installation instructions.

This section includes the following topics:

System requirements

This section includes the following topics:

Patroller system requirements

For system requirements, see the *Patroller System Requirements* document, available at: http://www.genetec.com/Documents/EN/Products/EN-Genetec-AutoVu-Patroller-System-Requirements.pdf.

SQL Express database requirements

The Patroller setup installs SQL Express 2008 R2 which supports up to 10 GB (that is, approximately 160,000 reads) of data for hotlists, permit applications, and overtime applications with wheel imaging.

Best practice: If you're upgrading Patroller, and you're still using SQL Express 2005, you should let the Patroller setup program install SQL Express 2008 R2.

Increase SQL server memory

If you are using the Sharp with both context and wheel images in high-definition, then you'll need to increase the SQL server memory on the mobile data computer running the Patroller application.

Before you begin: On the Patroller computer you'll need to set the SQL maximum server memory to 1 GB. You can set the SQL server memory from SQL Server Management Studio or from the command prompt.

To change the SQL server memory in SQL Server Management Studio:

1. In Object Explorer, right-click a server and select **Properties**.
2. Click the **Memory node**.
3. Under **Server Memory Options**, enter **1024 MB** in Maximum server memory.

To change the SQL server memory at the command prompt:

1. Depending on the version of SQL running, do one of the following:
   - For SQL 2005, type:

```
cd C:\Program Files\Microsoft SQL Server\90\Tools\Binn
```

   - For SQL 2008, type:

```
cd "C:\Program Files\Microsoft SQL Server\100\Tools\Binn"
```

2 Type the following:

```
Sqlcmd -S (local)\<name of DB server, ex: sqlexpress2005>
sp_configure 'show advanced options', 1
RECONFIGURE WITH OVERRIDE
GO
sp_configure 'max server memory', 1024
RECONFIGURE WITH OVERRIDE
GO
```

Default Patroller ports

This section describes all default ports used by Patroller. You can allow the Patroller setup program to automatically open these ports, or you can open them manually.

Computer	Inbound	Outbound	Port usage
Patroller in-vehicle computer	HTTP 8001		Communication from the LPR Manager role.
	TCP 4545	TCP 4545	Communication from the mobile Sharp units.
	TCP 4546		Time synchonization service for Sharp units.
	TCP 8899		Used by the Patroller's Updater Service to communicate with the mobile Sharp units (mobile Sharps are updated through Patroller).
	TCP 8666	TCP 8666	Used by Patroller and the Plate Reader Server (Sharp software) to communicate with their Updater Service.
		HTTP 2323	Used by the Patroller and the Sharp to determine which Extension to load.
		UDP 5000	Used to discover connected mobile Sharp units.
		TCP 8731	Communication to the LPR Manager role.
		TCP 8889	Used to notify the mobile Sharp's Updater Service to connect to the Patroller's Updater Service on a specific address and port (Updater Service discovery).
		TCP 8832	Used to communicate with the LPR Manager role for updates (used byPatroller's and fixed Sharps).

Before you install

This section lists the things you need to know and do before installing AutoVu Patroller.

This section includes the following topics:

Read the Release Notes

Before you install and upgrade AutoVu, read the *AutoVu Patroller Release Notes* for any known issues and other information about the release. The latest version of the release notes is available from the GTAP Documents page.

(Windows 7 and later) Disable User Account Control

Patroller will not accept remote updates or hotfixes from Security Center when the Windows User Account Control security option is enabled. You must disable it before installing AutoVu Patroller.

NOTE You can ignore this task if you are using Patroller Standalone.

1. Log on to the in-vehicle computer as an administrator.
2. Open the Control Panel, and then click **User Accounts and Family Safety** > **System and Security** > **Change User Account Control settings**.
3. Drag the slider to its lowest setting (**Never notify**), and then click **OK**.
4. Restart the computer.

(Windows 8) Enable Patroller clock synchronization with Security Center

To offload accurate LPR data such as timestamps for reads and hits, users on the Patroller computer must be granted permission to change the computer's system time. This allows the Patroller computer to synchronize its system clock with Security Center.

NOTE You can ignore this task if you are using Patroller Standalone.

1. Log on to Windows as an administrator.
2. Run `secpol.msc`.

   The **Local Security Policy** section of the Microsoft Management Console appears.
3. Go to **Local Policies** > **User Rights Assignment** > **Change the system time**.
4. Click **Add user or group**.

5 Follow the on-screen instructions to add your Patroller users to the list.

NOTE Add their Windows credentials, not their Security Center or Patroller usernames.

6 Restart the computer.

About the AutoVu Patroller installation package

This section includes the following topics:

Where can I find the installation package

The AutoVu Patroller installation package is available on DVD, or for download from the GTAP Product Download page.

NOTE You will need your username and password to log on to GTAP.

Installer languages

The AutoVu installer is available in English and French.

What's not included

The following items are not included with Patroller:

- **In-vehicle mapping.** In-vehicle mapping data is not included in Patroller packages, but can be purchased separately.
- **Customized configurations.** Customized hotlists, permit lists, and overtime configurations are not included with the purchase of AutoVu systems and may be subject to additional fees. Customizing is done by the integrator, the Genetec Technical Team, or both. For more information, contact your Genetec representative.

Installation overview

Install AutoVu Patroller components in the following order:

Phase	Task
1	Read "Before you install" on page 91. This section describes the things you should know and do before you install or upgrade AutoVu Patroller.
2	Depending on how you want to install Patroller, see "Install AutoVu Patroller" on page 95, or "Installing AutoVu Patroller in silent mode" on page 99.
3	"Download latest hotfixes (not applicable to Patroller Standalone)" on page 96.
4	(BeNomad users only) "Install BeNomad files on the in-vehicle computer" on page 97.
5	If you have an anti-virus installed, add the following Security Center executables to your anti-virus safe list to exclude them from virus scans and increase overall performance: • Patroller.exe • PatrollerConfigTool.exe • SecurityDesk.exe • GenetecServer.exe • ConfigTool.exe

Installing AutoVu Patroller

This section explains how you can install and upgrade AutoVu Patroller.

This section includes the following topics:

Install AutoVu Patroller

Before you begin: Read "Before you install" on page 91.

1. Insert the AutoVu installation DVD in your computer's DVD drive, or double-click *Setup.exe* in the root folder of the Patroller installation package.
2. Select the installation language (English or French), and click **OK**.
3. If you are prompted to install any missing prerequisites, click **Install**. A reboot may be required.
4. Once the prerequisite software is installed, In the InstallShield Wizard *Welcome* window, click **Next**.
5. Read and accept the License Agreement, and then click **Next**.
6. In the *Language Selection* page, select the user interface language for AutoVu Patroller applications, and click **Next**.
7. Select the default installation folder, and then click **Next**, or click **Change** to choose a different installation folder.
8. In the *Select Type* window, select **Complete** or **Custom** installation.
9. If performing a Custom installation, click the **Component** icon to display a list of installation choices. Select a component in the list. Under **Feature Description**, the requirements for each component are displayed. To remove the component, click **This feature will not be installed on local hard drive**.
10. To display the available space on the disk volumes of your machine, click **Space**.
11. In the **Patroller Connectivity** page, select whether you want Patroller to connect to Security Center or run in stand-alone mode.
12. If you chose to have Patroller connect to Security Center, select the Patroller configuration you want to install.
13. In the *Maps Configuration Selection* window, select whether to install maps or not.
14. In the **Database Server Selection** window, do one of the following:
    - If SQL database server is not installed on the computer, select **Install a new database server.**

This option will install Microsoft SQL Server 2008 Express Edition and create a database instance called SQLEXPRESS.

- If SQL database server is installed on the computer, and you would like to use this database, select **Use an existing SQL database server**. In the Database Server list, select the existing SQL Server name.

15 Click **Next**.

You'll be prompted to select your database server authentication method:

- *Windows Authentication*. Only users with Windows administrator privileges on the Patroller computer will be able to access the Patroller database.
- *SQL Server and Windows Authentication (mixed mode)*. This is the recommended authentication method. It allows users that don't have Windows administrator privileges to access the Patroller database. You'll need to choose a **Login** and **Password** for the Patroller application to be able to access the database.

  The login and password you choose will be embedded in the Patroller Config Tool *Connection string* (see "General" on page 345).

16 Click **Next.**

You'll be asked to allow the setup program to automatically create firewall rules. This will open the required ports that Patroller needs to communicate with Security Center and the connected Sharp units.

If you don't allow the setup program to open the ports, you'll need to open them manually after the installation is complete.

17 Click **Next**.

18 Click **Install**.

19 When the installation is complete, click **Finish**.

After you are done: Do the following:

- If you did not allow the setup program to automatically create firewall rules, open the default ports described in "Default Patroller ports" on page 90 to ensure that all AutoVu components can communicate with each other.
- "Download latest hotfixes (not applicable to Patroller Standalone)" on page 96.

Download latest hotfixes (not applicable to Patroller Standalone)

AutoVu Patroller hotfixes are available for download on the GTAP *Known Issue and Hotfixes* page, at https://gtap.genetec.com/Library/KnownIssues.

NOTE You will need a username and password to log on to GTAP.

Before you begin: "Install AutoVu Patroller" on page 95.

1 Log on to GTAP.

2 From drop-down lists in the *Known Issues and Hotfixes* page, show issues that have a Hotfix for AutoVu Products.

3 Download the latest AutoVu Patroller hotfixes.

4 Place the hotfixes in LPR Manager, in *root folder**Updates**Patroller**Hotfixes*\<*Patroller version*>.

The LPR Manager analyzes the content of the ZIP file and processes it. You can then update Patroller from Config Tool. For more information, see "Updating AutoVu with hotfixes or service packs" on page 105.

After you are done: (if you're using maps in Patroller) "Install BeNomad files on the in-vehicle computer" on page 97.

Install BeNomad files on the in-vehicle computer

If your AutoVu Patroller license supports mapping, you can use Patroller's default mapping solution *BeNomad* to provide map and reverse geocoding information.

When your AutoVu license is created, you receive an auto-generated email with a zip file containing the *BeNomad* maps for your geographic location, and a unique *.glic* file that contains your license information. You'll need both these files to install *BeNomad*.

Before you begin: (Law Enforcement only) Make sure that you installed the "Maps Engine" during Patroller installation in the *Map Configuration Selection* page.

To install *BeNomad*:

1 Unzip the contents of the *BeNomad* zip file to your computer.

A folder called BeNomad is created.

2 Copy the *BeNomad* folder to the Patroller's *MobileClient* folder on the in-vehicle computer.

The *MobileClient* folder is the main program folder that includes the *Patroller.exe* and *PatrollerConfigTool.exe* files. In a default Patroller installation, this folder is created on the in-vehicle computer at *C:\Program Files\Genetec AutoVu X.Y\MobileClient*.

3 Copy the *.glic* AutoVu license file from the auto-generated email to the *BeNomad* folder on the in-vehicle computer.

4 Open Patroller Config Tool.

5 Go to **Navigation** > **Maps**.

6 From the **Mapping type** list, select **BeNomad**.

7 Click **Apply**.

BeNomad maps are enabled when you start Patroller.

Using Bing for mapping and reverse gecoding

After March 15th 2015, Genetec will no longer support Bing as the default mapping solution. However, you can continue to use Bing for mapping and reverse geocoding by obtaining your own Bing license from Microsoft.

1. Obtain a Bing license from Microsoft.
2. Create a folder called "BingMaps" in the same folder where Security Center is installed. In a default installation the folder is located at: *C:\Program Files (x86)\Genetec Security Center 5.3*.
3. Copy the license key file to the “BingMaps” folder.

Installing AutoVu Patroller in silent mode

This section describes how to install AutoVu Patroller in *silent mode*, an installation method that does not display messages or windows during its progress.

Before you begin: For information on how to perform a silent install of SQL Express, see the GTAP knowledge base article *KBA00728: "How to Perform a Silent Install of SQL Express 2008 R2"* at the following link: https://gtap.genetec.com/Library/KnowledgeBaseArticle.aspx?kbid=728.

This section includes the following topics:

Silent install command

The syntax for calling the AutoVu Patroller installer in silent mode is:

`Setup.exe /L<language> /s /v"/qn <option_list>"`

The following table lists the setup program options.

Option	Description
`/L<language>`	Sets the language used by the installation program. Immediately precedes the four-digit language code. No space is allowed. • `/L1033` for English (default) • `/L3084` for French
`/s`	Sets the setup.exe program to run in silent mode with no user interaction.
`/v"`	Ensures that the options that follow within the quotation marks are sent directly to the *msiecxec.exe* executable. For more information about the possible options, see "Installer options" on page 100.
`/qn`	Runs the install in silent mode.

Option	Description
<*option_list*>"	Sets the installer option list. Each option in the list uses the following syntax: <*option*>=<*value_list*> where <*option*> is an option name, and <*value_list*> is a list of comma-separated values. No space is allowed on either side of the equal sign (=). If the value list must contain spaces, the entire value list must be included between a pair of double quotes preceded by a backslash (\"). The individual options and their values are described in "Installer options" on page 100.

Installer options

The following table lists the installer options.

Option	Description

INSTALLDIR	Specifies the path where the software will be installed.
	`INSTALLDIR=C:\MyChoiceOfFolder`
	`INSTALLDIR=\"D:\Program Files\Genetec AutoVu X.Y\"`
	Note that in the second example, (\") is required because the value contains spaces. If do you not specify a path, it will be installed at *C:\Program Files\Genetec AutoVu X.Y.*

ADDLOCAL	Specifies the features to be installed. • ALL (installs Patroller files and documentation) • Documentation (installs only AutoVu Patroller documentation) If the ADDLOCAL option is omitted, Patroller files are installed without documentation.
DATABASE_SERVER	Database server name. When omitted the default is "(local)\SQLEXPRESS".
SQLSERVER_AUTHENTICATION	Specifies the authentication method used to connect to SQL server. Possible values are 0 or 1. When omitted the default value is 1. • 0 = Windows Authentication • 1 = SQL Server and Windows Authentication. If 1 is specified, you also need to specify SQLSERVER_PASSWORD for the password. **EXAMPLE** `SQLSERVER_AUTHENTICATION=0`
SQLSERVER_DATABASE	Specifies the Mobile database server name.

Option	Description
LANGUAGECHOSEN	Language used by Patroller. The possible code values are: • Arabic - 1025 • Chinese (Simplified) - 2052 • Chinese (Traditional) - 1028 • Czech - 1029 • Dutch - 1043 • English - 1033 • French - 3084 • German - 1031 • Hebrew - 1037 • Hungarian - 1038 • Italian - 1040 • Japanese - 1041 • Korean - 1042 • Norwegian - 1044 • Persian - 1065 • Polish - 1045 • Brazilian Portuguese - 2070 • Spanish - 1034 • Thai - 1054 • Turkish - 1055 **EXAMPLE** LANGUAGECHOSEN=1033 If the code is invalid, English will be used. If this option is omitted, the installation language (specified with the /L option) will be used.
PATROLLER_CONNECTIVITY	Specifies whether or not to connect to Security Center. Accepted values are: • SecurityCenter • Standalone When omitted the default is SecurityCenter.
CONFIGURATION_MAPS_TYPE	Specifies whether or not to use maps. Accepted values are: • UseMaps • DoNotUseMaps When omitted the default is DoNotUseMaps. **EXAMPLE** CONFIGURATION_MAPS_TYPE=DoNotUseMaps

Option	Description
CONFIGURATION_TYPE	Specifies the Patroller configuration type. Accepted values are: • Law • University • City • CityWheelImaging • MLPI **EXAMPLE** CONFIGURATION_TYPE=Law
CREATE_FIREWALL_RULES	Adds the installed Patroller applications to the Windows Firewall exceptions list. Possible values are 0 or 1. When omitted, the default value is 1. • 0 = Do not create Firewall rules • 1 = Create Firewall rules **EXAMPLE** CREATE_FIREWALL_RULES=1
REBOOT	This option allows you to force or suppress a reboot after the installation has ended. Possible values are: • F - To force a reboot when your installation is complete. • S - To suppress any reboot except the one caused by the ForceReboot action. • R - To suppress any reboot caused by Windows Installer actions.

Sample installation commands

EXAMPLE This is the standard installation of AutoVu Patroller in English without any questions. Only the installation path is different.

```
Setup.exe /L1033 /s /v"/qn INSTALLDIR=c:\GENETEC_PATH ADDLOCAL=ALL
DATABASE_SERVER=your database server name SQLSERVER_PASSWORD=your password"
```

EXAMPLE This is equivalent to a Standard Installation in French, in silent mode without any questions.

```
Setup.exe /L3084 /s /v"/qn DATABASE_SERVER=your database server name
SQLSERVER_PASSWORD=your password"
```

EXAMPLE This is equivalent to a Complete Installation in French, in silent mode without any questions. The default database server name “(local)\SQLExpress” is used.

```
Setup.exe /L1033 /s /v"/qn ADDLOCAL=ALL DATABASE_SERVER=your database server name
SQLSERVER_PASSWORD=your password"
```

EXAMPLE This is equivalent to a Complete Installation in French, in silent mode without any questions. The default database server name “your database name” is used.

```
Setup.exe /L3084 /s /v"/qn DATABASE_SERVER=your database server name
SQLSERVER_PASSWORD=your password SQLSERVER_DATABASE=your database name"
```

EXAMPLE This is equivalent to a Complete Installation in English, in silent mode without any questions. This setup will create a log file located in c: drive.

```
Setup.exe /L1033 /s /v"/qn ADDLOCAL=ALL DATABASE_SERVER=your database server name
SQLSERVER_PASSWORD=your password
/L*v C:\Server.log"
```

EXAMPLE Complete Installation in English, in silent mode without any questions. Patroller applications will use Arabic.

```
Setup.exe /L1033 /s /v"/qn ADDLOCAL=ALL DATABASE_SERVER=your database server name
SQLSERVER_PASSWORD=your password LANGUAGECHOSEN=1025"
```

Uninstall AutoVu Patroller in silent mode

To uninstall AutoVu Patroller in silent mode:

- Run the following command from the *Full* folder of the Patroller installation package: `setup.exe /s /v"/qn" /x`

11

Upgrading AutoVu

This section explains how to upgrade the various AutoVu components (e.g. Patroller, Sharp cameras, and other services).

This section includes the following topics:

Updating AutoVu with hotfixes or service packs

This section describes how to install service packs and hotfixes on Security Center server computers, Patroller in-vehicle computers, and mobile or fixed Sharp cameras.

Before you begin: Do the following:

- Download the service pack or hotfix from GTAP.
- In a wireless system setup, connect to the components you want to upgrade. For example, if you want to upgrade Patroller, or upgrade mobile Sharp units, Patroller must first be connected to Security Center (see "Connect Patroller to Security Center" on page 181).

Update using the Security Center updater service

If your AutoVu components are connected to Security Center wirelessly or through a network, you can use the Security Center updater service to push the updates to Patrollers or certain Sharps.

NOTES

- If you have a fixed installation, the Sharp updates are automatically installed after you push the updates from Security Center.
- In mobile installations, the updates are pushed to Patroller, but you'll need to manually accept them using the Patroller interface.
- You can use the updater service to update Patroller with new sound files to use for hotlist hit alerts. To do this, you must first properly zip the files so they extract to the correct folder on the in-vehicle computer (see "Updating Patroller with new sound files" on page 111).
- Certain older Sharp models already deployed in the field may need to be upgraded to use the Security Center updater service. For more information on which Sharps need to be upgraded, and how to upgrade them, contact your Genetec representative.
- Sharp 1.5 and Sharp 2.0 units with 512 MB of RAM cannot be updated using the Security Center updater service, even if they are upgraded to the latest version.

To update 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 for Patroller in Patroller Config Tool.

Security Center creates the *Updates* folder under the *LPR Root Folder* on your computer. This is the folder where you will copy the Genetec zip files that contain the updates.

2 Copy the updates to the LPR Root Folder:

a From the Security Center Config Tool Home page, go to **LPR** > **General settings** > **Updates** to display all the Patroller and Sharp units on your system.

b Click the tab that corresponds to what you want to update:

- **Patroller and Sharp units**
- **Update services**
- **Firmware upgrade**.

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.

For example, if you have a Patroller hotfix, the default **Drop folder** location on the LPR Manager computer is *C:\Genetec\AutoVu\RootFolder\Updates\Patroller\Hotfix\<Current release>*.

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 it is ready to send it 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**.

You'll see an active **Update** button next to the component(s) eligible for an update.

b Click **Update** to update individual components, or click **Update all** to update all eligible components on the list.

You'll know the update was downloaded by the components when the status changes from **Waiting for connection…** to **Synchronized**.

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

If you have a fixed installation, you're finished, the update is automatically installed on the associated Sharps. For a mobile installation you need to manually accept the updates for Patroller and the associated Sharps (see Step 4).

4 (Mobile installations only) Manually accept Patroller and mobile Sharp updates.

a Start Patroller, and log on if required.

b In the Patroller notification bar, tap the Update icon ( ).

The **Update** dialog box appears, listing the Patroller updates that are ready to install.

c Tap the **Patroller** icon to start the update.

Once the update is installed, the Patroller application restarts and the Update icon reappears in the notification bar, indicating there are more updates to install. These updates are for the connected Sharps.

d Tap Update ( ).

The **Update** dialog box appears, listing the Sharp updates that are ready to install.

e Tap the **Sharp** icon to start the update.

The Sharp update is installed on all Sharps connected to Patroller, and the Plate Reader software restarts.

NOTE While Plate Reader is restarting, a message appears saying that the connection to the Sharp has been lost, and the status button in the Patroller notification bar will turn red. Once Plate Reader restarts, click the status button to acknowledge the error. The button will turn grey again (normal). You can also close and re-open Patroller to remove the error.

The Patroller and connected Sharps are now updated. In the Security Center Config Tool **Updates** page, the status for the Patroller unit and its Sharp units changes to **Installed**.

Upgrading Patroller to the latest version

This section explains how to upgrade AutoVu Patroller on your in-vehicle computer.

NOTE Your configuration settings are carried over from the previous version.

Before you begin: Do the following:

- Read the following Release Notes (see the GTAP Documents page) for any known issues and other information about the release:
  - *AutoVu SharpOS Release Notes*
  - *AutoVu Patroller Release Notes 6.1*
  - *Security Center Release Notes 5.2 SR10*
- Offload any remaining data in the Patroller database (see "Offload" on page 361).
- Close Patroller and Patroller Config Tool.

To upgrade Patroller:

1 Run the *Setup.exe* in the root folder of the Patroller installation package.

A message appears indicating that an earlier version of Patroller is installed, and asks you to confirm that you would like to start the upgrade process.

CAUTION After you click **Next** in the installation wizard, you cannot revert to the old version even if you interrupt the installation. You cannot keep two different versions of Patroller installed on the same machine.

2 Click **OK**.

3 Click **Next** to begin the upgrade, or click **Cancel** to stop the installation.

4 Read and accept the License Agreement, and then click **Next**.

5 Select the default installation folder, and then click **Next**, or click **Change** to choose a different installation folder.

6 In the **Select Type** window, select **Complete** or **Custom** installation.

7 If performing a Custom installation, click the **Component** arrow to display a list of installation choices. Select a component in the list. Under **Feature Description**, the requirements for each component are displayed. To remove the component, click **This feature will not be installed on local hard drive**.

8 To display the available space on the disk volumes of your machine, click **Space**.

9 In the **Database Server Selection** window, do one of the following:

- If an SQL database server is not already installed on the computer, select **Install a new database server.**

  This option will install Microsoft® SQL Server 2008 Express Edition and create a database instance called SQLEXPRESS.

- If SQL database server is already installed on the computer, and you would like to use this database, select **Use an existing SQL database server**. In the **Database Server** list, select the existing SQL Server name.

10 Click **Next**.

You'll be prompted to select your database server authentication method:

- *Windows Authentication*. Only users with Windows administrator privileges on the Patroller computer will be able to access the Patroller database.
- *SQL Server and Windows Authentication (mixed mode)*. This is the recommended authentication method. It allows users without Windows administrator privileges to access the Patroller database. Choose a **Password** for Patroller to access the database.

  NOTE The password you choose, along with the username "PatrollerUserDB," will be embedded in the Patroller Config Tool *Connection string* (see "General" on page 345).

11 Click **Next.**

12 Allow the setup program to automatically create firewall rules. This opens required ports that Patroller needs to communicate with Security Center and the connected Sharp units.

13 Click **Next**.

14 Click **Install**.

15 When the installation is complete, click **Finish**.

16 Upgrade the Patroller database:

a Start Patroller.

b In the notification area on the Windows taskbar, right-click the Patroller icon, and then select **Database** > **Drop and exit**.

The **Drop Database** window appears.

c Click **Yes** to delete the database.

Patroller closes when the database is deleted. A new database will automatically be created the next time you start Patroller.

The Patroller upgrade procedure is complete.

After you are done: Do the following:

- If you did not allow the setup program to create firewall rules, open the default Patroller ports (see "Default Patroller ports" on page 90).
- Upgrade Plate Reader on the mobile Sharp units (described in a separate document). For more information, contact your Genetec representative.
- The following Patroller settings are reset to their factory defaults after upgrading:
  - *Patroller window behavior*. The Patroller window's initial size, position, and state (normal, minimized, maximized) are reset. You re-size and re-position the window manually, and you configure the window's state from the User interface section in Patroller Config Tool.

  - *Map rotation behavior.* The option to have the Patroller icon or the map rotate with vehicle movement is reset. You can configure this setting from Patroller's **Options** tab.
  - *Main window display.* The option to display the map or the vehicle's context image in the Patroller main window is reset. You can configure this setting by clicking the thumbnail map or image in the Patroller information panel.
  - *Initial GPS position.* The Patroller's initial GPS position is reset. This will automatically be adjusted as the Patroller vehicle starts moving.
  - *MLPI Selection type.* (Mobile License Plate Inventory only) The way you patrol a parking facility in MLPI is reset. You can choose between **Route** or **Configuration** when selecting a parking facility in Patroller.
  - *Patroller location display.* How Patroller displays the vehicle's current location is reset. You can tap the address in the notification bar at the top of the Patroller window to toggle between displaying the reverse-geocoded address or GPS coordinates.
- You can refer to your old Patroller configuration files to update the current Patroller settings. The files are located on the in-vehicle computer at the default location *C:\Program Files\Genetec AutoVu X.Y\MobileClient\OldConfigFiles.* The configuration files from the earlier versions remain in their original directory.
- If you're using maps, you'll need to install and configure *BeNomad* maps because *MapInfo* is no longer supported (see "Install BeNomad files on the in-vehicle computer" on page 97).

Updating Patroller with new sound files

There are two ways you can update Patroller with new sound files (*.wav* format only) to use for LPR events. You can either copy the new sounds to the Patroller in-vehicle computer manually, or you can use the Security Center updater service to push the sound files to the computer as you would a hotfix or service pack.

This section includes the following topics:

About Patroller sound files

These are the four default sound files Patroller uses for LPR events:

- **HotlistHitEvent.** Used for hotlist hits.
- **OvertimeHitEvent.** Used for overtime hits.
- **PermitHitEvent.** Used for permit hits or shared permit hits.
- **VehicleEvent.** Used for plate reads.

These files are located on the in-vehicle computer in *C:\Program Files\Genetec AutoVu X.Y\MobileClient\Config\Sounds* (default location).

You need to know the following about these default sound files:

- Sounds for overtime hits, permit hits, and plate reads must use the filenames *OvertimeHitEvent*, *PermitHitEvent*, and *VehicleEvent*, and the files must be located in the *Sounds* folder. Patroller will not play new sounds for these events if they have different filenames or if they are in different locations.

  EXAMPLE If you have a file called *alert.wav*, and you want to use it for a permit hit, you must rename your file to *PermitHitEvent* before copying it to the *Sounds* folder (either manually or through the updater service). This way it overwrites the default sound file, and Patroller can play it.

- Sounds for hotlist hits have more flexibility. You can overwrite the default sound *HotlistHitEvent* in the *Sounds* folder, or you can use a different filename for each hotlist loaded in Patroller, as long as you specify the path to each hotlist's sound file in Security Center Config Tool (see "Advanced" on page 308).

  Best practice: Hotlist sound files can be anywhere on the in-vehicle computer, but you should keep them in the same *Sounds* folder as the default sound files. This makes it easier to update them later (see "Using the Security Center updater service" on page 112).

Copying sound files manually

You can manually copy new sound files to the Patroller in-vehicle computer (for example, using a USB key).

Before you begin: See "About Patroller sound files" on page 111.

1 Log on to the Patroller in-vehicle computer.
2 To overwrite any of the default sound files, do the following:
   a Open the folder *C:\Program Files\Genetec AutoVu X.Y\MobileClient\Config\Sounds*.
   b Rename your sound file to match the default file you want to overwrite.
   c Copy your new sound file to the *Sounds* folder so that it overwrites the default file.
3 To use different sound files for hotlists, do the following:
   a Copy your new sound file to any location on the in-vehicle computer.
   b In Security Center Config Tool, specify the path and filename to the sound file on the in-vehicle computer (see"Advanced" on page 308).
   c Do this for as many hotlists as you want.
4 Restart Patroller for your changes to take effect.

Patroller will use the new sound file for the LPR event.

Using the Security Center updater service

The updater service sends all sound files to the Patroller's *MobileClient* folder by default, but all sounds should be in the *Sounds* folder.

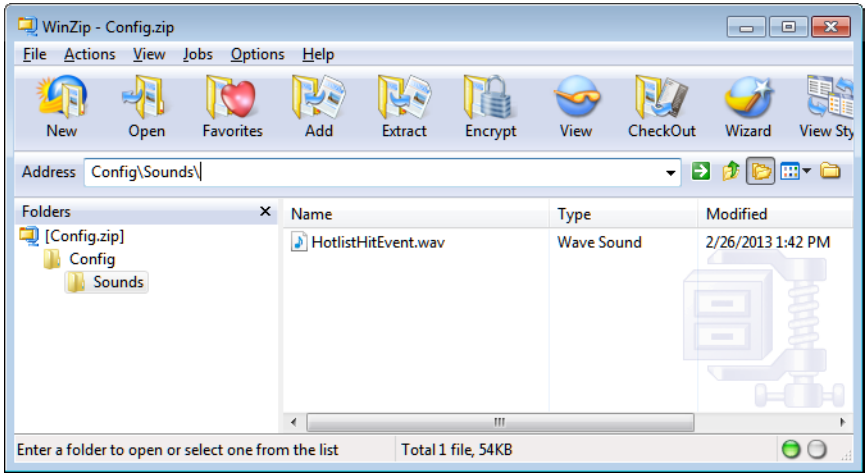
NOTE Sounds for permit hits, overtime hits, and plate reads **must** be in the *Sounds* folder for Patroller to be able to play them.

After sending the files to the *MobileClient* folder, you can manually move the files to the *Sounds* folder if you choose, but you can also zip your sound file so that Windows extracts it to the *Sounds* folder automatically.

Before you begin: See "About Patroller sound files" on page 111.

1 (Optional) If you want to overwrite a default sound file, rename your new sound file to match the name of the default file you want to replace (for example, *HotlistHitEvent.wav)*.
2 On the Security Center computer, create the same Windows Explorer file structure found on the Patroller in-vehicle computer (for example, *C:\Program Files\Genetec AutoVu X.Y\MobileClient\Config\Sounds*).
3 Copy your sound file to the *Sounds* folder you created in Step 2.

4 Zip the sound file at the *Config* level so that it mirrors the relative path from the *MobileClient* folder to the *Sounds* folder on the in-vehicle computer.



This file will now extract to the destination defined in the zip file path (*Sounds* folder).

5 (Optional for hotlist sounds) If the file has a different filename than the default *HotlistHitEvent*, you must specify the full path to the file, including the new filename (see "Advanced" on page 308).

6 Send the sound file to Patroller as if it were a Patroller hotfix (see "Updating AutoVu with hotfixes or service packs" on page 105).

Patroller restarts after installing the update, and will now use the new sound file for your chosen LPR event.

Updating a Sharp unit using the Web Updater

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 **Status** page of the portal.

NOTE The Web Updater does not check to see what version is currently installed before performing the update. Therefore, you should check your current SharpOS version and make sure that the one you are about to install is the most recent. The current version of the SharpOS is displayed in the Portal under the AutoVu logo. You can also click **File versions** under **Actions** on the **Status** page of the portal to see the current version.

Before you begin: Save and run the self extracting *Sharp_Complete_Update_Package_v_10_1.exe* file on the local machine you are using to log on to the Sharp portal. Click here to obtain the file. The update files are extracted to a folder that is named with following format: *SharpOS-version-YearMonthDay*. For example, SharpOS-10.1.-20140505.

To update the Sharp using the Web Updater:

1. Log on to the Sharp portal by entering *http://<Sharp name or IP address>/portal/* in your Web browser.
2. On the **Status** page under actions, click **Update**.
3. In the **Update** dialog box, browse to the location of the folder that contains the update files, and click **Open**.
4. Click **Upload**.

   The files are transferred to the Sharp.
5. Once the transfer is complete, click **OK**.

   The **Update** page opens and under **Applications** you can view which applications will be updated and the versions they will be updated to.
6. Click **Update now** to start updating the Sharp.

   The **Progress** window allows you to monitor the update. Once the upgrade is complete you will receive a message indicating that the upgrade was successful. If the update fails, you will receive a message and an automatic rollback occurs.

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

After you are done: Once the Sharp is updated, you can click **Go to Portal** and verify that your Sharp has been upgraded. You can check your Sharp file versions by clicking **File versions** under **Actions** on the **Status** page of the portal.

Part V

Software configuration

This part explains the software-related procedures required to configure a fixed or mobile AutoVu system. It includes general configuration tasks that apply to all types of AutoVu systems, as well as the additional tasks you'll need to configure for your specific AutoVu installation type (e.g. Law Enforcement, City Parking Enforcement, etc).

This part includes the following chapters:

12

General AutoVu configuration

This section includes the general configuration tasks that apply to all types of AutoVu systems (fixed or mobile).

This section includes the following topics:

Create an LPR Manager

The LPR Manager controls AutoVu-related entities and options. When you install Security Center, one LPR Manager role is created for you automatically, but you may want to add more depending on your installation requirements. For more information, see "LPR Manager" on page 284.

1. Log on to Security Center Config Tool.
2. From the Security Center Config Tool Home page, go to **System** > **Roles**, and then click the **Add** button ().

   The role creation wizard appears.
3. Select the **LPR Manager** role.
4. From the **Server** drop-down list, select the server assigned to this role and click **Next**.
5. Enter the **Specific info** for this role and click **Next**.
   - *Data server.* Type the path you indicate is relative to the selected server.
   - *Database.* Type the path you indicate is relative to the selected server.
   - *Discovery port.* This port is used for the automatic discovery of fixed Sharp units on your network. The default value is 5000.
   - *Listening port.* This port is used to listen for connection requests coming from fixed Sharp units and Patroller applications. The default value is 8731.
6. Enter the **Basic information** for this role and click **Next**.
   - *Entity name.* Enter a name for the LPR Manager.
   - *(Optional) Entity description.* Enter a description for the LPR Manager. For example, you could describe which LPR or Patroller units this LPR Manager will control.
   - *Partition.* Select which existing partition the LPR Manager will belong to, or choose a **New** or **System** partition.

     For more information on partitions, see the Config Tool help.
7. Confirm the information displayed on the **Creation summary** page.
8. Click **Create** and then click **Close**.
9. Click **Apply**.

The LPR Manager entity appears in Role view, with the **Identity** tab displayed.

Configure LPR Manager server, database, and database retention periods

Configure the servers and database assigned to the LPR Manager role. You can add failover capability to the LPR Manager by adding multiple servers. For more information on server and database management, see the *Security Center Administrator Guide*.

1. Log on to Security Center Config Tool.
2. From the Security Center Config Tool Home page, go to **System** > **Roles**, and then click the LPR Manager you want to configure.
3. In the LPR Manager page, select the **Resources** tab, then configure the LPR Manager server and database.
4. Select the **Properties** tab, click **General settings**, and then specify the database retention periods. They are set to 90 days by default.

   For more information, see "General settings" on page 286.
5. Click **Apply**.

Configure LPR Manager root folder

The LPR Manager root folder is the main folder that contains all the information required to manage the entities it controls (e.g. hotlists, permit lists, Patroller configuration files, etc). When you install Security Center, an initial root folder is created automatically on your computer at *C:\Genetec\AutoVu\RootFolder*. However, if you create a new LPR Manager on the same computer, you need to create and configure a new root folder for it.

1. Log on to Security Center Config Tool.
2. From the Security Center Config Tool Home page, go to **System** > **Roles**, and then click the LPR Manager you want to configure.
3. Select the **Properties** tab, click **General settings**, and enter the path to the root folder (create the folder on your computer first).

   Once you have set the root folder, the LPR Manager creates the required subfolders. For more information, see "General settings" on page 286.
4. Click **Apply**.

Configuring hotlists

This section describes how to create and configure hotlists. Hotlists are primarily used in a mobile Law Enforcement configuration, but you can also use them for City Parking Enforcement, University Parking Enforcement, or even in fixed AutoVu installations. Hotlists are not supported in MLPI (Mobile License Plate Inventory) installations.

This section includes the following topics:

Add a hotlist

Before you begin: Create the hotlist text file (*.txt* or *.csv*), and copy it to the LPR Manager root folder located by default at *C:\Genetec\AutoVu\RootFolder\Hotlists*.

1. Log on to Security Center Config Tool.
2. From the Security Center Config Tool Home page, go to **LPR** > **Hotlists**, and then click the **Add** button ( ) to add a hotlist.

   The hotlist creation wizard appears. For information on how to create an entity manually, see the Security Center Administrator Guide.
3. Complete the Basic information.

   For more information, see the Security Center Administrator Guide.
4. Complete the Partition information.

   For more information, see the Security Center Administrator Guide.
5. Click **Next**, **Next**, and **Finish**.
6. Click **Apply**.

The hotlist entity appears in a flat list view that displays all the hotlist entities in your Security Center system.

Configure hotlist properties

You configure the basic hotlist properties (hotlist priority, hotlist path, attributes, and so on) from the hotlist **Properties** tab.

1. Log on to Security Center Config Tool.
2. From the Security Center Config Tool Home page, go to **LPR** > **Hotlists**.
3. Select a hotlist from the list.
4. Select the **Properties** tab.
5. Configure the hotlist path and other hotlist properties.

   For more information, see "Properties" on page 305.
6. Click **Apply**.

Configure advanced hotlist properties

You configure the advanced properties of the hotlist (the color, sound, download frequency, and so on) from the hotlist **Advanced** tab. You can also use wildcard hotlists.

1. Log on to Security Center Config Tool.
2. From the Security Center Config Tool Home page, go to **LPR** > **Hotlists**.
3. Select a hotlist from the list.
4. Select the **Advanced** tab.
5. Configure the hotlist sound file path, color, email address, and other hotlist properties.

   For more information, see "Advanced" on page 308.
6. Click **Apply**.

Activate or deactivate hotlists on the LPR Manager

You can tell the LPR Manager which hotlists you want it to monitor by activating or deactivating any of the hotlist entities in your system.

NOTE When you create a new hotlist, it is active by default.

1. Log on to Security Center Config Tool.
2. From the Security Center Config Tool Home page, go to **System** > **Roles**, and then click the LPR Manager you want to configure.
3. Select the **Properties** tab.
4. Under **File association**, choose which hotlists you want the LPR Manager to manage.

   For more information, see "File association" on page 289.
5. Click **Apply**.

Activate hotlist filtering

Specify the character set that applies to the license plates in your hotlist. For example, if your hotlists contain Japanese characters, select the Japanese character set. You can also specify what the LPR Manager should do if it detects a hotlist with invalid characters, and where to log the filtering information.

1 Log on to Security Center Config Tool.
2 From the Security Center Config Tool Home page, go to **System** > **Roles**, and then click the LPR Manager you want to configure.
3 Select the **Properties** tab.
4 Under **Hotlist filtering**, select the **Character set** that applies to your hotlist.

NOTE Japanese military and private license plates must be kept in separate hotlists.

5 Specify how the LPR Manager should filter invalid hotlist characters.

For more information, see "Plate filtering" on page 291.

6 Click **Apply**.

Configure hotlist privacy settings

Configure Patroller to obscure plate numbers, or exclude plate, context, or wheel images from reads and hits.

1 Log on to Security Center Config Tool.
2 From the Security Center Config Tool Home page, go to **LPR** > **General settings**.
3 Select **Applications**, then configure the privacy settings.

For more information, see "Applications" on page 275.

4 Click **Apply**.

After you are done: You can override these privacy settings on individual hotlists in order to send an email with the LPR data to a specific recipient. To do this, go to the **Advanced** hotlist settings, then turn on **Override privacy for emails**. For more information, see "Advanced" on page 308.

Configuring email notifications for hotlist hits

You can configure Security Center to notify you by email when a hotlist hit occurs.

This section includes the following topics:

About email notifications for hotlist hits

You can configure Security Center to send email notifications when a hotlist hit occurs. There are two types of email notifications you can use:

- **At the hotlist entity level.** Security Center can send an email to a specific recipient when any license plate on a particular hotlist generates a hit.
- **At the license plate level.** Security Center can send an email to a specific recipient when an individual license plate on a hotlist generates a hit. You can specify a different email address for as many individual plates on a hotlist as you want.

The email contains the hit information (matched plate number, Patroller name, user, hotlist name, and priority) in the message body, and optional image attachments.

Before you begin

On the computer hosting the LPR Manager role, you'll need to configure the mail server in Server Admin. For more information on Server Admin, and how to configure the SMTP server responsible for sending email messages in Security Center, see the Security Center Administrator Guide.

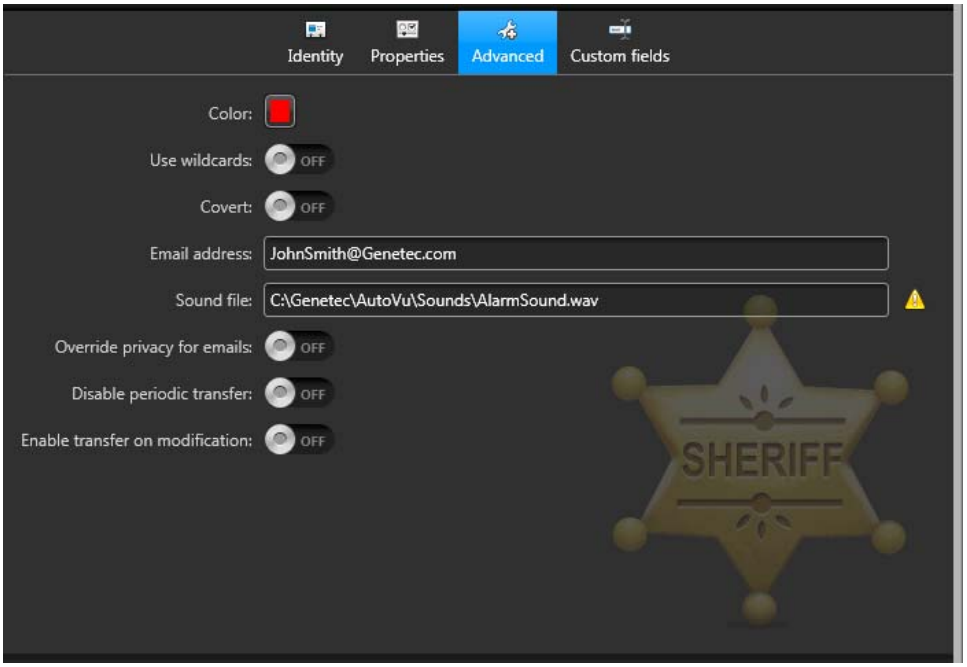
Configure email notifications at the hotlist entity level

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, go to **LPR** > **Hotlists**.

3 Select the hotlist you want to configure, then go to the **Advanced** tab.

4 Under **Email address**, specify the email address you want to notify.



5 Click **Apply**

When any license plate on this hotlist generates a hit, a notification email will be sent to the address you specified.

Configure email notifications at the license plate level

For Security Center to send email notifications when an individual license plate on a hotlist generates a hit, you need to do the following:

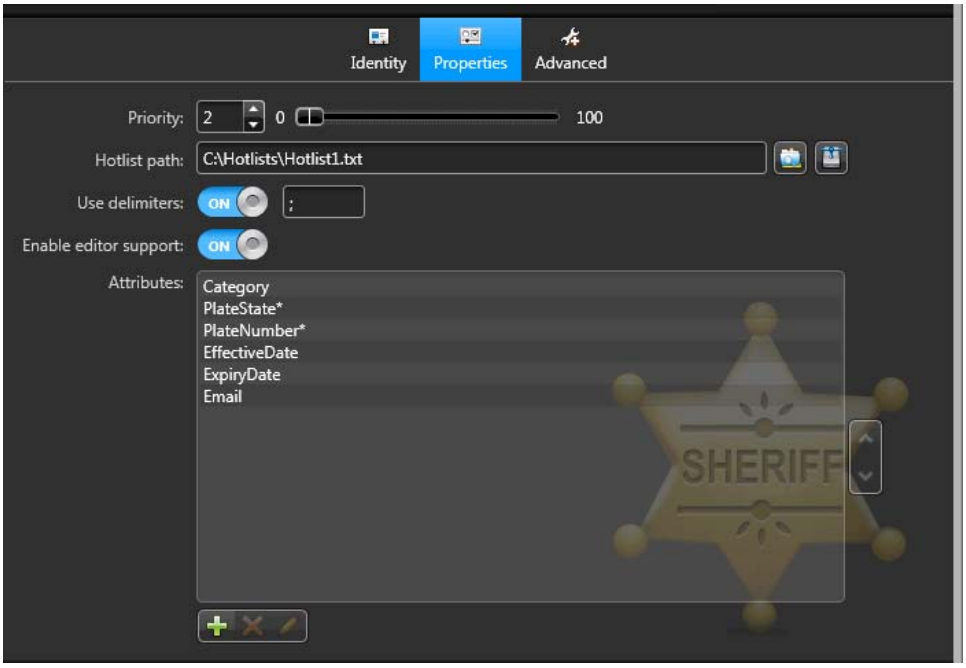
1 Add an email attribute to the hotlist entity:

a Log on to Security Center Config Tool.

b From the Security Center Config Tool Home page, go to **LPR** > **Hotlists**.

c Select the hotlist you want to configure, then go to the **Properties** tab.

d Under **Attributes**, add a new email-related attribute (for example, *Email*) so that Security Center knows to look for email addresses in the hotlist's source file.



NOTE The attribute name *Email* is only an example. You can choose any name you want for the attribute.

e Click **Apply**.

Security Center will now look for email addresses in the hotlist source file.

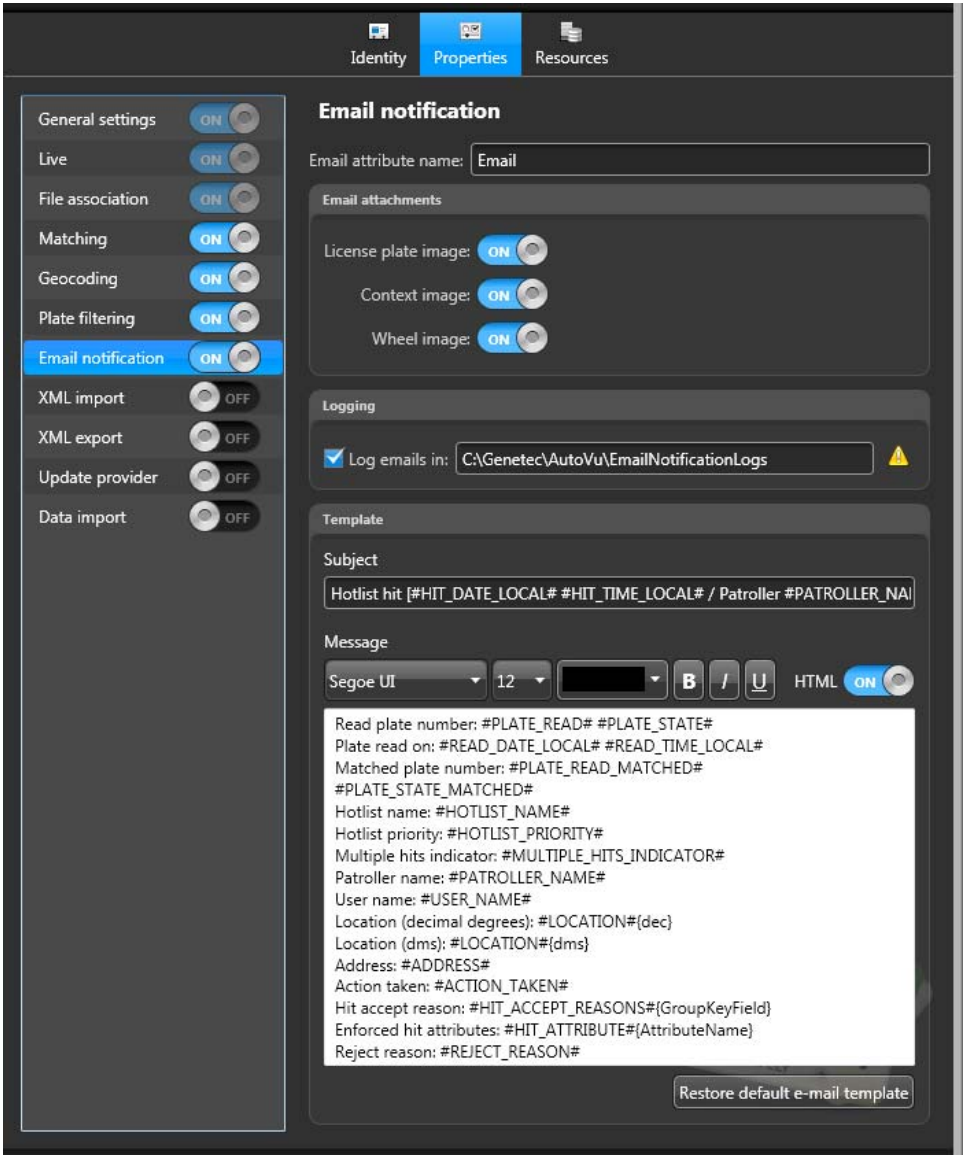
2 Turn on **Email notification** and configure the related settings:

a From the Security Center Config Tool Home page, go to **System** > **Roles**.

b Select the LPR Manager you want to configure and go to the **Properties** tab.

c Turn on **Email notification.**

d For **Email attribute name**, type the same attribute name (*Email*) you created in Step 1.



e (Optional) Under **Email attachements**, specify what information you want the email to contain. For example, you may want to send only the license plate text string without any images to keep the email's file size small.

f (Optional) Under **Logging**, choose where to store the email notification logs. These logs help you keep track of who received email notifications. For more information, see "Email notification" on page 293.

g Click **Apply**.

The LPR Manager now knows that some hotlists contain email addresses for individual license plate entries.

3 Add email addresses in the hotlist source file.

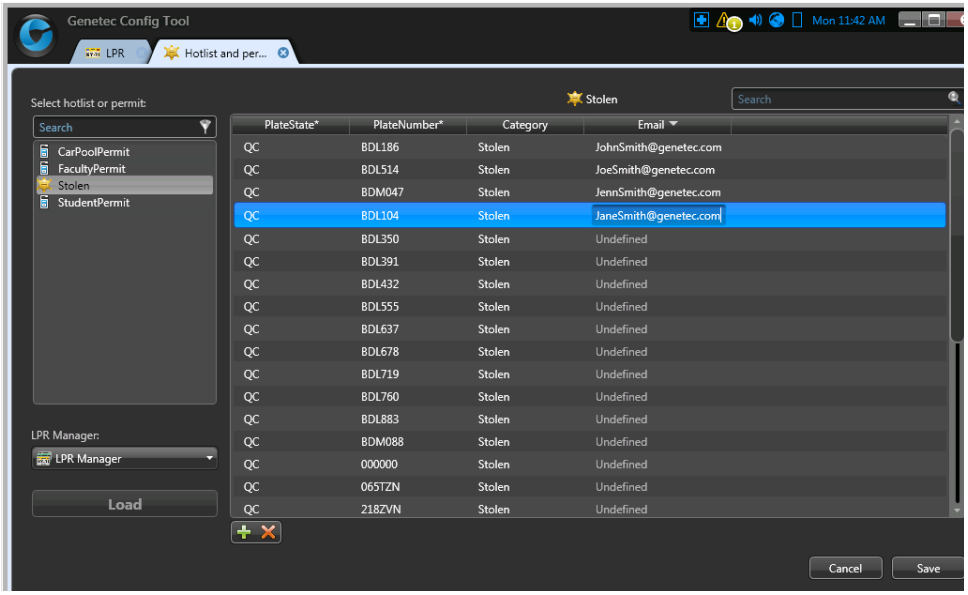
NOTE Since you added the *Email* attribute to the hotlist entity in Step 1, you can now use the *Hotlist and permit editor* to add email addresses. If you prefer, you can also add them directly to the hotlist's source file.

a From the Security Center Config Tool Home page, go to **Hotlist and permit editor**.

NOTE Make sure that **Enable editor support** is turned on. For more information, see "Advanced" on page 308.

b Select the hotlist you want to configure, then click **Load**.

c Add email addresses to as many license plates as needed.



d Click **Save**.

If a plate with an email address generates a hit, an email will be sent to the specified recipient.

Manage large hotlists using Simplematcher

Hotlists with millions of entries (e.g. 2.5 million or more) require much more CPU processing power and memory than smaller hotlists. Turning on the Simplematcher tells Patroller to ignore the `NumberOfDifferencesAllowed` portion of the *MatcherSettings.xml* file, which considerably

reduces the processing load on the Patroller in-vehicle computer. You'll also need to configure the LPR matcher to turn off OCR equivalence. This will ensure that you don't get too many false positive hits.

To turn on Simplematcher:

1 Open Patroller Config Tool.

2 Go to **Operation** > **Hotlists** and then turn on **Use Simplematcher**.

3 Click **Apply**.

After you are done: Turn off OCR equivalence in the LPR matcher (see "Configure LPR matcher settings" on page 141).

(Fixed Sharps only) Turn on hotlist matching

For a fixed Sharp unit to match plates to loaded hotlists, you need to turn on hotlist matching in Security Center Config Tool.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, go to **System** > **Roles**, and then click the LPR Manager you want to configure.

3 Select the **Properties** tab, then turn on **Matching**.

For more information, see "Matching" on page 290.

4 Click **Apply**.

The LPR Manager will then match the reads from the fixed Sharps against the activated hotlists.

Enabling privacy on individual hotlists

This section explains how to enable privacy for individual hotlists. This has the same effect as turning on all the privacy settings found in the LPR administration task, under **General settings** > **Applications** (for more information, see "Applications" on page 275). The only difference is that you can enable privacy on specific hotlists, rather than on all hotlists managed by the LPR Manager.

This section includes the following topics:

About privacy for specific hotlists

If you enable this feature, Security Center will keep the LPR data (e.g. plate numbers, GPS coordinates, date/time, etc), but disassociate that data from the hotlist that generated the hit.

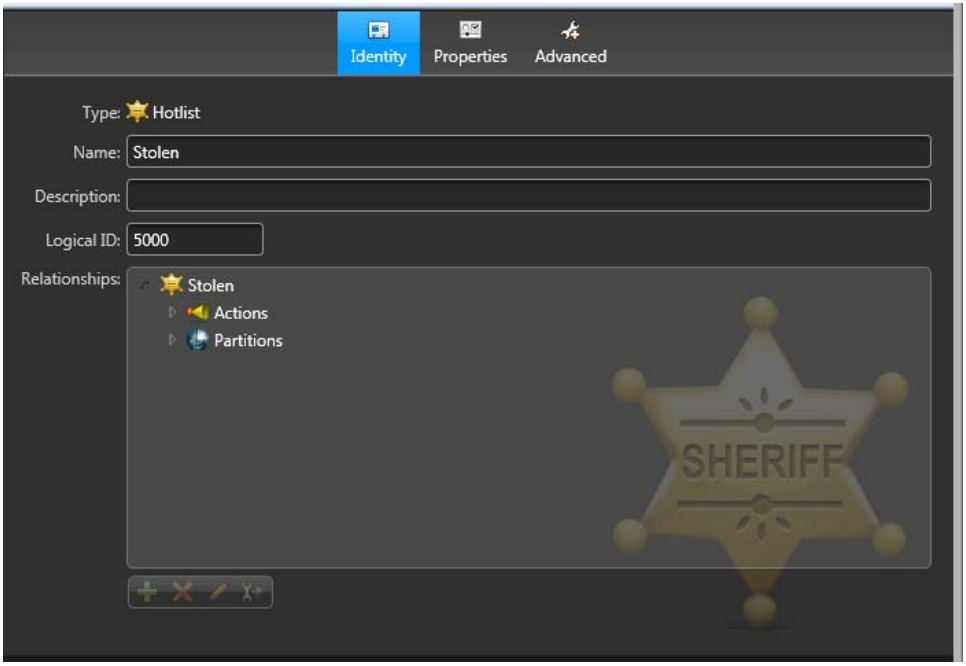
For example, if Patroller generates a hit from a hotlist called "StateWideFelons", you can keep all the LPR data on that hit, but you won't be able to see that the matched license plate was on the "StateWideFelons" hotlist. This allows you to keep the required LPR data, but disassociates the read from the hit on the "StateWideFelons" hotlist.

How to enable privacy on a specific hotlist

Before you begin: To use this feature, you must obtain a special DLL file from Genetec. For more information, contact your Genetec representative.

1. After you have the DLL file from Genetec, copy it to the Security Center root folder (e.g. *C:\Program Files\Genetec Security Center 5.2*).
2. Restart the Directory role from Server Admin:
   a. Open Internet Explorer.
   b. In the address bar, type *http://server IP address:port/Genetec* and press **Enter**.
      Server Admin opens.
   c. Log on to Server Admin.
   d. Under **Directory status**, click **Restart**.
   For more information on how to use Server Admin, see the Security Center Administrator Guide.
3. Log on to Security Center Config Tool.
4. From the Security Center Config Tool Home page, go to **LPR** > **General settings** > **Applications**.
5. Under **Privacy**, turn all the settings off.
   NOTE Enabling privacy on a specific hotlist takes precedence over the global privacy settings for the LPR Manager, but it is still recommended that you turn these settings off to avoid potential conflicts.
6. Click **Apply**.
7. From the Security Center Config Tool Home page, go to **LPR** > **Hotlists.**

8 Click on the hotlist(s) that you want to make private, then go to the **Identity** tab.



9 Under **Logical ID**, enter the value *5000*.

This marks the hotlist, and tells Security Center to make the LPR data private.

10 Click **Apply**.

This specific hotlist is now private, which means that license plate images, context images, and wheel images (if applicable) are not included in the offloaded data, or sent to Security Desk, and the license plate number is replaced by asterisks (*).

After you are done: Mark any other hotlist with a **Logical ID** of 5000 to make the LPR data private. You can do this for as many hotlists as you want.

Using wildcard hotlists

Wildcard hotlists contain entries with only partial license plate numbers. They can be used in situations where witnesses did not see or cannot remember the complete license plate number. This allows the officer to potentially intercept wanted vehicles that may not have been detected using standard hotlists.

This section includes the following topics:

- "About wildcard hotlists" on page 131
- "Activate wildcard hotlists" on page 131

About wildcard hotlists

A wildcard hotlist includes entries that have either one or two asterisks (*) in the license plate number field. The asterisks are the wildcards you use when you don't know the character. Only the plate number field accepts wildcard characters. If the asterisk is found in any other field (e.g. state or province), it is considered as a normal character.

NOTE Please note the following about wildcard hotlists:

- If you activate wildcards on a hotlist, Patroller will ignore all hotlist entries that do not contain a wildcard, or that have more than two wildcard characters.
- It is the number of wildcards in the *PlateNumber* field, and not the location of the wildcard character, that determines how many mismatched characters are allowed before a match can occur.
- The position of the wildcards cannot be enforced because, typically, when witnesses report a partial plate number, they do not remember the position of the characters they missed. The sequence of the normal characters in the *PlateNumber* is respected, such that the three patterns "S*K3*7", "**SK37", and "SK37**" are equivalent.

  EXAMPLE If a wildcard hotlist contains the license plate entry S*K3*7:

  - Plate reads NSK357 and ASDK37 *will* generate a hit because both reads have no more than two mismatched characters (in red) and the sequence "SK37" is respected.
  - Plate read SUKA357, *will not* generate a hit because it contains three mismatched characters (in red).
  - Plate read SKU573 read will not generate a hit because the sequence of characters SK37 is not found in the read.

Best practice: When using wildcard hotlists, observe the following best practices:

- Do not use more than one wildcard hotlist per Patroller.
- Use only one wildcard hotlist per LPR Manager.
- Limit the number of wildcard entries in a hotlist to 100 plates.

Activate wildcard hotlists

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, go to **LPR** > **Hotlists**, and then click the hotlist you want to configure.

3 Go to the **Advanced** tab, and turn on **Use wildcards**.

4 Click **Apply**.

After you are done: Make sure the hotlist is activated in **LPR Manager** > **Properties** > **File association**.

Configuring LPR matcher settings

The LPR matcher is the AutoVu software engine that matches license plates captured by Sharp cameras to license plates in a data source such as a hotlist or permit list, or to previously captured license plates, such as for overtime enforcement. The LPR matcher determines if a plate read results in a hit.

Environment challenges, such as hidden plate characters or damaged plates, can affect the license plate read accuracy rate. The LPR matcher uses a variety of techniques to compensate for these challenges and improve the read accuracy rate. Think of each technique as opening a door wider to let in more possible plate matches. The wider you open the door, the more possible matches you allow, which affects the read accuracy rate.

This section explains the different techniques, describes how to configure them, and lists some best practices on when to use them.

IMPORTANT Before you adjust any LPR matcher settings, test your system with the default settings. If the read accuracy rate meets your requirements, do **not** adjust LPR matcher settings.

This section includes the following topics:

Key concepts

This section explains the logic behind the LPR matcher, and describes the different techniques the LPR matcher uses to compensate for environment challenges affecting the plate read accuracy rate.

This section includes the following topics:

About LPR matcher logic

Real-world conditions make license plate recognition difficult. Some license plates may have characters that are hidden by dirt or snow, while other characters' paint may be faded or chipped. Some license plates have pictures, holograms, or even screws and rivets that can be misread as legitimate license plate characters.

If the LPR matcher were only capable of raising a hit based on an exact match, many plates that should be hits would instead be missed.

EXAMPLE A hotlist contains the plate ABC123. While on a patrol, a Sharp camera reads the license plate ABC12, but is unable to read the last character because the character's paint is chipped. If the LPR matcher were only capable of recognizing an exact match, it would ignore the plate read ABC12. If that last character was in fact a "3", then the patroller just drove past what should have been a legitimate hotlist hit.

The LPR matcher must be capable of more than just "yes/no" logic because the plate read ABC12 *might* be a match. It would be better to raise the hotlist hit, and let the Patroller operator decide whether or not the hit is legitimate. To do this, the LPR matcher uses different levels of "maybe" logic to allow for more possibilities for a plate match.

OCR equivalence

OCR equivalence is the first technique that the LPR matcher uses to improve the plate read accuracy rate.

AutoVu uses Optical Character Recognition (OCR) to convert a license plate image into data that the LPR matcher can read. Depending on the font design, some plate characters can look very similar to other characters. These are called OCR equivalent characters.

A default set of Latin-based characters, plus several Japanese and Arabic characters, are pre-defined in the LPR matcher. You can configure the matcher to allow for one or more of these OCR equivalent characters when looking for a match.

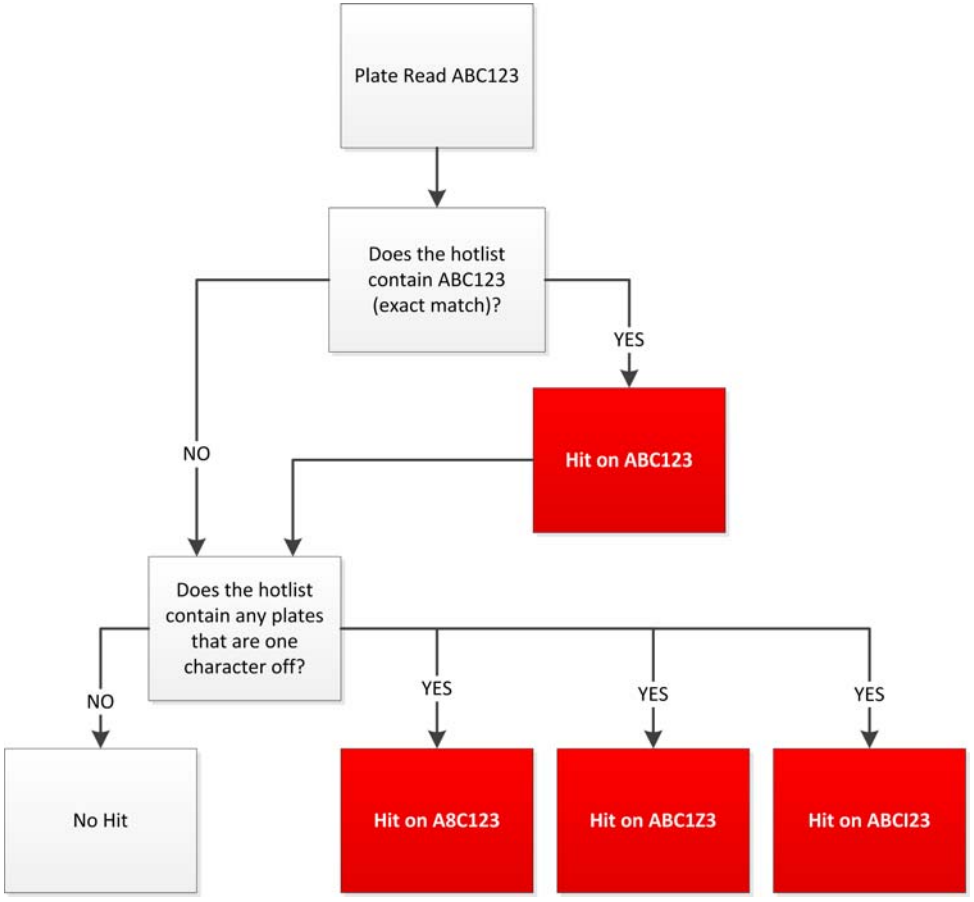
The default Latin-based OCR equivalent characters are the following:

- The number "0" and the letters "O", "D", and "Q".
- The number "1" and the letter "I".
- The number "2" and the letter "Z".
- The number "5" and the letter "S".

- The number “8” and the letter “B”.

Best practice: You shouldn’t allow more than two OCR equivalent characters because it would result in too many false-positive matches.

EXAMPLE The following example uses a hotlist with the LPR matcher configured to allow for *one* OCR equivalent character:



The LPR matcher finds the exact match ABC123 in the hotlist and raises a hit. It also looks for any plates that are one OCR equivalent character off, and finds A**8**C123, ABC1**Z**3, and ABC**I**23 in the hotlist, so it raises hits on them as well.

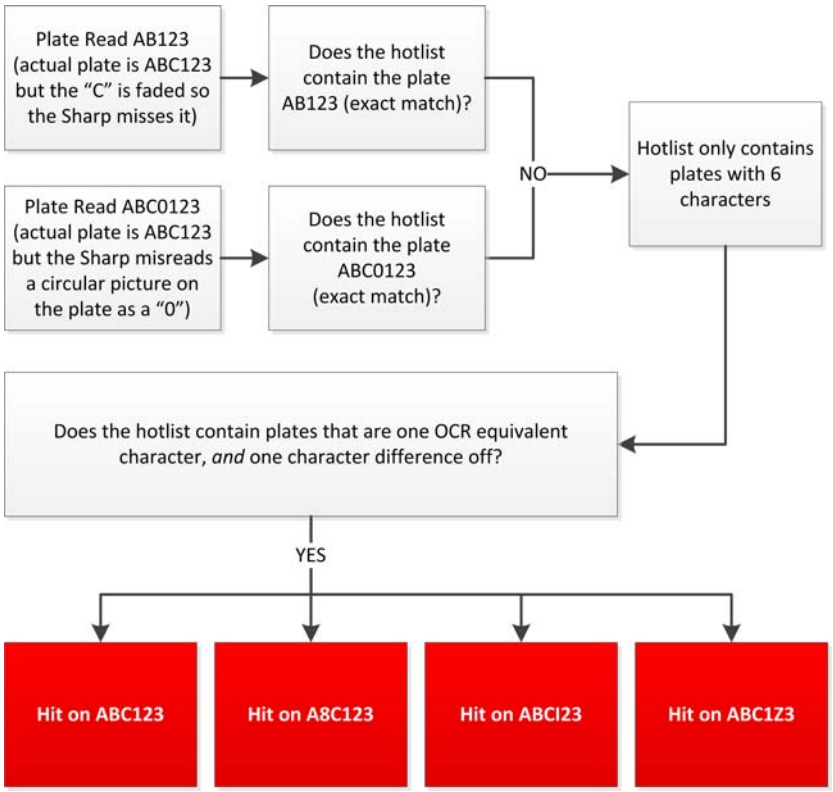
If the LPR matcher found the plate A**8**C**I****Z**3 (*three* OCR equivalent characters off), it would not raise a hit. By configuring the LPR matcher to allow for only one OCR equivalent character, you’ve decided that anything more than that is not visually similar enough to the plate read for the LPR matcher to consider it a match.

Allowing for differences in the number of characters

The second technique the LPR matcher uses to improve the plate read accuracy rate is to allow for a difference in the number of characters between the plate read and the plate number in the data source (a hotlist for example).

This technique is used to account for characters in the plate that cannot be read (faded paint, dirt, bad camera angle, and so on), and to account for objects on the plate that might be mistaken for a legitimate character (screws, rivets, pictures, and so on).

EXAMPLE The following example uses a hotlist with the matcher configured to allow for *one* OCR equivalent character, and *one* difference in the number of characters allowed:



Because you allowed for one OCR equivalent character *and* one character difference, the LPR matcher looks for both before it allows a match. This results in the following:

- There's no exact match possible for plate reads AB123 and ABC0123 because the hotlist contains only six-character plates.
- Both plate reads AB123 and ABC0123 match the plate ABC123 because you allowed for one character difference. It doesn't matter if it is one character more, or one character less than the matched plate.

- Both plate reads AB123 and ABC0123 match the plates A**8**C123, ABC**I**23, and ABC1**Z**3 because you allowed for one character difference, *and* one OCR equivalent character.
- If you were using a permit list instead of a hotlist, *none* of the matched plates in the example would raise hits (you get a permit hit when a plate is *not* on the permit list).

Common and contiguous characters

The third technique the LPR matcher uses to improve the plate read accuracy rate is actually two techniques in one. It allows for common and contiguous characters (sometimes called "fuzzy matching"), and is used for overtime parking enforcement only:

- **Necessary common characters.** The minimum number of characters that need to be common to both the first and second plate read. The characters must also appear in the same order in the plate, but not necessarily in sequence.
- **Necessary contiguous characters.** Minimum character sequence length between the first and second plate read.

In overtime enforcement, there is an extra margin of error because the LPR matcher is comparing a plate read against another plate read, not against a hotlist or permit list created by a human being.

EXAMPLE Here's an example with the LPR matcher configured to look for the default five common characters and four contiguous characters. The LPR matcher also allows for the default one OCR equivalent character, which can count as a common or contiguous character.

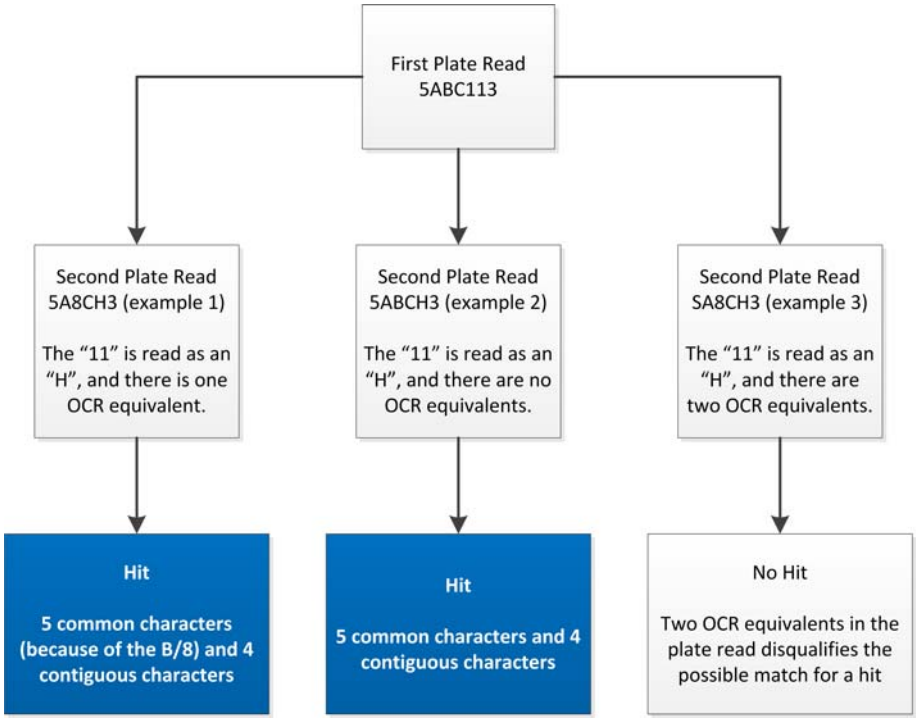


Plate read 5ABC113 matches with 5A8CH3 (example 1) and 5ABCH3 (example 2) because the following conditions are met:

- **OCR equivalence.** The OCR equivalents B and 8 are considered the same character and apply towards the common and contiguous character count.
- **Five common characters.** Both reads have 5, A, B/8, C, and 3 in common, and they all appear in the same order. The "3" is not in sequence, but it respects the order.
- **Four contiguous characters.** Both reads have 5, A, B/8, and C in sequence.

Plate read 5ABC113 does *not* match with SA8CH3 (example 3) because there are two OCR equivalents in the second read (S/5 and B/8). You allowed for only one OCR equivalent.

Using common and contiguous characters helps reduce the margin of error involved when both first and second plate reads are coming from the Sharp.

About the MatcherSettings.xml file

The *MatcherSettings.xml* file contains the LPR matcher settings for the techniques described in "Key concepts" on page 132; that is, OCR equivalence, number of character differences, and common and contiguous characters.

The file is located on the computer hosting the Security Center Directory role, in the folder *C:\Program Files\Genetec Security Center 5.2*.

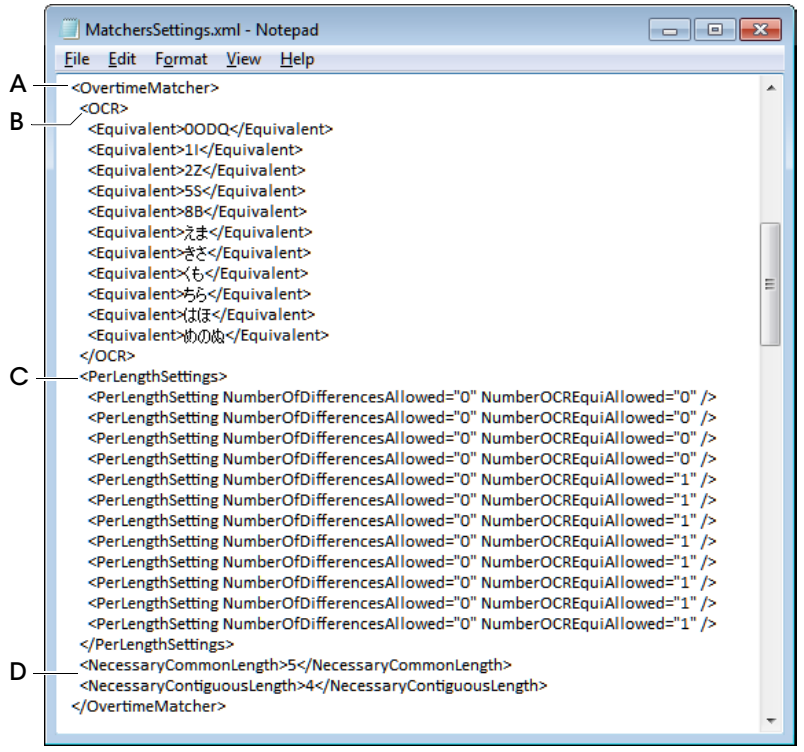
NOTE If you have a mobile AutoVu system, a copy of the same file is located on the Patroller in-vehicle computer. You make your changes in the Security Center version of the file. The file on the Patroller computer will then be overwritten the next time Patroller connects to Security Center wirelessly, or when you manually transfer Patroller settings with a USB key.

The *MatcherSettings.xml* file is composed of `<Matcher>` tags that define the settings for each type of matching scenario:

- **<HotlistMatcher>.** Settings for matching plate reads with hotlists.
- **<OvertimeMatcher>.** Settings for matching a plate read against all other plate reads in the Patroller database.
- **<PermitMatcher>.** Settings for matching plate reads with permit lists.
- **<MLPIMatcher>.** Settings for reconciling inventories in Security Desk.

The structure of the *MatcherSettings.xml* file allows you to have different behavior for the different enforcement scenarios. For example, to maximize your plate read accuracy rate in an enforcement scenario that includes both permits *and* hotlists, you'll typically want to use only OCR equivalence for the hotlist matcher, but also allow one difference in the number of characters for the permit matcher to decrease false-positives.

Here is an example of the *MatcherSettings.xml* file:



```
<OvertimeMatcher>
 <OCR>
  <Equivalent>0ODQ</Equivalent>
  <Equivalent>1I</Equivalent>
  <Equivalent>2Z</Equivalent>
  <Equivalent>5S</Equivalent>
  <Equivalent>8B</Equivalent>
  <Equivalent>えま</Equivalent>
  <Equivalent>きさ</Equivalent>
  <Equivalent>くも</Equivalent>
  <Equivalent>ちら</Equivalent>
  <Equivalent>はほ</Equivalent>
  <Equivalent>めのぬ</Equivalent>
 </OCR>
 <PerLengthSettings>
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
 </PerLengthSettings>
 <NecessaryCommonLength>5</NecessaryCommonLength>
 <NecessaryContiguousLength>4</NecessaryContiguousLength>
</OvertimeMatcher>
```

A	Matcher-specific settings	Each enforcement type (hotlist, permit, overtime, and MLPI) has its specific settings listed between the opening and closing `<Matcher>` tags. **EXAMPLE** Overtime matcher settings are listed between `<OvertimeMatcher>` and `</OvertimeMatcher>`.
B	OCR equivalent characters	The default OCR equivalent characters for each enforcement type are listed as between `<OCR>` and `</OCR>`. **NOTE** This tag does not *enable* OCR equivalence, it only defines the OCR equivalent characters. You enable OCR equivalence by defining how many OCR equivalent characters you want to allow in the PerLength settings.

C	PerLength settings	For each matcher, specify the number of differences allowed, and the number of OCR equivalents allowed for license plates of different character lengths. Here are some best practices for editing `PerLengthSettings`: • There are 12 `PerLengthSetting` lines, each containing `NumberOfDifferencesAllowed` and `NumberOCREquiAllowed` tags. • Each `PerLengthSetting` line corresponds to a plate character length. The line you edit depends on the number of characters on the license plates in your patrol region. • Ignore the first line because it represents plates with zero characters. The second line represents plates with one character, the third line represents plates with two characters, and so on for a maximum of 11 possible plate characters. • You can edit more than one line to apply settings to plates of different character lengths. **EXAMPLE** These are the default `PerLengthSettings`. No differences are allowed, and one OCR equivalent is allowed for plates that have 5 to 11 characters.

```
<PerLengthSettings>
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
</PerLengthSettings>
```

D	Common and contiguous character settings	These settings apply to the Overtime matcher only. • **<NecessaryCommonLength>.** Specify the minimum number of characters that need to be common to both the first and second plate read. The characters must also appear in the same order in the plate, but not necessarily in sequence • **<NecessaryContiguousLength>.** Minimum character sequence length between the first and second plate read.

Configure LPR matcher settings

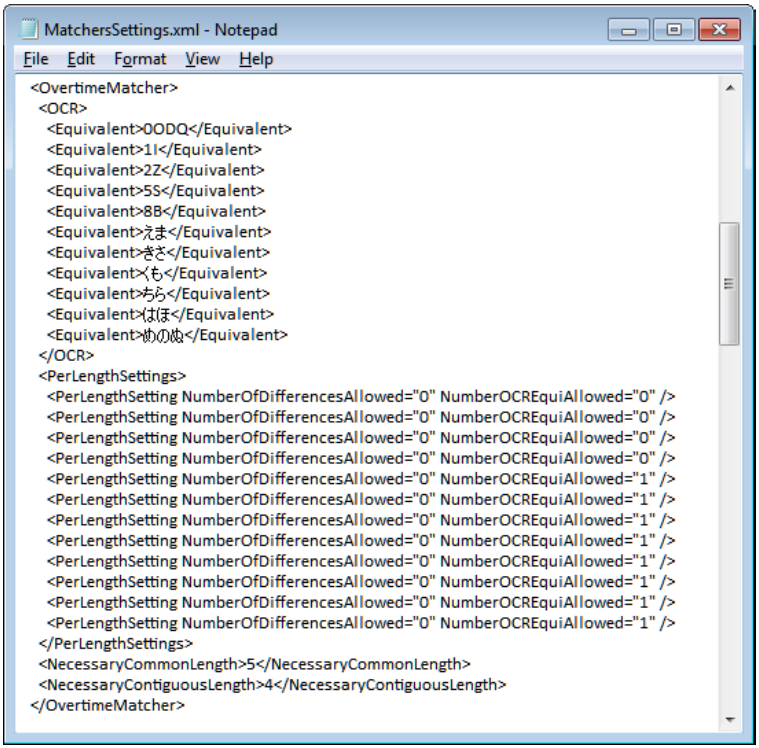
You configure LPR matcher settings in the *MatcherSettings.xml* file, and then apply your changes in Server Admin and the Server Admin console.

NOTE This procedure uses the overtime matcher as an example, but the same steps apply to all the matchers in the xml file.

1 On the computer hosting the Security Center Directory role, open Windows Explorer and then go to *C:\Program Files\Genetec Security Center 5.2*.

2 Open *MatcherSettings.xml* in Notepad or a similar text editor.

MatcherSettings.xml opens.



```
<OvertimeMatcher>
 <OCR>
  <Equivalent>0ODQ</Equivalent>
  <Equivalent>1I</Equivalent>
  <Equivalent>2Z</Equivalent>
  <Equivalent>5S</Equivalent>
  <Equivalent>8B</Equivalent>
  <Equivalent>えま</Equivalent>
  <Equivalent>きさ</Equivalent>
  <Equivalent>くも</Equivalent>
  <Equivalent>ちら</Equivalent>
  <Equivalent>はほ</Equivalent>
  <Equivalent>めのぬ</Equivalent>
 </OCR>
 <PerLengthSettings>
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
 </PerLengthSettings>
 <NecessaryCommonLength>5</NecessaryCommonLength>
 <NecessaryContiguousLength>4</NecessaryContiguousLength>
</OvertimeMatcher>
```

3 Add or remove OCR equivalent characters from the list.

The default OCR equivalent characters are listed between the `<OCR>` and `</OCR>` tags. Add new `<Equivalent>____</Equivalent>` lines, or delete the lines you don't want.

4 Specify the number of character differences you want to allow.

Edit the `PerLengthSetting` line that applies to the plates in your region. For example, Quebec plates typically have six or seven characters, so edit the `NumberOfDifferencesAllowed` value in the sixth and seventh `PerLengthSetting` lines.

NOTE A value of "0" turns the setting off.

5 Specify the number of OCR equivalent characters you want to allow.

Do the same thing you did in Step 4, except edit the `NumberOCREquiAllowed` value instead. This turns on OCR equivalence.

NOTE A value of "0" turns the setting off.

6 (Overtime only) Specify the number of common and contiguous characters.

For common characters, edit the `NecessaryCommonLength` value. For contiguous characters, edit the `NecessaryContiguousLength` value.

7 Save and close the text editor.

8 Apply the LPR matcher settings in the Server Admin console:

a From a web browser, open the Server Admin console by typing *http://<server>/genetec/console#/Commands*.

b From the **All commands** page, click **UpdateAutoVuGlobalSettings**.

c Close the Server Admin console.

9 Restart the Security Center Directory.

a From a web browser, open Server Admin by typing *http://<server>/genetec*.

b Click the **Directory** tab.

c Under **Directory status**, click **Restart**.

d After the Directory restarts, close Server Admin.

LPR matcher settings are now configured and applied to all the LPR Manager roles on your system. Patroller units will be updated the next time they connect to Security Center wirelessly, or when you manually transfer Patroller settings using a USB key.

After you are done: Verify that your LPR Manager roles have been updated by looking at the *MatcherSettings.xml* file in their corresponding root folders (*C:\Genetec\AutoVu\RootFolder\ManualTransfer\General*). You can also tell by the xml file's *Date modified* field that it has been updated.

Best practices for LPR matcher settings

How you configure the LPR matcher depends on your enforcement scenario. In some AutoVu systems, you'll want an exact match only. In other systems, you'll benefit from having a false positive on a potential match because it decreases the chances of missing a vehicle of interest.

Use the following best practices when configuring LPR matcher settings:

- **Exact match.** The LPR matcher always looks for an exact match if possible, but you can configure it to allow *only* exact matches. This is typically used when you have very large hotlists (millions of entries). By limiting the number of possible matches, you lighten the processing load on the Patroller computer, and you decrease the amount of false positives that you would normally get from a list of that size.

To allow only exact matches, turn on the *Simplematcher* feature in Patroller Config Tool (see "Manage large hotlists using Simplematcher" on page 127), and turn off OCR equivalence (see "Configure LPR matcher settings" on page 141).

- **OCR equivalence.** By default, the LPR matcher allows for one OCR equivalent character. You can allow as many as you want, but generally you should not allow more than two because you'll get too many false positives.
- **Number of differences allowed.** By default, the LPR matcher does not allow any number of differences. The number you allow depends on the plates in your region. The more characters on a plate, the more differences you can allow, but generally you should not allow more than two because you'll get too many false positives.
- **Common and contiguous characters.** (Used for overtime enforcement only) By default, the LPR matcher looks for five common, and four contiguous characters to generate an overtime hit. The number you specify depends on the plates in your region. The more characters on a plate, the more common and contiguous characters you can allow.

Configuring the Sharp for an FTP connection

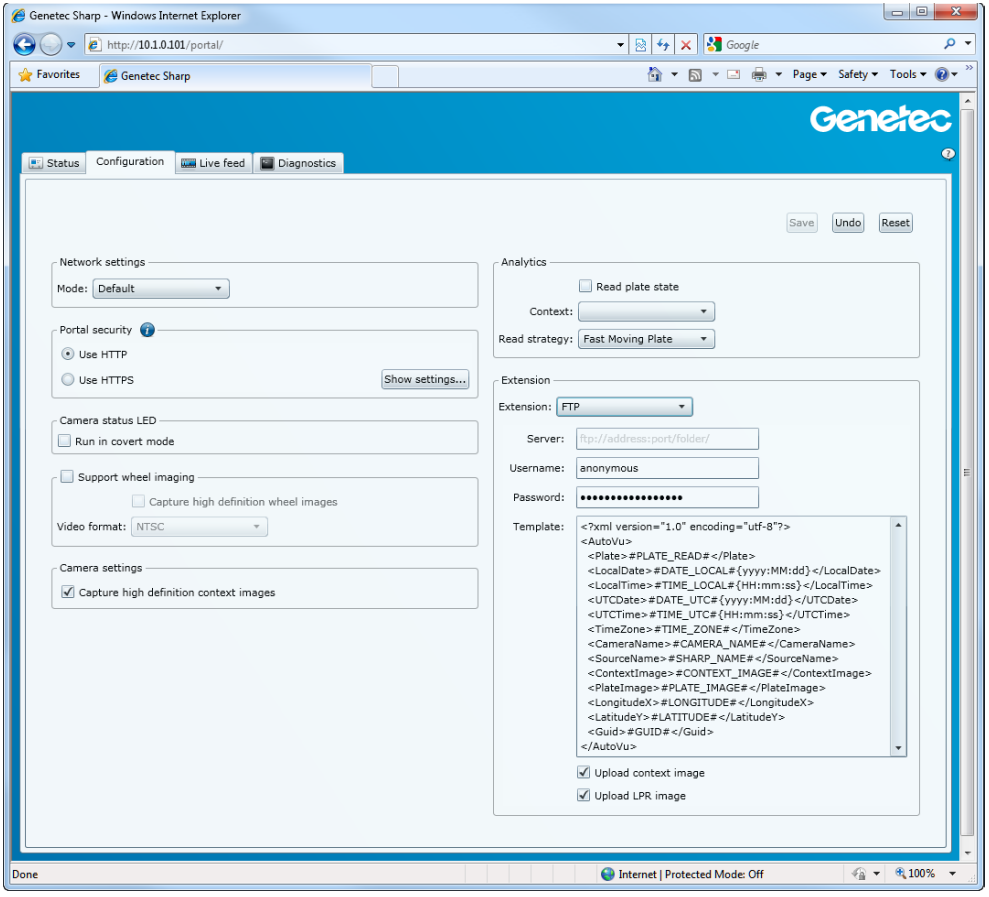
This section describes how to set the Sharp to send LPR data to an FTP server instead of to Patroller or Security Center.

This section includes the following topics:

Configure the Sharp for FTP

1 Log on to the Sharp Portal.

2 Go to the **Configuration** page.



3 Under **Extension**, 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.* Username for the FTP server.
- *Password.* Password for the FTP server.
- *Template.* Modify the FTP XML.
- *Upload context image.* Export the context image (in JPEG format).
- *Upload LPR image.* Export the plate image (in JPEG format).

4 Click **Save**.

Modify the FTP XML

The xml code defines the structure of the xml files generated by the Sharp. You can re-sort or remove any of the fields. The xml file name consists of the Sharp name and a unique identification number (for example, SHARP0015_6ee17b00-82c1-466b-9fd6-003417bc82c4_lpr.xml).

Template:

```
<?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)</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>
```

NOTES

- 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 (see "Connect Sharp units to Patroller" on page 182).
- `SourceName` is the Sharp name (e.g. Sharp1234).
- `ContextImage` and `PlateImage` are encoded into text.

- `Guid` is the unique identification of the event read.
- You can add the following custom fields to the template:
  - *State Name.* The Sharp will attempt 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 `<PlateState>#CUSTOM_FIELDS#{State Name}</PlateState>` to the xml, and then select **Read plate state** in the Sharp Portal (see "If there is a warning associated with a camera, there will be a yellow warning icon next to the interface number. Hover your mouse over the warning icon to see the details." on page 377).

    NOTE Note the following:

    - The LPR Context you are using must support the state name feature.
    - The Sharp must be able to correctly read the plate state from the license plate.
  - *Relative Motion.* When the Sharp 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 Sharp can read these symbols, it will display 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)</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 Sharp Portal security

The first time you connect to the Sharp Portal, it is over a non-encrypted HTTP connection. After you connect, you can then configure the Sharp Portal to accept logons with SSL encryption (HTTPS). To do this, you'll need an SSL certificate. You can either use the included Genetec SSL certificate, or use a signed certificate from a Certificate Authority such as VeriSign.

This section includes the following topics:

Why use encryption?

When you log on to the Sharp Portal over a non-encrypted connection, anyone on the network can read the data transmitted (including the password). This isn't a problem if you're on a private network only accessible by authorized personnel, or if you're in a vehicle (which *is* a private network). However, if you're on a public network, you should use the HTTPS protocol to log on to the Sharp because the logon credentials and the data transmission (except for the video feed) are encrypted.

Configure encryption with a Genetec certificate

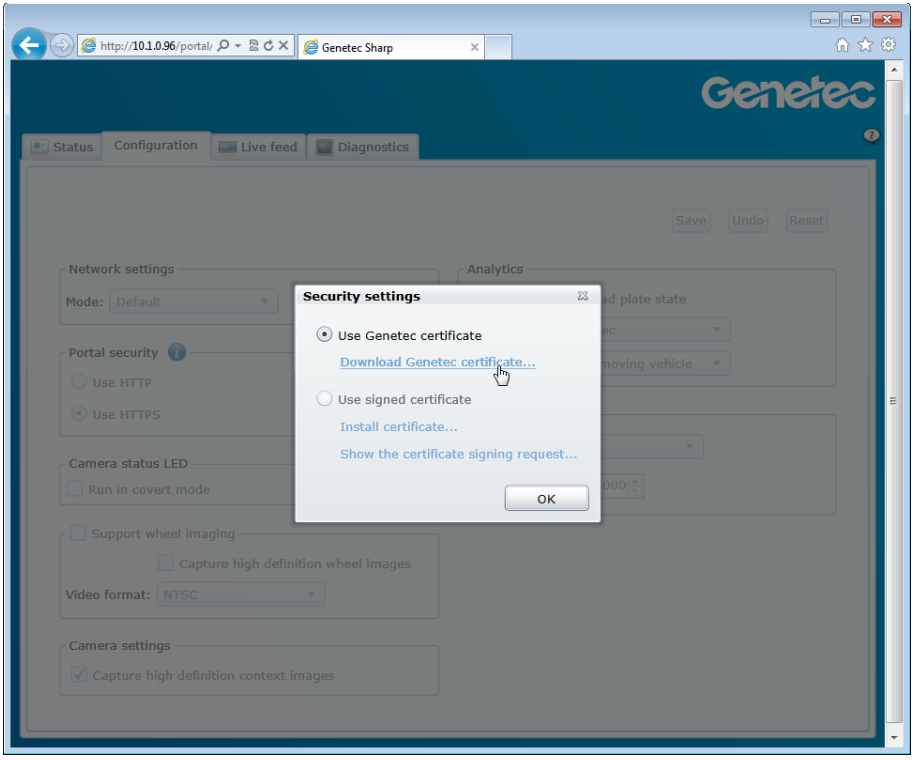
This section explains how to configure Sharp Portal encryption using an SSL certificate generated by Genetec. If you use a Genetec certificate, you can also install the certificate on your client machine (e.g. the machine used to log on to the Sharp Portal).

1 Log on to the Sharp Portal.

2 Go to the **Configuration** page.

3 Under **Portal security**, select **Use HTTPS**, then click **Show settings**.

The **Security settings** window appears.



4 Select **Use Genetec certificate**, then click **OK**.

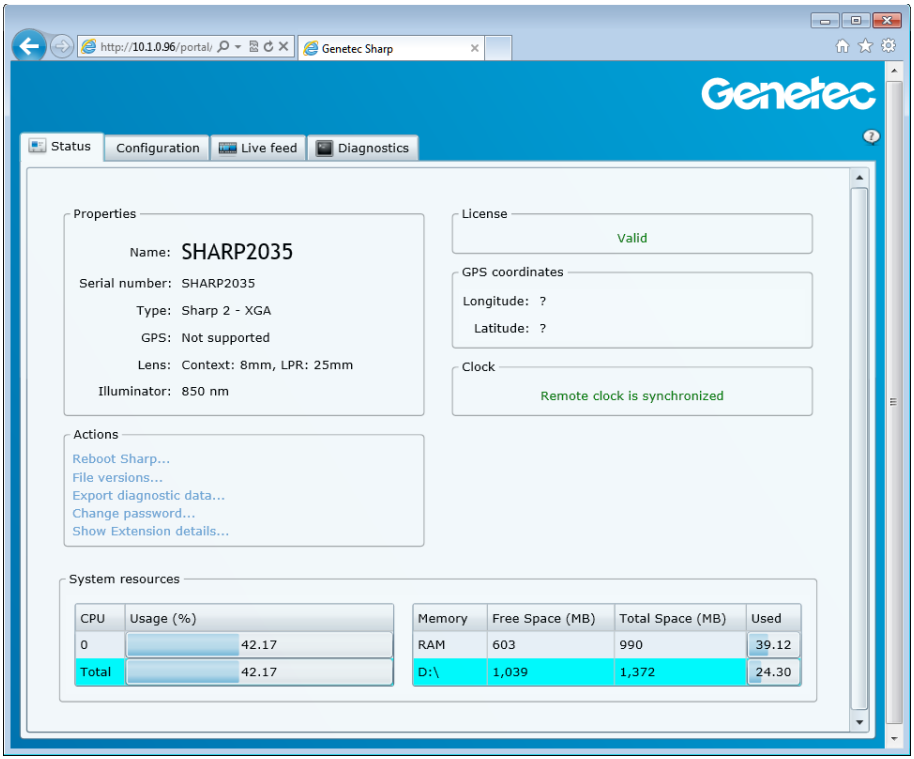
You'll return to the Configuration page.

5 Click **Save**.

You'll be asked to confirm your changes.

6 Click **OK**.

7 Go to the **Status** page.



8 Restart the Sharp unit.

9 Log on to the Sharp Portal using HTTPS in the address bar instead of HTTP.

NOTE If you see a warning saying there is a problem with the website's security certificate, do one of the following:

- To remove the warning, install the certificate on the client machine. For more information, see "Install the Genetec certificate on the client machine" on page 151.
- Disregard the warning and continue to the Sharp Portal.

  NOTE The warning does not indicate that the Sharp Portal is not encrypted, it only means that the certificate is not signed by a Certificate Authority (e.g. VeriSign), or is not recognized by Windows. Rest assured that even if you see the warning, the connection is properly encrypted.

You are now logged on to the Sharp with a secure connection.

After you are done: From the Sharp Portal's **Status** page, click **Change password**, and change the default password from "Genetec" to something else.

Install the Genetec certificate on the client machine

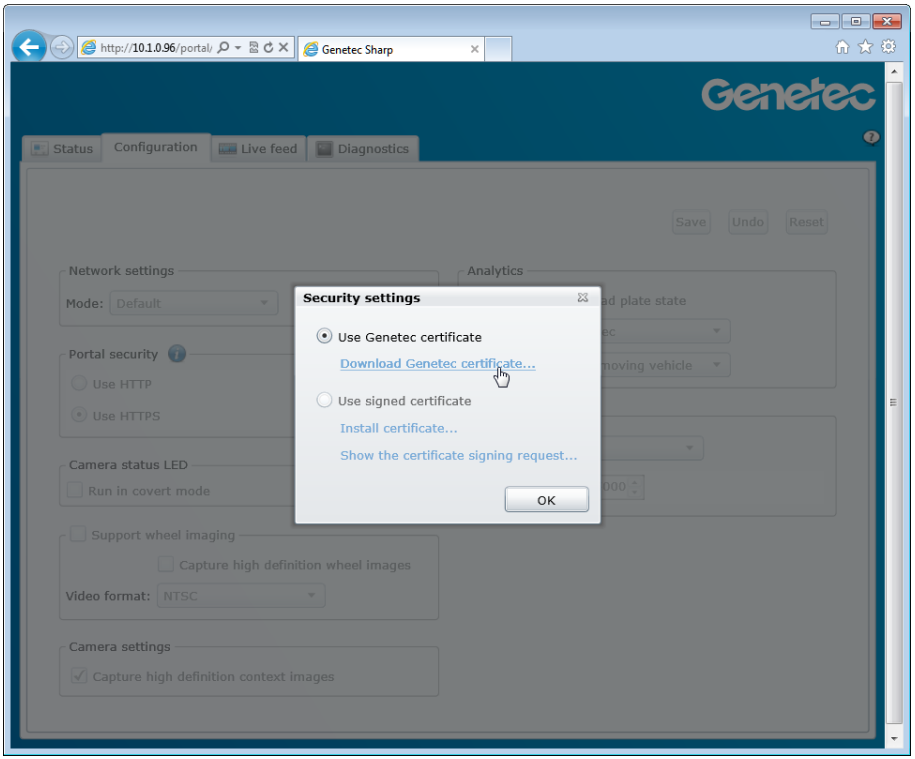
This section explains how to install the Genetec SSL certificate on the client machine. You use this procedure when you want to remove the warning page that appears when you log on to the Sharp Portal using an encrypted HTTPS connection.

1 Log on to the Sharp Portal.

2 Go to the **Configuration** page.

3 Under **Portal security**, select **Use HTTPS**, then click **Show settings**.

The **Security settings** window appears.



4 Click **Download Genetec certificate**, then click **Save** to save the certificate to your computer.

After you are done: Install the Genetec certificate on your machine using the Microsoft Management Console. For more information on using the Microsoft Management Console, see your Microsoft Windows Help.

Configure encryption with a signed certificate

This section explains how to configure Sharp Portal encryption using an SSL certificate signed by a certificate authority such as VeriSign.

Before you begin: If you already have a signed certificate installed, you need to delete it and then Restart the Sharp unit before installing a new certificate.

1 Log on to the Sharp Portal.

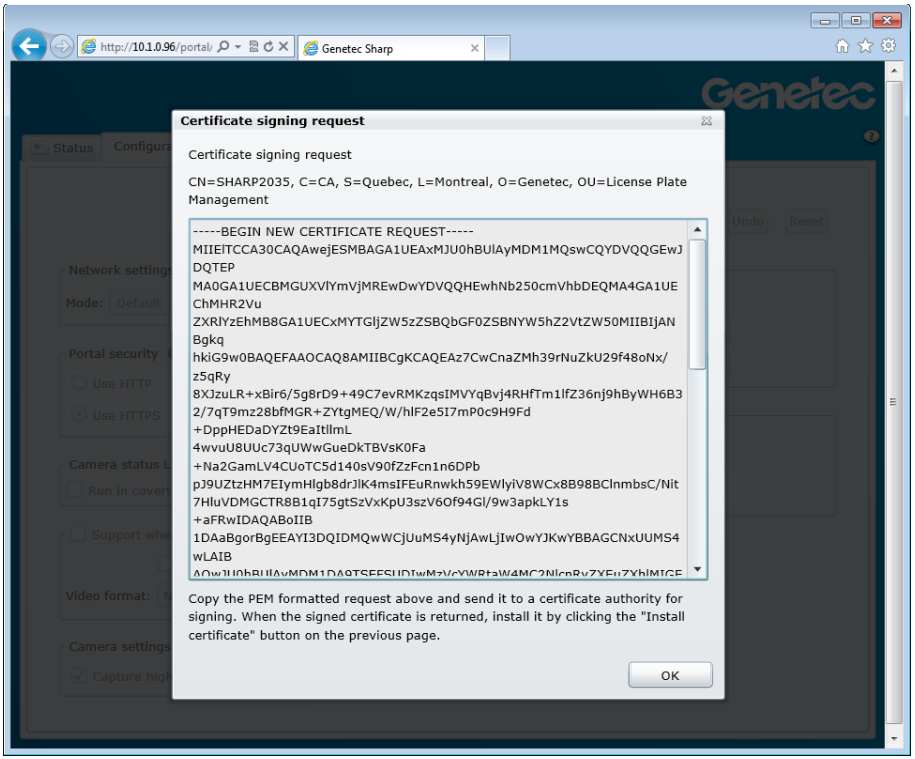
2 Go to the **Configuration** page.

3 Under **Portal security**, select **Use HTTPS**, then click **Show settings**.

The **Security settings** window appears.

4 Click **Show the certificate signing request**, then click **OK**.

The **Certificate signing request** window appears.



5 Copy the text string in the **Certificate signing request** (including the "----BEGIN NEW CERTIFICATE----") to your clipboard.

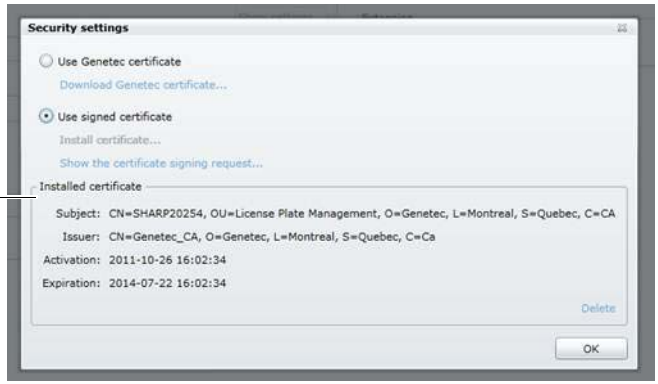
6 Send the Certificate signing request to a Certificate Authority (e.g. VeriSign).

You'll receive an SSL certificate signed by the Certificate Authority.

NOTE If your Certificate Authority is not recognized by Windows, when you log on to the Sharp Portal, you will receive a warning saying there is a problem with the website's security certificate. You can disregard the warning (rest assured the connection is encrypted), or install the certificate on the client machine.

7 After you have received the signed certificate, return to the **Security settings** window, click **Install certificate**, then select your signed certificate.

If the certificate is successfully installed, it will appear in the **Security settings** window.



8 Click **OK**.

9 Click **Save**, and **OK** to restart the Plate Reader service.

10 Restart the Sharp unit.

11 Log on to the Sharp Portal using HTTPS in the address bar instead of HTTP.

Your connection to the Sharp Portal is now encrypted.

After you are done: From the Sharp Portal's **Status** page, click **Change password**, and change the default password from "Genetec" to something else.

Switching images on the Sharp

Some Sharp cameras are shipped with multiple images embedded on the hard drive, each image compatible with a different version of Security Center. These disk images allow you to quickly switch versions on the Sharp in order to be compatible with the latest version of Patroller and Security Center. This section explains how to switch the image on a Sharp.

1 Start a **Remote Desktop Connection**, and enter the name or IP address of the Sharp you want to connect to.

NOTE Please note the following:

- If the Sharp is connected to a network with DNS capability, you can connect using the Sharp name (e.g. Sharp1234). The name is printed on the Sharp unit's label.
- If DNS is not available, you'll need to connect using the default IP address of the Sharp (192.168.10.100).

2 Click **Connect**.

3 Enter the following logon information (username and password are case sensitive):

a **Username:** enter **gopher**

b **Password:** enter **AutoVu_g0pher**

4 In the notification area on the Windows taskbar, close the **Watchdog** and **PlateReaderServer** applications.

a Right-click the **Watchdog** icon, then click **Exit**.

b Right-click the **PlateReaderServer** icon, then click **Exit**.

5 Go to the root *D:*\AutoVu folder.

You'll see one or more folders with names based on different versions of Security Center. For example, you should see a folder called *Plate Reader_5.1 SR1*. This folder contains the files the Sharp needs to be compatible with the release Security Center 5.1 SR1.

6 Choose the folder that corresponds to the Security Center version you want, and then delete the underscore suffix. For example, if you want to use the Sharp with 5.1 SR1, rename the folder *Plate Reader_5.1 SR1* to just *Plate Reader.*

This will tell the Sharp to use the 5.1 SR1 files and services contained in the folder.

7 Do the same for the other folders with the same underscore suffix.

8 When you are finished renaming the folders, power cycle the Sharp to restart it (disconnect the Sharp cable for a few seconds and then reconnect it).

When the Sharp restarts, it will be compatible with the version of Security Center you chose by deleting the underscore suffix from the folders on the Sharp.

Moving Patroller or LPR units between LPR Managers

You can use the *Move unit* tool in Security Center Config Tool to move LPR or Patroller units from one LPR Manager to another. After the unit is moved, the new LPR Manager takes on the command and control functions of the unit, while the old manager continues to manage the unit data collected before the move.

After you move a unit in Config Tool, you need to update the unit's network settings in Patroller Config Tool and in the Sharp Portal so that the unit can communicate with its new LPR Manager. Specific unit settings (e.g. unit name, logical ID, etc) are automatically carried over to the new LPR Manager.

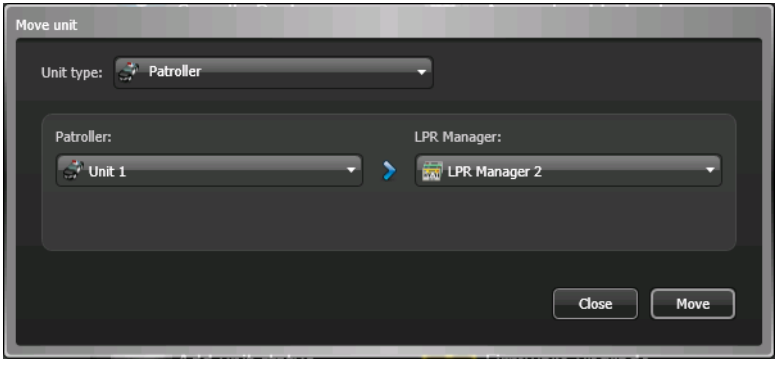
EXAMPLE If you move a Patroller unit from *LPR Manager* to *LPR Manager 2*, you need to configure the Patroller unit to communicate with *LPR Manager 2* the same way you did when you originally added the unit to *LPR Manager*. This requires changing network settings in Patroller Config Tool so that they match the network settings for *LPR Manager 2* in Security Center Config Tool.

To move an LPR or Patroller unit:

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, go to **Tools** > **Move unit**.

The Move unit dialog box opens.



3 From the **Unit type** list, select the Patroller or LPR unit you want to move.

4 From the **Patroller/LPR unit** list (the name of the list changes depending on the type of unit you're moving), select the unit you want to move.

5 From the **LPR Manager** list, select the new LPR Manager that will control the unit.

6 Click **Move**.

The unit is now added to the new LPR Manager

After you are done: Update the following settings:

- For Patroller units:
  - **a** Open Patroller Config Tool.
  - **b** Click the **Security Center** page, and update the **IP address**, **Port**, and **Update provider port** settings to match the settings for the new LPR Manager that is now controlling the unit.

    For more information, see "Security Center" on page 359.
- For LPR units:
  - **c** Log on to the Sharp Portal.
  - **d** Go to the **Configuration** page, and then under **Extension**, update the **Address**, **Port**, **Discovery port**, and **Update provider port** settings to match the settings for the new LPR Manager that is now controlling the unit.

    For more information, see "Extension" on page 379.
- For hotlists, permit lists, and Patroller user groups (if applicable):
  - **e** Log on to Security Center Config Tool.
  - **f** From the Security Center Config Tool Home page, go to **System** > **Roles**, click on the LPR Manager that is now controlling the unit you moved, and then go to **Properties** >**File association**.
  - **g** Activate the hotlists and permit lists, and assign a Patroller user group for this LPR Manager.

The unit can now communicate with its new LPR Manager.

Limiting user access to hotlists and permit lists

You can use Security Center privileges to configure which users have access to the *Hotlist and permit editor* task, and to manage how those users edit hotlists and permit lists.

IMPORTANT This feature will not prevent users from modifying a hotlist's or permit list's original source file (*.txt* or *.csv*) if they have access to it.

Before you begin

- Turn on **Enable editor support** in the hotlist or permit list entity's **Properties** page.
- Make sure you have the required privileges to configure other users' privileges.

What you should know

If your Security Center system uses partitions, you can limit user access to hotlists and permit lists even further by adding or removing the hotlist or permit entities from your different partitions. By doing this, the accepted users of a partition only have access to the hotlists or permit lists that are members of that partition.

Before you configure hotlist and permit list access rights, you should familiarize yourself with your Security Center system's layout. For example, you should know if your system has multiple partitions, nested partitions, users in multiple user groups, user groups in multiple partitions, and so on.

For more information on how users, user groups, and partitions work, see the section "Managing software security" in the *Security Center Administrator Guide* found on the GTAP Documents page.

Allowing or denying user access to the Hotlist and permit editor task

You can allow or deny users access to the *Hotlist and permit editor task* in Security Center Config Tool and Security Desk.

1 Log on to Security Center Config Tool.
2 From the Security Center Config Tool Home page, go to **Security** > **Users** or **User groups**.
3 Select the user or user group you want to configure.
4 From the **Set of privileges** drop-down list, select **Basic privileges**.
5 Go to **All privileges** > **Task privileges** > **Operation**, and then **Allow** or **Deny** access to the *Hotlist and permit editor*.
6 Click **Apply**.

Configuring hotlist and permit list editing privileges

You can use Security Center privileges to determine what information users are allowed to edit in hotlists and permit lists.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, go to **Security** > **Users** or **User groups**.

3 Select the user or user group you want to configure.

4 From the **Set of privileges** drop-down list, select **Basic privileges**, or select the partition you want to configure.

You can apply specific editing privileges to users and user groups on different partitions. Partition privileges take precedence over basic privileges.

5 Go to **All privileges** > **Administrative privileges** > **LPR management** > **Hotlists and permit lists**, and then select the privileges you want to allow.

The following combinations are possible:

- View, add, delete, and modify.
- View, add, and delete.
- View, add, and modify.
- View, delete, and modify.
- View and delete.
- View and modify.
- View and add.
- View only.
- Add only.

If you deny all the above privileges, users may still see the hotlist and permit entity names if the entities are members of the user's partition. However, they will not be able to load the lists into the *Hotlist and permit editor*.

6 Click **Apply**.

Adding or removing hotlists and permit lists from partitions

You can configure which hotlists and permit lists are available to users for editing by adding or removing the lists from your different partitions.

What you should know

When a hotlist or permit entity is a member of a partition, it means that the entity is visible to the accepted users of the partition in the *Hotlist and permit editor* task. However, even if the entity is visible, it is the user's privileges that determine if the hotlist or permit list can be edited, and in what way it can be edited.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, go to **Security** > **Partitions**.

3 Select the partition you want to configure.

4 Go to the **Properties** tab.

5 From the **Members** list, add or remove the hotlist or permit list entities as needed.

Changes you make on the **Properties** tab are automatically applied to the partition. You will not be prompted to apply your changes.

Configuring Security Desk to automatically display high-resolution context images

You can configure Security Desk to automatically load the high resolution vehicle context images for plate reads and hits displayed in Monitoring task tiles.

This can increase the efficiency of Security Desk operators that would normally have to manually display the high-res images, but it requires higher than normal bandwidth, and results in increased CPU usage on the computer hosting the LPR Manager role.

When this feature is enabled, the button to manually display high-res images in Security Desk is disabled. Operators will always see the high-res version of the images.

Before you begin: Close Security Desk if it is running.

To configure Security Desk to automatically display high-res context images:

1. On the Security Desk client computer, go to *C:\Program Files (x86)\Genetec Security Center 5.2\ConfigurationFiles*.

   This is the default folder location.
2. Open the file *App.SecurityDesk.config* in Notepad or a similar text editor.
3. In the <*Presentation*> tag, find the parameter *AutoLoadHighResImages*, and then change the value to "True".
4. Save and close Notepad.
5. Start Security Desk.

All vehicle context images are displayed in high-resolution, and the button to toggle between high and low resolution images is no longer visible.

After you are done: Do the same thing on any Security Desk client machine that requires automatically displayed high-resolution context images in Monitoring task tiles.

Customizing the information displayed in Security Desk Monitoring task tiles

You can choose what kind of LPR information you want to display in Monitoring task tiles for reads and hits. This ensures that Security Desk operators see only the information that is required for your LPR deployment scenario.

This feature works by adding different xml attributes and parameters to a specific Security Desk configuration file located on the Security Desk client machine. Each xml attribute corresponds to different LPR information.

Before you begin: Close Security Desk if it is running.

To customize the information displayed in Security Desk Monitoring task tiles:

1. On the Security Desk client computer, go to *C:\Program Files (x86)\Genetec Security Center 5.2\ConfigurationFiles*.

   This is the default folder location.
2. Open the file *App.SecurityDesk.config* in Notepad or a similar text editor
3. Find the following tag in the config file:

   ```
   <Presentation IgnoreSizeConstraints="False" DisplayResourcesIds="False"
   SearchFormState="" AutoLoadHighResImages="False"/>
   ```

   You can add additional xml attributes anywhere between the opening bracket and the closing slash and bracket.
4. To customize the display of read-related information in a tile, add the `"ReadDescription="` attribute, followed by any of the following parameters. Add the character `&#13;` if you want to force a carriage return in the Security Desk tile.
   - `{Read.Address}`. The address of the plate read.
   - `{Read.Confidence Score}`. The Confidence Score analytic information of the plate read (see "If there is a warning associated with a camera, there will be a yellow warning icon next to the interface number. Hover your mouse over the warning icon to see the details." on page 377). If the Sharp camera is not configured to send this analytic information, the xml tag will be displayed in the Security Desk tile.
   - `{Read.Vehicle Type}`. The Vehicle Type analytic information of the plate read (see "If there is a warning associated with a camera, there will be a yellow warning icon next to the interface number. Hover your mouse over the warning icon to see the details." on page 377). If the Sharp camera is not configured to send this analytic information, the xml tag will be displayed in the Security Desk tile.
   - `{Read.Relative Motion}`. The Relative Motion analytic information of the plate read (see "If there is a warning associated with a camera, there will be a yellow warning icon next to the interface number. Hover your mouse over the warning icon to see the details." on page 377). If the Sharp camera is not configured to send this analytic information, the xml tag will be displayed in the Security Desk tile.

- {Read.Plate}. The license plate characters as read by the LPR matcher.
- {Read.PlateState}. The license plate's issuing state, province, or country.
- {Read.Timestamp}. The date and time of the plate read.
- {Read.User}. The name of the Patroller unit that read the plate.

EXAMPLE Here is an example of what the config file looks like with **all** the read attributes included:

```
<Presentation IgnoreSizeConstraints="False" DisplayResourcesIds="False"
SearchFormState="" AutoLoadHighResImages="False"
ReadDescription="{Read.Plate}, {Read.Confidence Score}%, {Read.PlateState},
{Read.Timestamp}&#13;{Read.Address}, User:{Read.User}"/>
```

5 To customize the display of hit-related information in a tile, add the "HitDescription=" attribute, followed by any of the following parameters. Add the character
 if you want to force a carriage return in the Security Desk tile.

- {Hit.Category}. The "category" attribute of the hotlist or permit list.
- {Hit.Id}. The GUID of the hit.
- {Hit.MatchPlate}. The plate number that was matched by the LPR matcher.
- {Hit.Rule}. The name of the hotlist or permit list entity in Security Center.
- {Hit.Timestamp}. The date and time of the hit.
- {Hit.Type}. The type if hit (hotlist, permit, overtime, MLPI).
- {Hit.User}. The name of the Patroller unit that raised the hit.
- {Hit.Watermark}. The watermark of the hit.

EXAMPLE Here is an example of what the config file looks like with **all** the read and hit attributes included:

```
<Presentation IgnoreSizeConstraints="False" DisplayResourcesIds="False"
SearchFormState="" AutoLoadHighResImages="true"
ReadDescription="{Read.Plate}, ={Read.Confidence Score}%, {Read.PlateState},
{Read.Timestamp}&#13;{Read.Address}, User: {Read.User}"
HitDescription="{Read.Plate}, {Read.ConfidenceScore}%, {Read.PlateState},
{Read.Timestamp}, {Read.Address}&#13;{Hit.Type}, {Hit.Rule} / {Hit.MatchPlate},
{Hit.Timestamp}&#13;Category: {Hit.Category}, User: {Hit.User}&#13;{Hit.Id}"/>
```

NOTE You can add read information to a hit description because all hits are linked to at least one read. For example, you may want both the read and hit timestamps in the hit description because there may be a delay in the hit being processed.

6 Save and close Notepad.

7 Start Security Desk.

The Monitoring task tiles will now display the LPR information you added to the config file.

After you are done: Do the same thing on any Security Desk client machine that requires specific LPR information in Monitoring task tiles.

Enabling Cyrillic character support

For fixed or mobile AutoVu Law Enforcement installations, the LPR matcher supports Cyrillic character matching. This means that Security Center and Patroller can filter and match against hotlists with Mongolian plates. You can also enable a Patroller virtual keyboard with Cyrillic characters so you manually capture Mongolian plates.

For matching to work in fixed Sharp installations, the **Matching** module must be ON (see "Matching" on page 290), and only hotlists with Mongolian plates must be assigned to the LPR Manager role (see "File association" on page 289).

NOTE Cyrillic language support is limited to plate matching, plate filtering, and the Patroller Cyrillic virtual keyboard. The Security Center and Patroller user interfaces are not currently available in Cyrillic.

Enabling Patroller's Cyrillic virtual keyboard

When the virtual keyboard is set to Cyrillic, any text box for any option in Patroller or Patroller Config Tool must be entered in Cyrillic. If the Patroller computer is not configured in Windows for a Cyrillic physical keyboard, you will need to use the virtual keyboard for all text entries.

1. On the Patroller in-vehicle computer, go to the folder *C:\Program Files (x86)\Genetec AutoVu X.Y\MobileClient\ConfigurationFiles*.

   This is the default folder location.
2. Open the file *App.Patroller.config* in Notepad or a similar text editor.
3. In the <*Presentation*> tag, add the attribute *KeyboardCultures="mn"* to the end of the list, so that the tag looks like the following:

   ```
   <Presentation DisableHardwareAcceleration="true"
   AdjustDimensionsToScreenSize="false" setting EnableVirtualKeyboard="false" to
   "true"="false" KeyboardCultures="mn" />
   ```

   NOTE You can enable the virtual keyboard now by setting the parameter `EnableVirtualKeyboard=` to `"true"`, or you can enable it later in Patroller Config Tool.
4. Save and close Notepad.
5. (If you did not enable the keyboard) Open Patroller Config Tool, go to **User interface** > **General**, and then turn on the setting **Enable virtual keyboard**.
6. Click **Apply**.

Enabling plate filtering for Cyrillic hotlists

Security Center can filter invalid plates for Cyrillic hotlists.

NOTE If you use Cyrillic hotlists, you must either configure the filter for Cyrillic, or turn **Plate filtering** off entirely. If you leave filtering on without setting the character set to Cyrillic, Security Center will filter out all Cyrillic plates or characters because it is looking for another character set.

1. Log on to Security Center Config Tool.
2. From the Security Center Config Tool Home page, go to **LPR** > **Roles and units.**
3. Click on the LPR Manager you want to configure, and click on **Plate filtering**.
4. If you don't want Security Center to filter plates, turn **Plate filtering** off.
5. If you want Security Center to filter plates, turn **Plate filtering** on, and then configure the following settings:
   - *Character set*. Select **Cyrillic** from the drop-down list.
   - *Invalid plate number*. Select how you want Security Center to filter invalid characters. If you select **Modify record**, Security Center will remove any non-alphanumeric characters from the plate number. If you select **Remove record**, the entry will be deleted from the list entirely.
   - *Logging*. Select **Log filtering in**, and then specify where you want the log file to be saved. The destination folder you choose must be accessible to the computer hosting the LPR Manager role.
6. Click **Apply**.

Security Center will now filter and match against Cyrillic characters, and the virtual keyboard opens with Cyrillic characters when you click on a text box in Patroller or Patroller Config Tool.

After you are done: For fixed Sharp installations, the **Matching** module must be ON (see "Matching" on page 290), and only hotlists with Mongolian plates must be assigned to the LPR Manager role (see "File association" on page 289).

13

Additional configuration for AutoVu fixed systems

This section includes the configuration tasks that apply to fixed AutoVu systems.

This section includes the following topics:

Configure Sharp units for a fixed AutoVu system

This is what you need to do to log on to the Sharp Portal and configure the Sharp. You'll learn how to view the live video feed, configure the IP address and read strategy, choose to send LPR data to Security Center or to an FTP server, and more.

1 Log on to the Sharp Portal.

2 Go to the **Live feed** page to verify that the Sharp unit is working.

For more information, see "Live feed" on page 382.

3 Go to the **Configuration** page, and then configure the following:

a Under **Network settings**, select **DHCP** or **Static** (default).

For more information, see "Network settings" on page 373.

b Under **Camera settings**, configure the settings for the type of Sharp you're using.

For more information, see "Camera settings" on page 376.

c Under **Analytics**, select the Sharp context (e.g. Quebec, Oregon, etc), and read strategy (fast moving or slow moving vehicles).

For more information, see "If there is a warning associated with a camera, there will be a yellow warning icon next to the interface number. Hover your mouse over the warning icon to see the details." on page 377.

d Under **Extension**, specify if you want the Sharp to send LPR data to Security Center, or to an FTP server.

For more information, see "Extension" on page 379.

e Configure the other settings as required for your specific installation (e.g. set Sharp Portal encryption, turn off the Sharp LED, etc).

For more information, see "Configuration" on page 373.

Connect Security Center to fixed Sharp units

You need to configure the LPR Manager listening port to connect to fixed Sharp units on the network. The default value is 8731.

Before you begin: You need to know the IP address of the computer that is hosting the LPR Manager role.

1. Log on to Security Center Config Tool.
2. From the Security Center Config Tool Home page, go to **System** > **Roles**, and then click the LPR Manager you want to configure.
3. Click the **Properties** tab, and then select **Live**.
4. In **Listening port**, enter the port number used to transfer LPR data between fixed Sharps and the LPR Manager.

   For more information, see "Live" on page 288.
5. Click **Apply**.

After you are done: If you haven't already done so, perform the procedure described in "Configure Sharp units for a fixed AutoVu system" on page 166.

Configure discovery port for fixed Sharp units

The LPR Manager uses the discovery port to find fixed Sharp units on the network. You'll also need to modify settings in the Sharp Portal.

1. Log on to Security Center Config Tool.
2. From the Security Center Config Tool Home page, go to **System** > **Roles**, and then click the LPR Manager you want to configure.
3. Select the **Properties** tab.
4. Under **Live**, specify the **Sharp discovery port** used to discover fixed Sharps.

   Each LPR Manager must use a unique discovery port. For more information, see "Live" on page 288.
5. Click **Apply**.

After you are done: The Sharp discovery port number must match the port number in the Sharp Portal. For more information, see "Extension" on page 379.

Configure which LPR images the Sharp sends to Security Center

Configure which images to send to Security Center when the Sharp reads a plate. For example, you may want to only send images when a plate generates a hit.

1. Log on to Security Center Config Tool.
2. From the Security Center Config Tool Home page, go to **System** > **Roles**, and then click the LPR Manager you want to configure.
3. Select the **Properties** tab.
4. Under **Live**, specify which images to send to Security Center (license plate image and/or context image).
5. Click **Apply**.

These images are displayed in Security Desk when monitoring LPR events from fixed Sharps.

Configure fixed Sharp time zone and location

The time zone setting guarantees that the license plate reads that are collected from the Sharp unit are associated with the correct timestamp. The geographical location setting allows you to plot the LPR events (reads and hits) associated to the Sharp unit on the map in Security Desk.

You can set the time zone and location of a fixed Sharp from the LPR unit **Location** tab. For more information, see "Location" on page 272.

Using AutoVu for access control

This section explains the key concepts and configuration tasks required to use AutoVu License Plate Recognition technology for access control. In this scenario, Sharp cameras are installed at a facility's entry points (for example, parking lots, university campuses, and so on), and match plates to one or more hotlists to automatically grant or deny access to vehicles that want to enter.

This section includes the following topics:

How LPR-based access control works

In an LPR-based access control scenario, you use Sharp cameras, hotlists, and Security Center event-to-actions to automate access to a parking lot or similar facility.

You begin by installing your Sharp cameras at a facility's entry points to capture the plates of vehicles attempting to enter. You then create the hotlists that contain the license plates of the vehicles which are allowed to enter, and assign them to the Sharp units as needed in Security Center Config Tool. Each Sharp is responsible for the vehicles on the hotlist(s) assigned to it.

After creating and assigning your hotlists to the Sharp cameras, you then create Security Center event-to-actions for the "License plate hit" and "No match" events generated by the Sharps and hotlists. These event-to-actions are what grant or deny access to the vehicles.

For example, if a plate matches one or more hotlists assigned to a Sharp, Security Center triggers an action that lifts a gate or opens a garage door, while a "No match" event (plate does not match any assigned hotlist) triggers an action that sounds an alert, or sends a message to security personnel so they can question the vehicle's driver.

You can also trigger event-to-actions on hotlists of stolen vehicles, scofflaws, or other vehicles of interest. These hotlists are typically assigned to the LPR Manager so that the event-to-action can be triggered by any of the Sharps capturing the plate.

Key concepts

This section explains the key concepts required to configure an LPR-based access control solution. These concepts are the building blocks that will allow you to build an access control system for your specific needs.

This section includes the following topics:

Assigning hotlists to Sharp cameras

Hotlists are lists of vehicle license plates that can be assigned either to an LPR Manager role, or to individual Sharp units. When you assign a hotlist to an LPR Manager, all the Sharp units controlled by the LPR Manager can match against the hotlist. When you assign a hotlist to an individual Sharp unit, only that specific Sharp unit can trigger hits.

In LPR-based access control, a Sharp camera acts as a gatekeeper for a specific facility entry point. Depending on your deployment, you may want to allow only specific vehicles access to certain sections (for example, VIP parking, staff parking, and so on).

This is why you need the option of assigning hotlists to specific Sharp cameras. For example, this allows you to assign a VIP hotlist to a Sharp camera that is installed at the entrance to the VIP parking garage. The Sharp will then allow only the vehicles on its associated VIP hotlist to enter that section of the garage. Any vehicle that is not on the Sharp's hotlist doesn't get in.

This feature is particularly useful for large and complex parking facilities, such as university campuses which have multiple parking lots, each with multiple entry points, and each allowing access to different groups of vehicles.

License Plate Hit and No Match events

There are two main types of Security Center events used in an LPR-based access control system, *License Plate Hit* and *No Match*.

NOTE You can also use *License Plate Read* events to trigger actions such as starting video recording for the Sharp's context camera. However, only the License Plate Hit and No Match events are described in this topic.

- **License Plate Hit events.** When you turn on *Matching* for an LPR Manager in Security Center Config Tool, Security Center tries to match the plates captured by Sharp cameras to plates on loaded hotlists.

  If a plate is matched to a hotlist, Security Center generates a "License plate hit" event. By creating an event-to-action that triggers on this event, Security Center can grant access to a facility by opening a gate, a garage door, and so on.
- **No Match events.** You can also turn on "No match" events for an LPR Manager in Security Center Config Tool. A "No match" event is generated when a plate is *not* matched to a hotlist. For example, you can use a "No match" event to account for guests, delivery vehicles, or other vehicles not typically registered ahead of time on a hotlist.

  Event-to-actions for "No match" events can either have a hotlist or a Sharp camera as the source of the event. If the hotlist is the source, it means the plate is not found on that particular hotlist. However, if the Sharp is the source, it means that the plate is not found on *any* of the hotlists assigned to the Sharp. This is a subtle but important difference you should keep in mind when configuring your system because you can have more than one hotlist assigned to a single Sharp.

"No match" events are not generated against hotlists assigned to the LPR Manager because they would apply to all the Sharps controlled by the role. For example, if you have a hotlist of stolen vehicles assigned to the LPR Manager, any plate read not on that list would generate a "No match" event. Since the majority of the plates read by the Sharp will not be stolen vehicles, "No match" events would be generated for nearly every plate read.

Configuring AutoVu for access control

This section explains how to configure an LPR-based access control solution, using a university campus as an example. It includes a configuration overview, and specific configuration tasks required for this type of deployment.

You can deploy an LPR-based access control solution in a variety of ways, but the university example used here includes all the building blocks described in "Key concepts" on page 171. Understanding how to configure this university example will allow you to customize a solution for your specific deployment.

NOTE Some tasks, such as hotlist configuration, are not discussed in this section since they are also used for other AutoVu deployments. The overview includes links to other sections of the documentation for these types of tasks.

This section includes the following topics:

Configuration overview

This section summarizes how to deploy an LPR-based access control solution for a hypothetical university campus with the following parking rules:

- **Faculty.** Can park in Lot A and Lot B.
- **Students.** Can park in Lot B.
- **Management.** Can park in Lot C.
- **Maintenance.** Can park in Lot B on weekdays from 6:00 PM to 10:00 PM.
- **Guests.** Can park in any lot with approval from security.
- **Scofflaws.** Cannot park anywhere on campus, and security must be alerted if seen.

To deploy this scenario:

1 Install Sharp cameras at each parking lot entry point. For more information, see "Hardware installation" on page 51.

2 Get a fixed AutoVu system up and running. For more information, see "Roadmap for fixed deployment" on page 44.

Before you can configure an LPR-based access control solution, you must get your fixed AutoVu system up and running. This includes installing Security Center, configuring Sharp camera options in the Sharp Portal, and so on.

3 Name the Sharp entities. For more information, see "LPR unit" on page 327.

Security Center automatically detects all Sharps connected to the network, but you should name each Sharp entity according to its function or location. In our example, use the names *Sharp Lot A*, *Sharp Lot B*, and *Sharp Lot C*.

NOTE Configuration is simpler when all Sharps are on the same LPR Manager. However, if the Sharps are on multiple LPR Managers, you'll have to assign your hotlists accordingly.

4 Turn on hotlist matching. For more information, see "Matching" on page 290.

In Security Center Config Tool, turn on **Matching** and **No match** events for the LPR Manager controlling your Sharps.

5 Configure hotlists. For more information, see "Configuring hotlists" on page 120.

Create and configure the hotlists you're going to use. Name each hotlist according to its contents. In our example, use the names *Faculty*, *Students*, *Management*, *Maintenance*, and *Scofflaws*.

NOTE In our example, *Guests* represent anyone that shows up unannounced. Therefore, they are they are not included on any hotlist.

6 Create a schedule. For more information, see "Create a schedule" on page 175.

Because you want *Maintenance* staff to only have access to your parking lot between 6:00 PM and 10:00 PM, you must create a schedule in Security Center that reflects that. You'll use this schedule later on when you create your event-to-actions.

7 Assign your hotlists to Sharps and the LPR Manager. For more information, see "LPR unit" on page 327, and "File association" on page 289.

Assign your hotlists as follows:

- *Faculty* to *Sharp Lot A* and to *Sharp Lot B*.
- *Students* to *Sharp Lot B*.
- *Management* to *Sharp Lot C*.
- *Scofflaws* and *Maintenance* to the LPR Manager.

NOTE The *Maintenance* hotlist must be assigned to the LPR Manager because it depends on a schedule. All hotlists that you combine with schedules must be assigned to the LPR Manager.

8 (Optional) If you have only one LPR Manager on your system, you must unassign the *Faculty*, *Students*, and *Management* hotlists from your LPR Manager. For more information, see "File association" on page 289.

When you have only one LPR Manager, new hotlists are assigned to that LPR Manager by default (new hotlists are left unassigned if you have multiple LPR Managers). When you assign a hotlist to a Sharp, Security Center does not automatically unassign it from the LPR Manager; you must do it manually. Otherwise you will get duplicate match events from the other Sharps.

EXAMPLE If you assign the *Students* hotlist to *Sharp Lot B*, but forget to unassign it from the LPR Manager, a plate read from that list by *Sharp Lot B* will also trigger matches on *Sharp Lot A* and *Sharp Lot C*.

9 Configure the event-to-actions for the *Sharp Lot A*, *Sharp Lot B*, and *Sharp Lot C* units. For more information, see "Create event-to-actions" on page 176.

10 Configure the event-to-actions for the *Scofflaws* and *Maintenance* hotlists. For more information, see "Create event-to-actions" on page 176.

This is where you'll need the schedule you created for the maintenance staff.

Deployment is complete. Access to the parking lot is automated for permitted vehicles, and actions are taken when unknown or scofflaw vehicles are detected.

Create a schedule

You create a schedule when you want to grant certain vehicles scheduled access to your parking lot (for example, maintenance staff vehicles on weekdays from 6:00 PM to 10:00 PM). You use the schedule as a conditional entity when configuring your Security Center event-to-actions.

NOTE This procedure is an excerpt from the *Security Center Administrator Guide* found on the GTAP Documents page.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, go to **System** > **Schedules.**

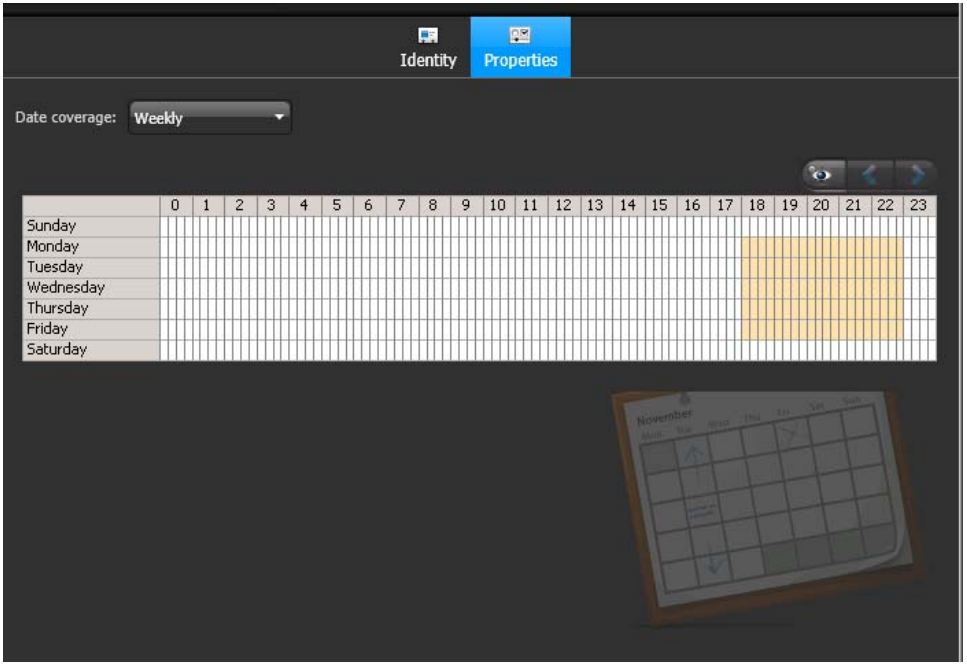
3 Click **Schedule**.

4 Give the schedule an appropriate name (for example, **Weekdays 6:00 PM to 10:00 PM**).

5 Click the **Properties** tab.

6 Select the **Date coverage** (for example, select **Weekly**).

A selector grid appears (the grid uses 24-hour notation).



7 Click and drag to select the block of time for weekdays between 6:00 PM to 10:00 PM (right-click if you want to clear the selection).

8 Click **Apply**.

Your schedule is created, and you can select it as a conditional entity when you configure an event-to-action.

Create event-to-actions

In an LPR-based access control scenario, Security Center event-to-actions trigger actions based on the "License plate hit" and "No match" events returned by Sharps or hotlists (for example, opening gates, activating security intercoms, sending emails, and so on). You must create event-to-actions to account for all the possible outcomes that can occur in your access control scenario.

NOTE This procedure is an excerpt from the topic "Automating system behavior" in the *Security Center Administrator Guide* found on the GTAP Documents page.

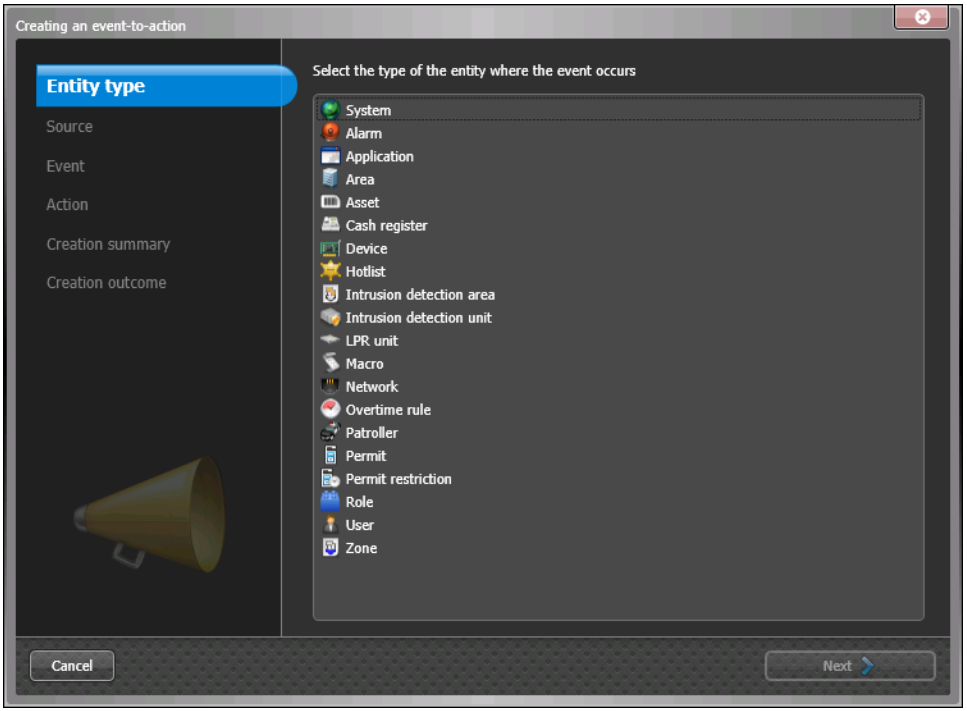
Before you begin: See "Create a schedule" on page 175.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, go to **System** > **General settings** > **Actions.**

3 Click **Add an item** ( ) to open the event-to-action creation wizard.

The wizard opens.



4 Create event-to-actions for the events generated by Sharp units installed at your parking lot's entry points. You need a "License plate hit" and "No match" event-to-action for each Sharp unit:

a From the **Entity type** tab, select **LPR unit**, and then click **Next**.

b From the **Source** tab, select which Sharp unit will be the source of the event, and then click **Next**.

c From the **Event** tab, select the following:

- From the main list, select **License plate hit** or **No match**.
- From the **Entity** drop-down list, select **Unassigned**.
- From the **Schedule** drop-down list, select **Always**.
- Click **Next.**

d From the **Action** tab, select the action and attributes for each type of event, and then click **Next**.

- For **License plate hit** events, select **Trigger output**, and then select the **Output pin** and **Output behavior** required to grant access to the parking lot (for example, open a gate).
- For **No match** events, select the action you want Security Center to take. For example, you could send a message to a particular Security Center user, or use another **Trigger output** action to activate a security intercom at the gate.

e From the **Creation summary** tab, review your event-to-action, and then click **Save** to proceed, or **Back** to make changes.

5 Create event-to-actions for the events generated by hotlists assigned to the LPR Manager (for example, lists of wanted vehicles, or vehicles with scheduled access):

a From the **Entity type** tab, select **Hotlist**, and then click **Next**.

b From the **Source** tab, select the *Scofflaw* or *Maintenance* hotlist.

c From the **Event** tab, select the following:

- From the main list, select **License plate hit**.
- From the **Entity** drop-down list, select **Unassigned** for the *Scofflaws* list, or **Sharp Lot B** (the Sharp responsible for Lot B entry point) for the *Maintenance* list.
- From the **Schedule** drop-down list, select **Always** for the *Scofflaws* list, or **Weekdays 6:00 PM to 10:00 PM** (the schedule you created in "Create a schedule" on page 175) for the *Maintenance* list.

IMPORTANT This may result in a limitation where a Maintenance vehicle is read correctly between 6:00 PM to 10:00 PM (the gate to Lot B will open), but an intervention message will still be generated because of No Match events to faculty and student vehicles.

- Click **Next**.

d From the **Action** tab, select the action and attributes for each type of event, and then click **Next**.

- For **License plate hit** events on the *Maintenance* list, select **Trigger output**, and then select the **Output pin** and **Output behavior** required to grant access to the parking lot (for example, open a gate).
- For **License plate hit** events on the *Scofflaws* list, select the action you want Security Center to take. For example, you could send a message or email to security personnel.

e From the **Creation summary** tab, review your event-to-action, and then click **Save** to proceed, or **Back** to make changes.

New event-to-actions are added to the list of system actions.

14

General AutoVu mobile configuration

This section includes the general configuration tasks that apply to all mobile AutoVu systems: Law Enforcement, City Parking Enforcement (with or without Wheel Imaging), University Parking Enforcement, and (MLPI) Mobile License Plate Inventory.

This section includes the following topics:

Configure Sharp units for a mobile AutoVu system

This is what you need to do to log on to the Sharp Portal and configure the Sharp. You'll learn how to view the live video feed, configure the IP address and read strategy, and more.

1 Log on to the Sharp Portal.

2 Go to the **Live feed** page to verify that the Sharp unit is working.

For more information, see "Live feed" on page 382.

3 Go to the **Configuration** page, and then configure the following:

a Under **Network settings**, select **DHCP** or **Static** (default).

For more information, see "Network settings" on page 373.

NOTE If you're using two LPR Processing Units in the same vehicle, see "Using a SharpX system with multiple LPR Processing Units" on page 195

b Under **Camera settings**, configure the settings for the type of Sharp you're using.

For more information, see "Camera settings" on page 376.

c Under **Analytics**, select the Sharp context (e.g. Quebec, Oregon, etc), and read strategy (fast moving or slow moving vehicles).

For more information, see "If there is a warning associated with a camera, there will be a yellow warning icon next to the interface number. Hover your mouse over the warning icon to see the details." on page 377.

d Under **Extension**, configure the Sharp to send LPR data to Patroller.

For more information, see "Extension" on page 379.

e Configure the other settings as required for your specific installation (e.g. set Sharp Portal encryption, turn off the Sharp LED, etc).

For more information, see "Configuration" on page 373.

Connect Patroller to Security Center

You need to configure Patroller and Security Center so the LPR Manager can discover and communicate with the Patroller units it controls.

1 In Security Center Config Tool, do the following:

   a Log on to Security Center Config Tool.

   b From the Security Center Config Tool Home page, go to **System** > **Roles**, and then click the LPR Manager you want to configure.

   c Select **Properties**, and then configure the settings under **Live**.

   For more information, see "Live" on page 288.

2 In Patroller Config Tool, do the following:

   a Open Patroller Config Tool.

   b Click **Security Center**, and then configure the settings.

   For more information, see "Operation" on page 349.

The LPR Manager will now discover the Patroller unit, and you'll be able to continue configuring Patroller.

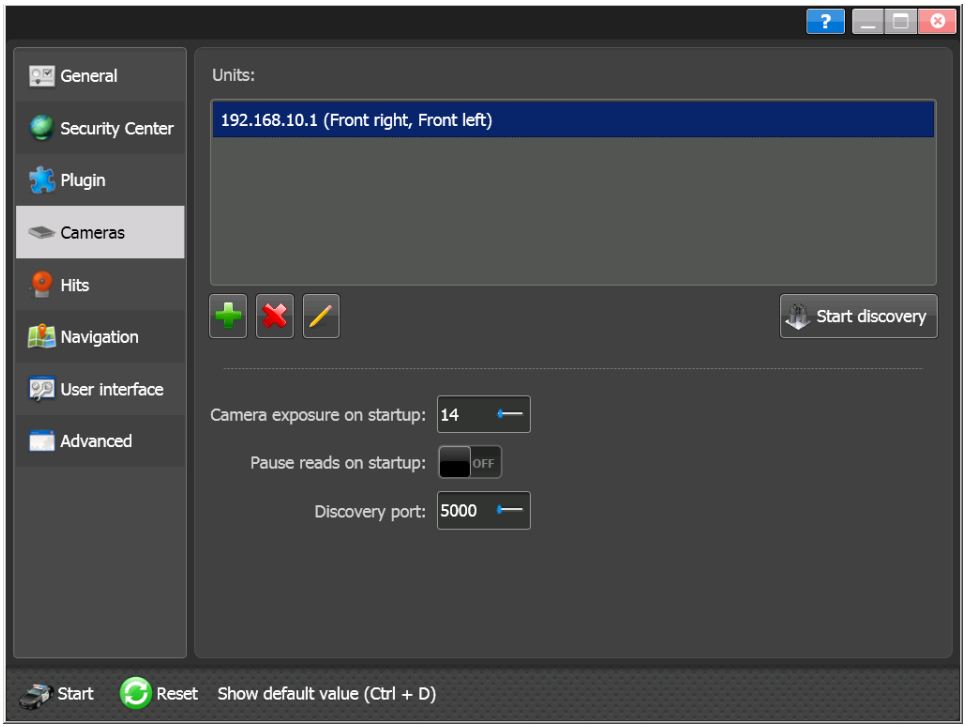
Connect Sharp units to Patroller

This section describes how to add Sharp camera units to the in-vehicle network so they can capture license plates and send the data to Patroller and Security Center (if applicable). You can have Patroller auto-detect all installed Sharps (the most common scenario), or you can add the Sharps manually. In either case, you need to specify the orientation for each Sharp, meaning where on the vehicle it is located (right, left, rear right, etc).

Before you begin: Configure Sharp units for a mobile AutoVu system.

1 Open Patroller Config Tool.

2 Go to the **Cameras** page.



3 To auto-detect all Sharps connected to the LPR Processing Unit, do the following:

a Make sure the **Discovery port** matches the discovery port you set for the Sharp in the Sharp Portal. For more information, see "Extension" on page 379.

NOTE The default discovery port for all Sharps is 5000, therefore you shouldn't need to change the port number.

b Click **Start discovery**.

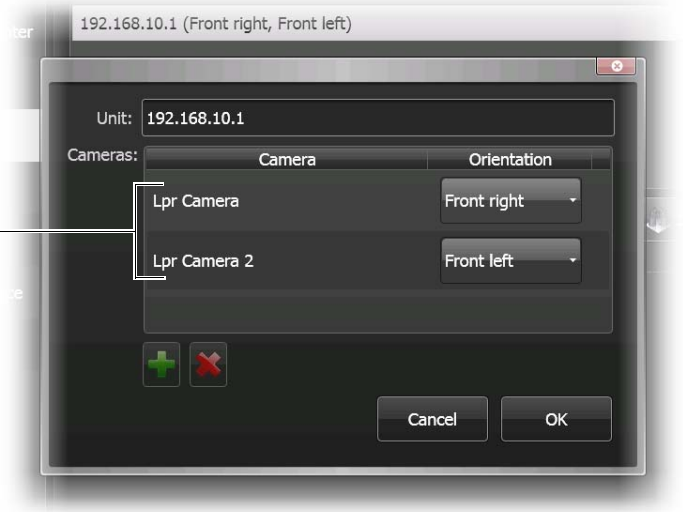
Patroller detects the connected Sharps and adds them to the **Units** list.

c Make sure each Sharp in the **Units** list has a different orientation. To do this, click on a Sharp, click the **Edit** button ( ), and then change the orientation of the Sharp to match where the Sharp is located on the vehicle.

When selecting the orientation, if there are two LPR cameras shown for one Sharp unit, it means that the Sharp is connected to an LPR Processing Unit with multi-threading capability, and a single "Unit" is actually controlling two Sharp cameras. In this case, make sure that both LPR cameras have a different orientation.

If you see two LPR cameras, it means you're on a *SharpX - Multi* system.

Spell the camera names exactly as shown. They must be **"Lpr Camera"** and **"Lpr Camera 2"** (case-sensitive).



4 (Optional) If you want to manually add a Sharp camera instead of using the automatic discovery feature, click the **Create** button ( ), and do the following:

a Under **Unit**, enter the Sharp's IP address (e.g. 192.168.10.1), or the Sharp name as it appears on the Sharp camera unit's label (e.g. Sharp1234).

If you're using a *SharpX - Multi* system, the "unit" corresponds to a single processor on the LPR Processing Unit, which controls two SharpX camera units. In this case, go to Step b to add your second camera. If you don't have a *SharpX - Multi*, go to Step c.

b (For *SharpX - Multi*) Under **Cameras**, click the **Create** button ( ) to add the second LPR camera.

IMPORTANT Please note the following:

- Enter camera names as "Lpr Camera" and "Lpr Camera 2" (case-sensitive).
- You can't add more than two LPR cameras. If you do, you will receive an error when you click **Apply**.

c Choose the camera's orientation from the drop-down list.

5 (Optional) Select the Sharp camera's initial exposure settings. In general, higher exposure is for darker environments, and lower exposure is for brighter environments.

NOTE The Sharp has auto-exposure capability that compensates for different plate reflectivity, as well as exterior ambient light. You shouldn't need to change the default value for this setting.

6 (Optional) Click **Start suspended mode** to start Patroller with plate reading turned off.

7 Click **Apply**.

The Sharp cameras are now connected to Patroller, and you should be able to see the live feed from the Patroller application.

Configure Patroller unit settings from Security Center

You can configure a Patroller unit's sound management, acknowledgement buffer, and hit delay settings from Security Center Config Tool. After you have configured the Patroller unit, you can use the *Copy configuration tool* to copy the settings to another Patroller unit. For more information on the Copy configuration tool, see *Security Center Administrator Guide*.

This section includes the following topics:

Configure sound management for Patroller units

Configure Patroller to play a sound when reading a plate and/or generating a hit, and choose whether sounds should be played even when Patroller is minimized.

1. Log on to Security Center Config Tool.
2. From the Security Center Config Tool Home page, go to **Logical view**, and then click the Patroller unit you want to configure.
3. Select the **Properties** tab, and then configure the settings under **Sound management**.

   For more information, see "Properties" on page 331.
4. Click **Apply**.

Configure acknowledgement buffer settings for Patroller units

Specify a buffer restriction that limits how many hits remain unacknowledged (not accepted or rejected) before Patroller automatically rejects all subsequent hits. You can also choose (by priority) which hotlists should comply with this restriction.

1. Log on to Security Center Config Tool.
2. From the Security Center Config Tool Home page, go to **Logical view**, and then click the Patroller unit you want to configure.
3. Select the **Properties** tab, and then configure the settings under **Acknowledgement buffer**.

   For more information, see "Properties" on page 331.
4. Click **Apply**.

Configure hit delay for Patroller units

Specify a hit delay that tells Patroller to disregard multiple hits on the same plate for the duration of the delay. For example, if you set a delay of 10 minutes, no matter how many times Patroller reads the same plate during those 10 minutes, it will generate only one hit.

1. Log on to Security Center Config Tool.
2. From the Security Center Config Tool Home page, go to **Logical view**, and then click the Patroller unit you want to configure.
3. Select the **Properties** tab, and then configure the settings under **Hotlist**.

   For more information, see "Properties" on page 331.
4. Click **Apply**.

   NOTE If you are using Patroller 6.0 or later, this setting is applicable for permits as well.

Configure offload options

You need to configure how Patroller offloads LPR data to Security Center. You can offload data to a file on the local Patroller computer (LocalFile), or directly to Security Center or a network drive (WcfTransfer).

Before you begin: If you're going to offload data directly to Security Center, see "Connect Patroller to Security Center" on page 181.

1 Open Patroller Config Tool.

2 Go to **Security Center** > **Offload**.

3 From the **Offload method** drop-down list, choose **LocalFile** or **WcfTransfer**, then configure the required settings.

For more information, see "Offload" on page 361.

Configure the Patroller unit name and logon options

Assign a name to the Patroller unit, and configure Patroller to ask for a username and password when a user logs on.

NOTE The Patroller unit name is **not** the Patroller user's username. The username is set in Security Center Config Tool when you create a user. The Patroller unit name is the name of the vehicle entity as it appears in Security Center.

1 Open Patroller Config Tool.

2 Go to the **General** page, then configure the required settings.

For more information, see "General" on page 345.

3 Click **Apply**.

Configure Patroller hit options

You configure most of the options related to hotlist hits from Security Center Config Tool, but certain options are specific to each Patroller unit. Here are some of the hotlist hit options you can configure in Patroller Config Tool:

- **Allow consecutive hits.** Turn on to allow multiple hits with the same information (plate number and state) to appear in a row.
- **First hit on top.** Choose the order that hits are displayed.
- **Enable new wanted.** Turn on to allow Patroller users to add *New wanted* hotlist entries.
- **Bypass hit enforcement.** Specify whether to accept and then enforce the hit, or just accept.
- **Auto-enforce hotlist hits.** Enable Patroller to run in "unattended mode" where it does not require any user interaction.
- **Display hits by priority.** Display hits by the priority specified in Security Center Config Tool when the hotlist is created.

To configure hotlist hit options:

1 Open Patroller Config Tool.

2 Go to the **Hits** page, then configure the settings.

For more information, see "Operation" on page 349.

3 Click **Apply**.

Configure the Patroller navigation and map settings

If you're using Patroller with GPS or maps, you need to configure the related settings in Patroller Config Tool.

This section includes the following topics:

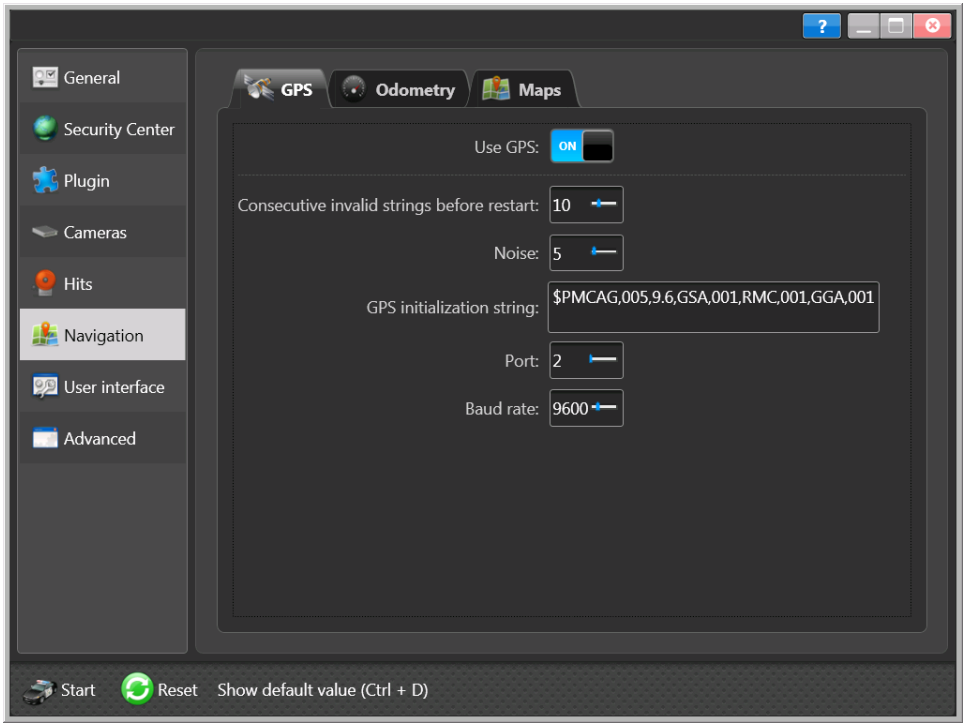
Configure GPS settings

These settings apply to both types of Genetec GPS devices, the USB GPS that connects directly to the in-vehicle computer, and the GPS antenna that connects to the Navigator box.

1 Open Patroller Config Tool.

2 Go to **Navigation** > **GPS**.

The **GPS** page appears.



3 Turn on **Use GPS**, then configure the following:

- *Consecutive invalid strings before restart.* Specify the number of consecutive invalid GPS strings (i.e. can't detect GPS signal) allowed before the device is restarted. The default number is 10.

  IMPORTANT You should not need to change this setting.

- *Noise.* Specify the noise value. If the distance from 0,0 to the GPS position is less than the value you define, no GPS event is generated. The default noise value is 5.

  IMPORTANT You should not need to change this setting.

- *GPS initialization string.* Do not modify. This is a default firmware setting.
- *Port.* Specify the COM port number of the GPS device as seen in Windows Device Manager. If you're using the USB GPS, the name of the device is *Prolific USB-to-Serial Comm Port*. If you're using the GPS antenna that connects to the Navigator box, the name of the device is *u-blox 5 GPS and GALILEO Receiver*.
- *Baud rate.* The speed of the GPS communications channel (serial port). The default value is 9600, but some USB GPS devices require a reduced speed of 4800. For example, if you're using the USB GPS receiver provided by Genetec (model number BU-353), you need to change this value to 4800.

4 Click **Apply**.

Patroller GPS settings are configured.

After you are done: You'll need to install the GPS driver on the Patroller computer. For more information, see "Install the GPS driver" on page 197.

Configure Map settings

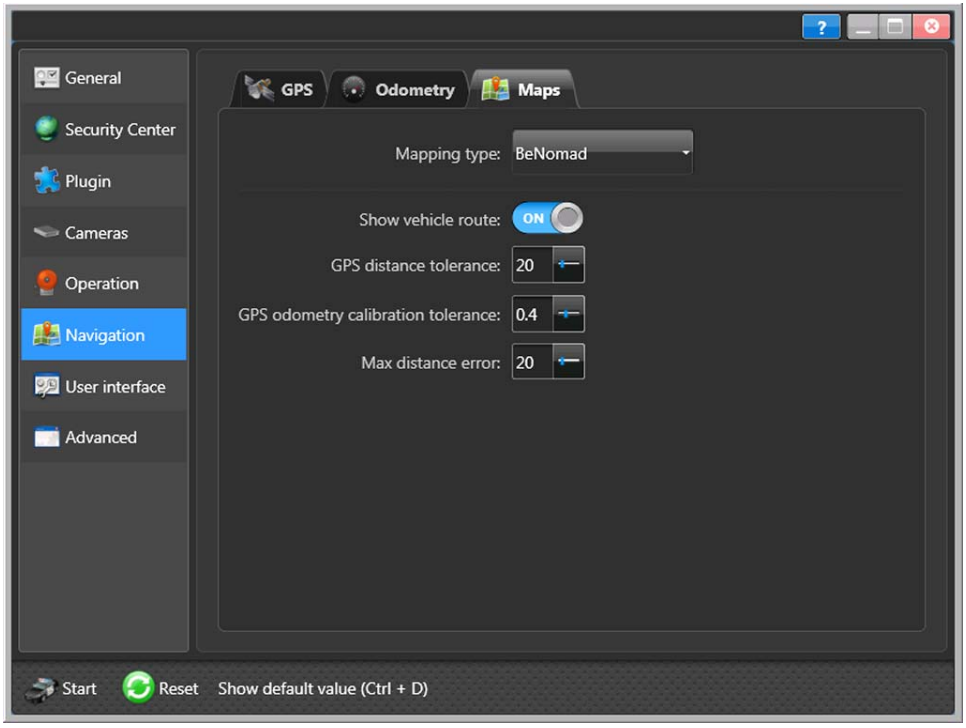
Select the Patroller mapping option to use, and configure the related settings.

Before you begin: If you're using maps, you need to install the *BeNomad* files, Patroller's mapping solution. For more information, see "Install BeNomad files on the in-vehicle computer" on page 97.

1 Open Patroller Config Tool.

2 Go to **Navigation** > **Maps**.

The **Maps** page appears.



3 From **Mapping type**, select **BeNomad**.

The default map type for AutoVu.

4 Configure the following settings:

- *Show vehicle route.* Displays a trail behind the Patroller icon that allows you to see the route Patroller has taken. Turn this setting off to show only the Patroller's current position.
- *GPS distance tolerance.* Specify the distance (in meters) where a GPS match is almost 100% certain. For example, a value of 50 means that a location result from the GPS matcher is almost 100% accurate within 50 meters. The smaller the value, the more aggressive are the GPS matching location corrections. The default distance is 20 meters.
- *GPS odometry calibration tolerance.* Specify the error in which the odometry calibration factor is correct with near 100% certainty. For example, a value of 0.4 means that it's almost certain that a calibration result from the GPS matcher is accurate within 40%. The smaller the value, the more aggressive the GPS odometry calibration corrections. The default tolerance is 0.4.

- *Max distance error*. Specify the maximum distance error (in meters). If the distance between the vehicle and the closest map item is greater than this value, no snapping will occur.

5 Click **Apply**.

Patroller mapping settings are configured.

Customize the Patroller user interface

These are general settings that determine how Patroller looks and behaves. Use these settings to customize the Patroller application for your needs. Here are some of the options you can configure:

- **Circle plate.** Circle the license plates in the context images.
- **Show hotlist status indicator.** Shows the indicator in the Patroller notification bar.
- **Enable minimize button.** Allow Patroller users to minimize the application.
- **Silent mode.** The Patroller window is minimized at startup, and stays that way until you get a hit.

To configure User interface options:

1 Open Patroller Config Tool.

2 Go to the **User interface** page, then configure the settings.

For more information, see "User interface" on page 364.

3 Click **Apply**.

Using a SharpX system with multiple LPR Processing Units

If you are using two SharpX LPR Processing Units on the same network (e.g. in the same vehicle), follow the procedures described in this section to resolve the IP address conflicts between the units.

This section includes the following topics:

About the LPR Processing Unit's default IP addresses

All SharpX LPR Processing Units have seven internal components. Each component has a factory-assigned static IP address. These components are:

Component	Default IP address
Single Board Computer 1 (SBC1)	192.168.10.1
Single Board Computer 2 (SBC2)	192.168.10.2
Genetec Video Processor 1 (GVP1)	192.168.10.3
Genetec Video Processor 2 (GVP2)	192.168.10.4
Camera Unit 1 (CAMU1)	192.168.10.5
Camera Unit 2 (CAMU2)	192.168.10.6
Mobile Processing Unit (MPU)	192.168.10.7
Camera Unit 3 (CAMU3)[a]	192.168.10.8
Camera Unit 4 (CAMU4)[a]	192.168.10.9

a. For *SharpX – Multi* with four camera ports.

If you're using only one LPR Processing Unit on the network (e.g. in a vehicle), you don't have to change any of the default settings. If you're using two units on the same network (sometimes referred to as "daisy-chaining"), the duplicate IP addresses on the units will conflict. This means you'll need to change the default IP addresses on one of the units. You can do this using the Sharp Portal.

Change the LPR Processing Unit's default IP addresses

To change the default IP addresses on an LPR Processing Unit, you only need to change the IP address on one of the SBCs. By doing this, the remaining IP addresses will automatically adjust in sequence.

EXAMPLE

- **If you're connected to SBC1.** If you change the IP address to 192.168.10.11, the remaining components will increment by one (e.g. SBC2 will become 192.168.10.12, GVP1 will become 192.168.10.13, and so on).
- **If you're connected to SBC2 (SharpX – Multi only).** If you change the IP address to 192.168.10.12, SBC1 will become 192.168.10.11, and the remaining components will increment by one (e.g. GVP1 will become 192.168.10.13, GVP2 will become 192.168.10.14, and so on).

To change the IP address of SBC1:

1. Connect your laptop to one of the LAN ports (LAN1 or LAN2) on the LPR Processing Unit you want to configure.
2. Log on to the Sharp Portal using the IP address 192.168.10.1 for SBC1, or 192.168.10.2 for SBC2. For more information, see the example above.
3. Go to the **Configuration** page.
4. Under **Network settings**, click **Edit**, then select **Static** and change the IP address.

   For more information, see "Network settings" on page 373.
5. (Optional) Change the **Subnet mask** and **Gateway**, if applicable. For example, if the new IP address you choose for the Sharp has a different subnet, change the **Subnet mask**.

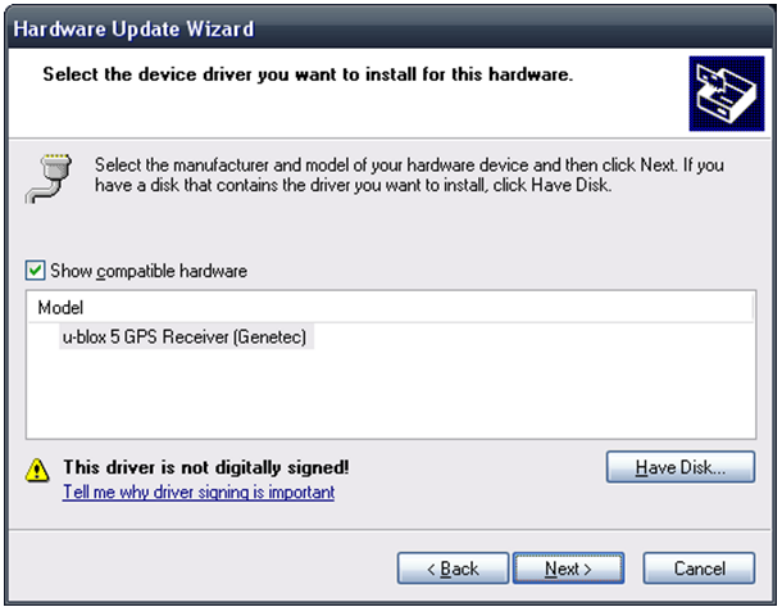
   For more information, see "Network settings" on page 373.
6. Restart the Sharp unit.

This resolves all IP address conflicts, and you can proceed with configuring your system.

Install the GPS driver

The Patroller in-vehicle computer receives information from the GPS system. If you're using the GPS receiver provided by Genetec, you need to install a new driver for the GPS system.

1 On the in-vehicle computer, open Windows Device Manager.
   a Right-click **My Computer**.
   b Select **Manage**.
   c Select **Device Manager**.
2 Expand the **Ports** menu.
3 Right-click the u-blox 5 GPS Receiver port and select **Update Driver**.
4 In the Hardware Update Wizard, select **Install from a list or specific location (Advanced)**.
5 In the following window, select the **Don't search. I will choose the driver to install** option and click **Next**.
6 Click **Have Disk** in the next window.
7 Retrieve the new driver on the installation CD, and click **OK**.



8 Click **Finish** to complete the installation of the new GPS driver.

After you are done: If you're using the USB GPS receiver provided by Genetec, you also need to change the baud rate of the device to 4800. For more information, see "GPS" on page 355.

Using a SharpX – Multi system

This section explains how the multi-threading capability of the *SharpX – Multi* system affects how you add and configure cameras.

This section includes the following topics:

About the SharpX – Multi

The SharpX system consists of a SharpX camera unit and an LPR Processing Unit (also referred to as a "trunk unit"). For more information, see "AutoVu SharpX components" on page 4.

The *SharpX – Multi* is a SharpX system with a trunk unit that has multi-threading capability. This means that one internal processor (also called an SBC for "single board computer") can control two SharpX camera units. There are two versions of the *SharpX – Multi:*

- **SharpX – Multi (2-port).** Trunk unit with two physical camera ports, and one multi-thread processor controlling both ports.
- **SharpX – Multi (4-port).** Trunk unit with four physical camera ports, and two multi-thread processors. One processor controls the first pair of ports, and the other processor controls the second pair of ports.

For more information, see the AutoVu SharpX specification sheet.

Connect and configure cameras for a SharpX – Multi 4-port system

You can connect any SharpX or SharpX VGA camera unit to any of the trunk unit's camera ports. However, the SharpX is an XGA camera, and it needs more processing power to capture plates at 30 fps than a SharpX VGA. At 30 fps, SharpX can capture plates on vehicles travelling at up to 300 km/h.

If you want the SharpX to capture at 30 fps, it can't share a processor with any another SharpX camera. If it does, its frame rate will drop to 15 fps, which means it will only be able to capture plates on vehicles travelling at a maximum of 150 km/h.

EXAMPLE If you have *one* SharpX and *two* SharpX VGAs, do the following:

1 Connect the SharpX cameras as shown:

By connecting the SharpX to **Interface 3**, and leaving **Interface 4** empty, you ensure that the SharpX has full use of the processor controlling interfaces 3 and 4.

Now you need to tell the trunk unit that there is no camera connected to **Interface 4**, and that it should allocate all processing power to **Interface 3**.

2 Log on to the Sharp Portal.

You need to log on to the processor that controls the SharpX camera connected to **Interface 3**. If you haven't changed the default IP addresses on the SharpX trunk unit, this means you should connect to 198.168.10.2. This IP address corresponds to the second processor.

For more information, see the following:

- "Using the Sharp Portal with SharpX" on page 37
- "Camera settings" on page 376

3 Go to the **Configuration** page > **Camera settings**.

4 For **Interface 4**, set the **Model** to **None**.

This tells the trunk unit that there is no camera physically connected to **Interface 4**, and the SharpX connected to **Interface 3** will use the processor's full power to run at 30 fps.

5 Click **Save**.

You now have a three-camera SharpX solution with two SharpX VGAs and one SharpX, all running at maximum capacity of 30 fps.

Associate user custom fields with reads and hits

You can add user custom fields to LPR annotation fields in order to associate a user's metadata with individual Patroller reads and hits. This allows you to query and filter for the user custom fields in Security Desk "Reads" and "Hits" reports.

NOTE This section describes how to create a user custom field for the specific purpose of associating it to Patroller reads and hits. For more information on the other types of custom fields available and how you use them, see the *Security Center Administrator Guide*, available on the GTAP Documents page.

EXAMPLE You have several Patroller users that alternate between different patrol teams, such as police officers moving between different city zones. By defining each patrol team as a user custom field, you can generate a report in Security Desk that displays the reads or hits collected when the officer was in patrol team A, patrol team B, and so on.

Before you begin: You must configure Patroller to require a username and/or password to log on. You cannot use this feature if Patroller is set to "No logon" because the reads and hits must be attached to a valid username. For more information, see "General" on page 345.

This section includes the following topics:

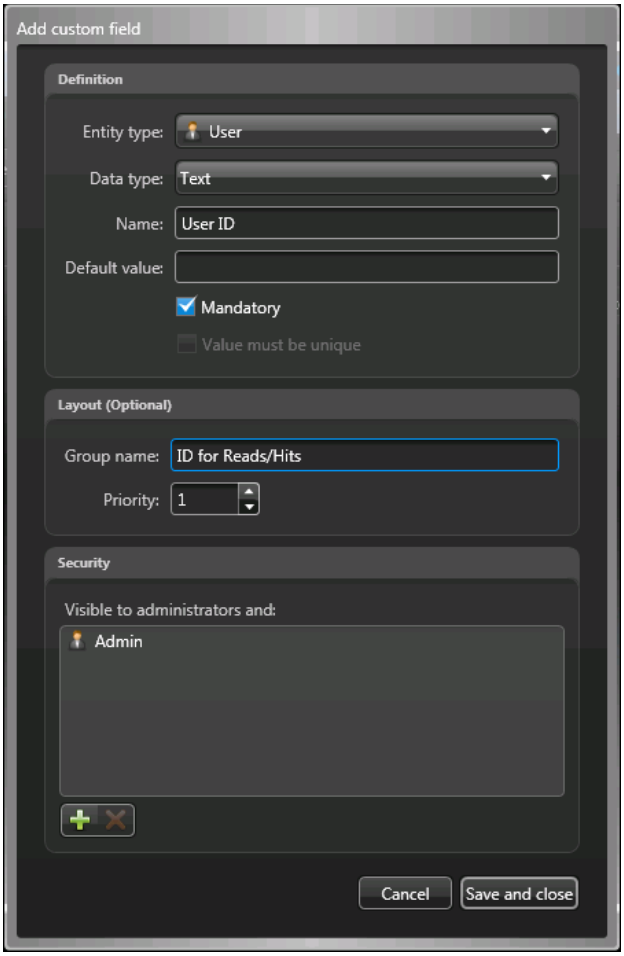
Create the user custom field

The first thing you must do to associate user custom fields to reads and hits is to create a user custom field.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, go to **System** > **General settings** > **Custom fields**.

3 Click ✚ at the bottom of the custom field list.
The **Add custom field** dialog box appears.



4 From the **Entity type** drop-down list, select **User**.
5 From the **Data type** drop-down list, select the data type for this field.
For example, select **Text**.
6 In the **Name** field, type the name for this custom field.
For example, type **User ID**.
7 (Optional) In **Default value** field, type or select the default value for this field.
8 Depending on the selected data type, the following additional options appear:
- *Mandatory.* Select it if this custom field cannot be empty.
- *Value must be unique.* Select it if the value of this custom field must be unique.

NOTE The *unique value* option can only be enforced after the field is created. To enforce this option, you must first make sure that all entities in your system have a distinct value for this custom field, then come back to this tab to apply the unique value option to it.

9 (Optional) Under the **Layout** section, type the **Group name,** and select the **Priority** from the drop-down list.

These two attributes are used when displaying the field in the **Custom fields** tab of associated entity. The group name is used as the group heading, and the priority dictates the display order of the field within the group.

10 (Optional) Under the **Security** section, click  to add users and user groups that will be able to see this custom field. By default, only administrative users can see a custom field.

11 Click **Save and close**.

The new user custom field **User ID** is available in your users' **Custom fields** tab.

After you are done: "Define the user custom field" on page 202.

Define the user custom field

After you have created a user custom field, you must define it. For example, give each of your Patroller users a unique **User ID**.

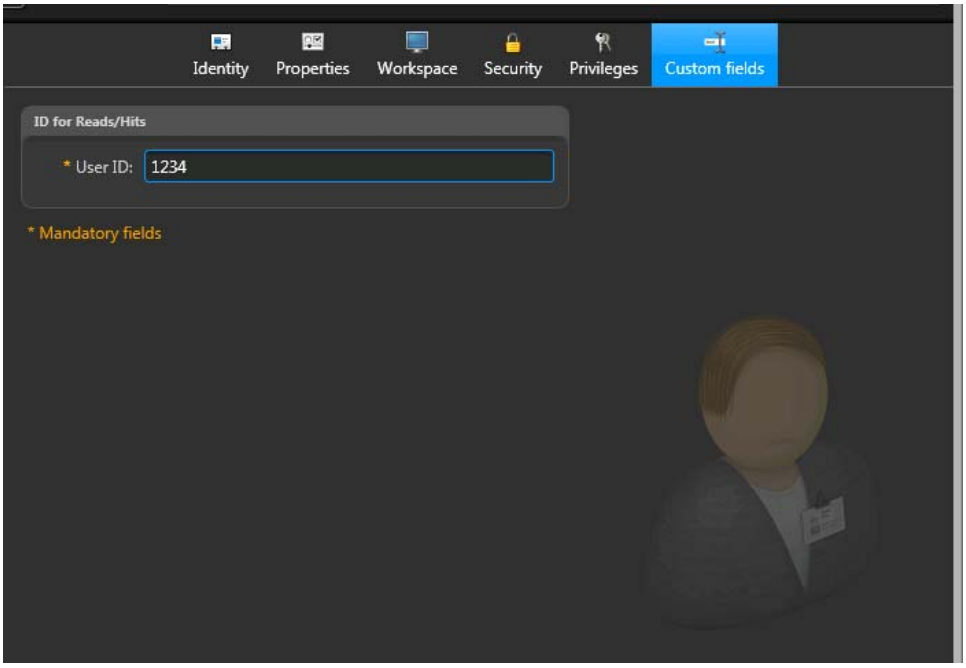
Before you begin: "Create the user custom field" on page 200.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, go to **Security** > **Users**, and then select the user you want to configure.

3 Select the **Custom fields** tab.

The user custom field **User ID** that you created in "Create the user custom field" on page 200 is displayed.



4 Type the **User ID** for the current Patroller user.

For example, type **1234**.

5 Click **Apply**.

This Patroller user now has a User ID of 1234. You can now add this custom field as an annotation field for reads and hits.

After you are done: "Add the custom field as an annotation field" on page 203.

Add the custom field as an annotation field

After you have created and defined your custom field, you must add it to the list of annotation fields for Patroller reads and hits.

Before you begin: "Define the user custom field" on page 202.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, go to **LPR** > **General settings** > **Annotation fields**.

3 Click **Add an item** ( ).

The **Add an annotation field** window appears.

4 Under **Type**, select **Read** or **Hit**.

5 Select **Custom field**, and then select the user custom field you created in "Create the user custom field" on page 200.

6 Click **Add**.

Your user custom field is added to the list of annotation fields for all Patroller reads or hits, depending on what you selected in Step 4. Security Center now associates reads or hits with the user custom field (the **User ID** in this case) that was logged on to Patroller at the time the event occurred. This value is stored in the database for each read or hit.

NOTE If you want the same user custom field for reads *and* hits, you must define it as an annotation field twice, once for reads and once for hits.

After you are done: The custom field is now available as two separate columns in Security Desk "Reads" and "Hits" reports. One is a *Custom field* column that displays the latest value configured for the User entity. The other column is an *Annotation field* column that displays the value for the User entity when the read or hit was stored by the LPR Manager role. For more information, see the *Security Desk User Guide*, available on the GTAP Documents page.

15

Additional configuration for AutoVu Law Enforcement systems

This section includes the additional configuration tasks that apply to AutoVu Law Enforcement systems.

NOTE Hotlist configuration is not described in this chapter. Although hotlists are an essential component of a Law Enforcement system, they can also be used in other types of AutoVu installations (e.g. City Parking Enforcement, University Parking Enforcement, etc). For that reason, information on how to configure hotlists is located in the General AutoVu configuration chapter (see "Configuring hotlists" on page 120).

This section includes the following topics:

Configure hit accept and hit reject reasons

You can create and configure customized reasons to appear in Patroller when the user rejects or accepts a hit. The settings are downloaded along with the selected hotlists/permit lists to Patrollers when the Patroller user logs on. Hit reject and accept reasons are applied at the Directory level, which means that all the LPR Managers in your system will share the same settings.

- **Hit reject reasons.** List of reasons for rejecting hotlist hits. These values also become available as Reject reason filter options for generating hit reports in Security Desk. Several categories are pre-configured for you when you install Security Center.
- **Hit accept reasons.** Create a form that contains a list of questions that Patroller users must answer when they accept a hit. The information from the hit form can be queried in the Security Desk Hit report.

The attributes you create are also available as filter options for hit reports in Security Desk.

To create Hit accept or reject reasons:

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, go to **LPR** > **General Settings**.

3 Under **Hotlist**, add, delete, or modify Hit accept or Hit reject reasons as needed.

For more information, see "Hotlist" on page 304.

4 Click **Apply**.

The Hit accept and reject reasons are downloaded to Patroller the next time it is connected to Security Center.

Configuring New wanted attributes and categories

The *New wanted* feature allows you to manually add a license plate to Patroller's local hotlist file on the in-vehicle computer. You use this feature when you're searching for a specific plate that isn't on the hotlists loaded in Patroller. For example, if you aren't wirelessly connected to headquarters, Patroller can't download a new vehicle's information. Instead, you enter the plate as a *New wanted* entry directly in Patroller.

- **New wanted attribute.** Attributes other than the standard ones (plate number, plate issuing state, category) that the Patroller user is asked to specify when entering a new wanted item in the Patroller.
- **New wanted categories.** List of categories that a Patroller user can pick from when entering a new wanted item. The category is the attribute that says why a license plate number is wanted in a hotlist.

New wanted categories and attributes are applied at the Directory level, which means that all the LPR Managers in your system will share the same settings.

This section includes the following topics:

Create in Security Center Config Tool

1. Log on to Security Center Config Tool.
2. From the Security Center Config Tool Home page, go to **LPR** > **General Settings**.
3. Under **Hotlist**, add, delete, or modify *New wanted* attributes and categories as needed.

   For more information, see "Hotlist" on page 304.
4. Click **Apply**.

The *New wanted* attributes and categories are downloaded to Patroller the next time it is connected to Security Center.

Configure in Patroller Config Tool

After you have created the *New wanted* attributes and categories, and they have been pushed to Patroller, you need to configure them in Patroller Config Tool.

1. Open Patroller Config Tool.
2. Go to **Hits** > **Hotlists**, turn on **Enable new wanted**, and then configure the following settings as needed:
   - *Enable new wanted management.* Turn on to allow Patroller users to edit and delete *New wanted* entries from the database.

- *Enable comments for new wanted.* Turn on to activate a text box where you can enter a comment when entering a *New wanted* hotlist item.
- *New wanted expiry options (in days).* Select one or more expiration options for New Wanted entries.

For more information, see "Hotlists" on page 350.

3 Click **Apply**.

Patroller users can now add and manage (if enabled) *New wanted* entries.

16

Additional configuration for AutoVu City and University Parking Enforcement systems

This section includes the additional configuration tasks that apply to AutoVu City Parking Enforcement, City Parking Enforcement with Wheel Imaging, and University Parking Enforcement systems.

This section includes the following topics:

Roadmap for City Parking Enforcement configuration

The following table lists the tasks required to configure AutoVu for City Parking Enforcement (with or without wheel imaging), and links you to the configuration procedures.

Phase	Description	See
1	Perform the general AutoVu configuration tasks that lead up to the specific City Parking Enforcement configuration tasks described in this chapter.	• "Roadmap for mobile deployment" on page 47
2	Create and configure the overtime rules for your enforcement scenario.	• "Create an overtime rule" on page 212 • "Configure an overtime rule" on page 212
3	Create and configure the permit lists for your enforcement scenario.	• "Create a permit" on page 215 • "Configure a permit" on page 216
4	(Optional) Create and configure hotlists, if applicable.	• "Configuring hotlists" on page 120
5	(*City Parking Enforcement with Wheel Imaging* only) Calibrate the Navigator box to provide accurate odometry readings to Patroller.	• "Calibrating the Navigator box for wheel imaging" on page 225
6	Enable and configure overtime rules in Patroller.	• "Configure Patroller overtime settings" on page 245
7	Enable and configure permit lists in Patroller.	• "Configure Patroller permit settings" on page 247
8	(*City Parking Enforcement with Wheel Imaging* only) Configure the Patroller settings related to wheel imaging.	• "Configuring Patroller wheel imaging settings" on page 248
9	Configure the Patroller GPS and Map settings. All parking enforcement systems require GPS and mapping capability.	• "Configure GPS settings" on page 190 • "Configure Map settings" on page 191

Roadmap for University Parking Enforcement configuration

The following table lists the tasks required to configure AutoVu for University Parking Enforcement, and links you to the configuration procedures.

Phase	Description	See
1	Perform the general AutoVu configuration tasks that lead up to the specific University Parking Enforcement configuration tasks described in this chapter.	• "Roadmap for mobile deployment" on page 47
2	Create and configure the overtime rules for your enforcement scenario.	• "Create an overtime rule" on page 212 • "Configure an overtime rule" on page 212
3	Create and configure the permit lists for your enforcement scenario.	• "Create a permit" on page 215 • "Configure a permit" on page 216
4	Create and configure the permit restrictions for your enforcement scenario.	• "Create a permit restriction" on page 219 • "Configure a permit restriction" on page 220
5	Create and configure parking lots for your overtime rules and permit restrictions.	• "Configure parking lots in Security Center" on page 223
6	(Optional) Create and configure hotlists, if applicable.	• "Configuring hotlists" on page 120
7	Enable and configure overtime rules in Patroller.	• "Configure Patroller overtime settings" on page 245
8	Enable and configure permit lists in Patroller.	• "Configure Patroller permit settings" on page 247
9	Configure the Patroller GPS and Map settings. All parking enforcement systems require GPS and mapping capability.	• "Configure GPS settings" on page 190 • "Configure Map settings" on page 191

Configuring overtime rules in Security Center

You can use overtime rules for both City Parking Enforcement and University Parking Enforcement. This section explains how to set up overtime rules. First you create the overtime rule entity, then you configure the entity's settings for your enforcement scenario.

This section includes the following topics:

Create an overtime rule

You create an overtime rule entity in Security Center Config Tool. After you create the entity, you'll configure its settings for your enforcement scenario.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, click **LPR** > **Overtime rules**, then click () **Overtime Rule**.

3 In the Identity tab that opens, enter the required information:

- *Name.* In City Parking Enforcement, this name will appear in Patroller on the overtime rule selection page. In University Parking Enforcement, this name will appear appended to the parking lot name on the zone selection page. For more information on how zones work in University Parking Enforcement, see "About parking lots and zones in Patroller" on page 22.

  TIP Choose a name that describes the details of the enforcement scenario. This makes it easier to select it in Patroller when you have more than one available.

- *(Optional) Description.* You can add a longer description for the rule. This field does not appear in Patroller.
- *(Optional) Logical ID.* Enter a Logical ID if applicable.

4 Click **Apply**.

The overtime rule appears in a flat list view that displays all the overtime rules on your system. Patroller downloads overtime rules when it connects to Security Center.

After you are done: See "Configure an overtime rule" on page 212.

Configure an overtime rule

After you have created an overtime rule entity in Security Center Config Tool, you need to configure it for your enforcement scenario.

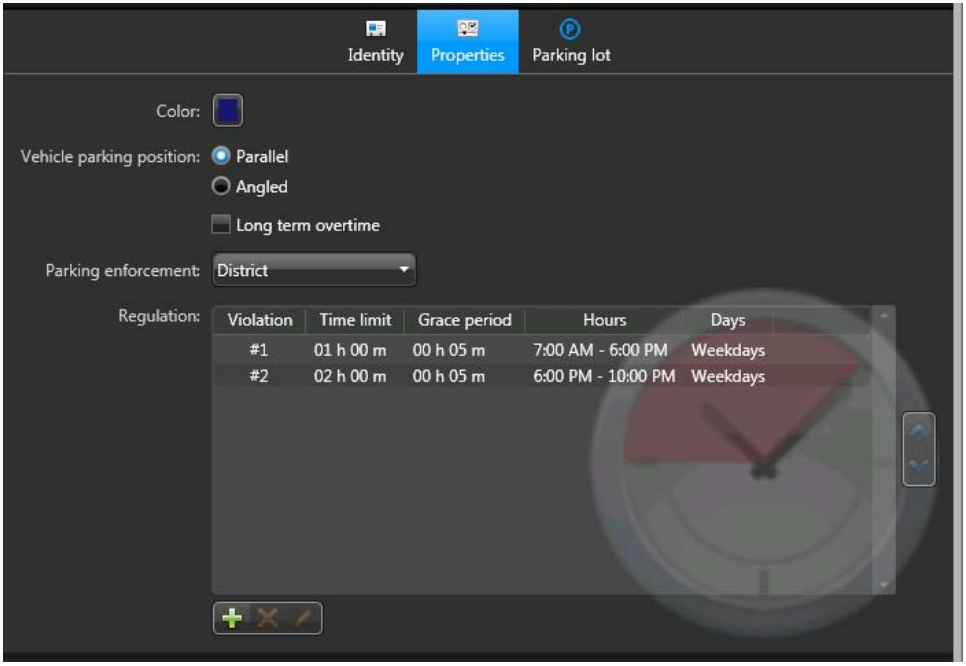
Before you begin: See "Create an overtime rule" on page 212.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, click **LPR** > **Overtime rules.**

3 Select the rule you want to configure, then click **Properties**.

The **Properties** page appears.



4 Select a **Color** for the overtime rule.

This will be the color of the overtime hit screen in Patroller and Security Desk, as well as the plate reads due for enforcement on the Patroller map.

5 (City Parking Enforcement with Wheel Imaging only) Select the **Vehicle parking position**.

Tells Patroller which parameters to use for wheel imaging: Parallel or Angled (45-degree).

NOTE You cannot use the same overtime rule for both Parallel and Angled parking enforcement. If you're doing both types of enforcement, you need to create separate overtime rule entities for each.

6 (Optional) Select **Long term overtime** to allow vehicles to park in the same spot for over 24 hours.

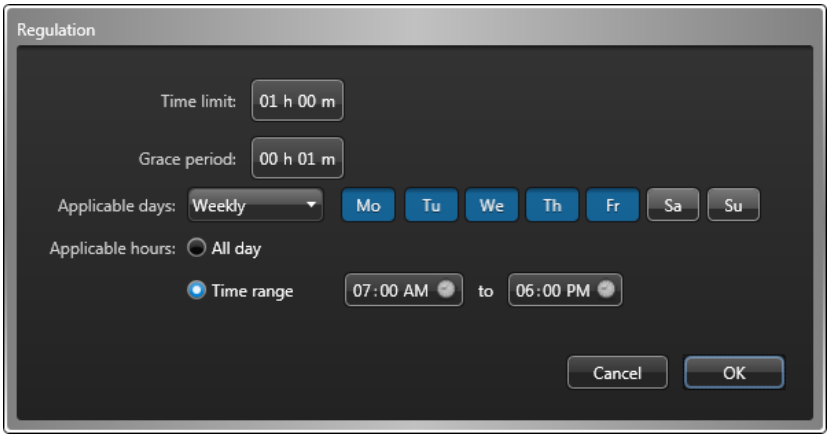
When selected, the parking time limit is specified in days (2 to 5 days), and the *Parking enforcement* option is automatically set to *Same position*.

7 From the **Parking enforcement** list, select **District**, **Block face (2 sides)**, or **Same position**.

For more information on each type of overtime rule, see "Types of overtime rules" on page 12.

8 Under **Regulation**, click **Add an item** ( ) to define the parameters of the overtime rule (e.g time limit, grace period, applicable days, etc).

The **Regulation** window appears.



9 Configure the following, then click **OK**:

- *Time limit.* Enter how long in hours and minutes a vehicle is allowed to park.
- *Grace period.* Add extra time beyond the *Time limit* before raising an overtime hit. For example, if you set a 10 minute time limit, and a 5 minute grace period, Patroller will raise a hit after 15 minutes.
- *Applicable days.* Select which days to enforce the *Time limit*.
- *Applicable hours.* Select what time of day to enforce the *Time limit*.

10 (Optional) Under **Regulation**, configure multiple violations as needed.

This specifies the maximum number of citations that can be issued to the same vehicle for the same overtime offence. For more information, see "About multiple violations" on page 17.

11 Click **Apply**.

The overtime rule is configured, and will be downloaded to Patroller the next time it connects to Security Center.

After you are done: See the following:

- (If applicable) "Calibrating the Navigator box for wheel imaging" on page 225.
- "Configuring Patroller for City and University Parking Enforcement" on page 244.

Configuring permits and permit restrictions in Security Center

You can use permits for both City Parking Enforcement and University Parking Enforcement. In University Parking Enforcement, you also need to apply restrictions to permits to create an enforcement rule. This section explains how to set up permits, and how to configure permit restrictions for them when needed.

This section includes the following topics:

Create a permit

You create a permit entity in Security Center Config Tool. After you create the entity, you'll configure its settings for your enforcement scenario.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, click **LPR** > **Permits**, then click () **Pemit**.

3 In the Identity tab, enter the required information:

- *Name.* In City Parking Enforcement, this name will appear in Patroller on the permit selection page.

  TIP Choose a name that describes the details of the enforcement scenario. This makes it easier to select it in Patroller when you have more than one available.

- *Description.* You can add a longer description for the permit. This field does not appear in Patroller.
- *(Optional) Logical ID.* Enter a Logical ID if applicable.

4 Click **Apply**.

The permit appears in a flat list view that displays all the permits on your system.

All newly-created hotlists and permit lists are automatically downloaded to Patroller when a connection to Security Center is available. If you don't want a hotlist or permit list to be downloaded to Patroller, you can deactivate it from the LPR Manager's **File association** page (see "File association" on page 289).

After you are done: See "Configure a permit" on page 216.

Configure a permit

After you have created a permit entity in Security Center Config Tool, you need to configure it for your enforcement scenario.

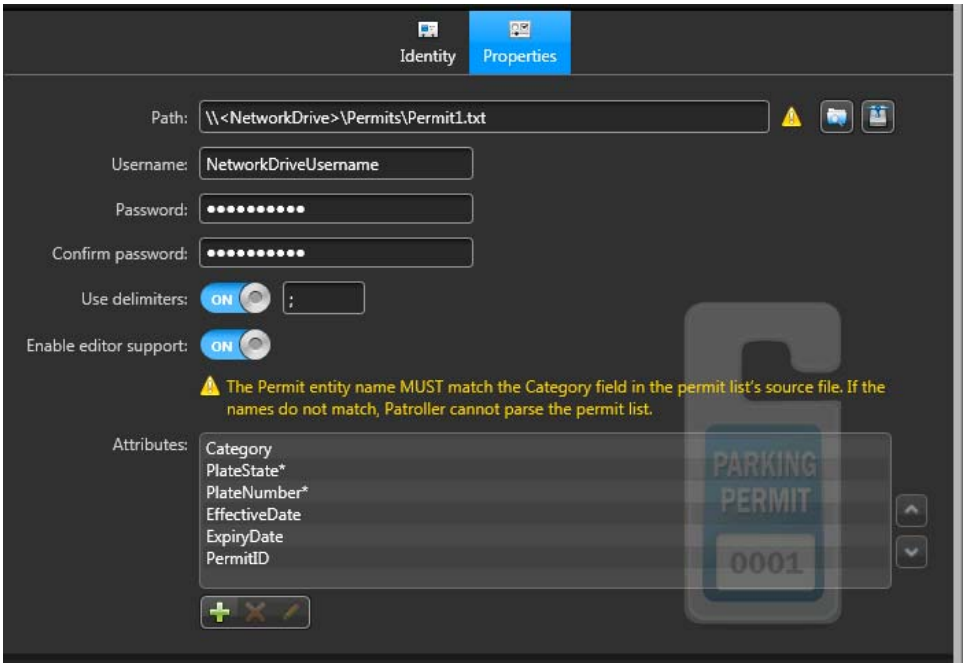
Before you begin: See "Create a permit" on page 215.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, click **LPR** > **Permits**.

3 Select the permit you want to configure, then click **Properties**.

The **Properties** page appears.



4 Enter the **Path** on the computer where the permit list's source file is located.

The source file must be accessible from the computer hosting the LPR Manager.

5 Turn **Use delimiters** on or off, and enter the type of delimiter used.

Tells Security Center that the fields in the source text file are of variable length, and indicates the type of character used to separate each field in the file. By default, **Use delimiters** is set to **On**, and the delimiter specified is a **semi-colon** (;). If your source text file is made up of fixed length fields, set **Use delimiters** to **Off**.

Security Center supports the following delimiters:

- Colon (:)
- Comma (,)

- Semi-colon (;)
- Tab (Tab)

If your source list file uses Tab as a delimiter (i.e. the "Tab" key on your keyboard), type the word "Tab" as the delimiter character.

IMPORTANT Security Center considers one Tab space to be a valid delimiter. Do not use more than one Tab space to align columns in your file or Security Center may not be able to parse the permit list.

6 Turn **Enable editor support** on or off.

Allow a user to edit the permit list in the *Hotlist and permit* editor task.

IMPORTANT In order to edit a permit list in Security Desk, the *Hotlist and permit* editor privilege must be granted to the user. For more information on user privileges, see the *Security Center Administrator Guide*.

7 Configure the **Attributes** to match the permit list's text file.

Tells Security Center the name and order of the fields (attributes) in the source text file. You can add, delete, or edit the fields.

IMPORTANT There cannot be any spaces within an attribute name.

- *Category.* (Mandatory field) The name of the parking permit. This field in the permit list's source text file *must* match the permit entity name for the entry to be downloaded to Patroller.

  This field allows you to use one permit list for several permit entities on your system, provided you create permit entities for each permit category in your permit list.

  EXAMPLE Here is a simple permit list with three different permit categories (*Students*, *Faculty*, and *Maintenance)*.

  You can use this same permit list for three different permit entities. Create a *Students* permit entity, a *Faculty* permit entity, and a *Maintenance* permit entity, and then point all of them to the same source text file. Security Center will extract the license plates (and related information) whose category is the same as the name of the permit entity.

  IMPORTANT The permit entity name *must* match the category name exactly.

- *PlateState.* (Mandatory field) Issuing state (or province, or country) of the license plate.
- *PlateNumber.* (Mandatory field) The license plate number.

The following fields are shown by default, but are optional.

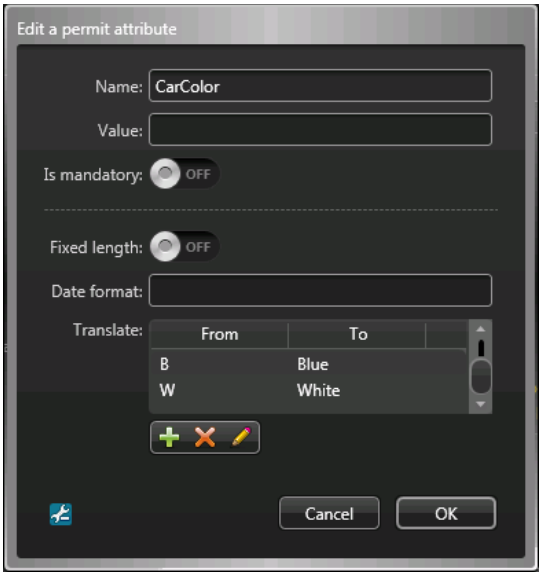
- *EffectiveDate.* Date from which the particular permit on the list starts to be effective.
- *ExpiryDate.* Date after which the particular permit on the list is no longer valid.

- *PermitID.* (*University Parking Enforcement* only) Used when multiple entries in a permit list share the same permit (e.g. car pool permits). Can be used to identify the number of the permit issued to the vehicle whose license plate is identified in *PlateNumber*. In the case of shared permits, normally up to four separate vehicles would all have the same permit number.

  A violation results in a *Shared Permit* hit in Patroller. For more information, see "About shared permits" on page 22.

8 (Optional) Add (+) or edit (✎) an attribute.

The Attribute window appears.



Configure the following:

- *Name.* Only the three compulsory fields, *Category*, *PlateState,* and *PlateNumber* cannot be renamed. Names may contain spaces.
- *Value.* The default value is interpreted differently depending on whether delimiters are used or not.
  - If delimiters are in use, the default value is written into this field. Fields already populated will be overwritten.
  - If delimiters are not in use, and if the field is empty, the default value is written into this field. Fields already populated will not be overwritten.
- *Is mandatory.* A mandatory attribute cannot be blank in the hotlist source file. For example, if you add a mandatory attribute called *CarColor*, the column for *CarColor* in the hotlist must have text in it.

- *Fixed length.* This option is enabled only if you chose to use fixed length data fields. Indicate the start position of the field in the file record and its length. The position of the first character is zero (0).
- *Date format.* Specify a time format if the field contains a date or time value. All standard date and time format strings used in Windows are accepted. If nothing is specified, the default time format is "yyyy-MM-dd".

  For example, the following is what you may find in a variable field length data file using a semicolon (;) as delimiter and using the fields: *Category*, *PlateState*, *PlateNumber*, *EffectiveDate*, *ExpiryDate*, and *PermitID*.

  ```
  MyPermit;QC;DEF228;2012-01-31;2012-05-31;PermitID_1
  MyPermit;QC;345ABG;2012-01-31;2012-07-25;PermitID_2
  MyPermit;QC;067MMK;2012-03-31;2012-09-11;PermitID_1
  MyPermit;QC;244KVF;2012-01-31;2012-03-31;PermitID_3
  ```

- *Translate.* You can apply an optional transformation to the values read from the data file. Use this feature to shorten certain values to save space on the Patroller or to enforce spelling consistency.

9 (Optional) Delete (✖) an attribute.

If you aren't using one of the attributes in the permit list, you can delete it. For example, if the permits on your list don't expire, you can delete the *ExpiryDate* attribute.

10 Click **Apply**.

The permit entity is configured and enabled in Security Center.

After you are done: See "Configuring Patroller for City and University Parking Enforcement" on page 244.

Create a permit restriction

You create a permit restriction entity in Security Center Config Tool. After you create the entity, you'll configure its settings for your enforcement scenario.

Before you begin: See "Create a permit" on page 215 and "Configure a permit" on page 216.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, click **LPR** > **Permit restrictions**, then click (✚) Permit.

3 Enter the required information:

- *Name.* This name will appear appended to the parking lot name on the zone selection page. For more information on how zones work in University Parking Enforcement, see "About parking lots and zones in Patroller" on page 22.

  TIP Choose a name that describes the details of the enforcement scenario. This makes it easier to select it in Patroller when you have more than one available.

- *Description.* You can add a longer description for the permit restriction. This field does not appear in Patroller.
- *(Optional) Logical ID.* Enter a Logical ID if applicable.

4 Click **Apply**.

The permit restriction appears in a flat list view that displays all the permit restrictions on your system. Patroller downloads permit restrictions when it connects to Security Center.

After you are done: See "Configure a permit restriction" on page 220.

Configure a permit restriction

After you have created a permit restriction entity in Security Center Config Tool, you need to configure it for your enforcement scenario.

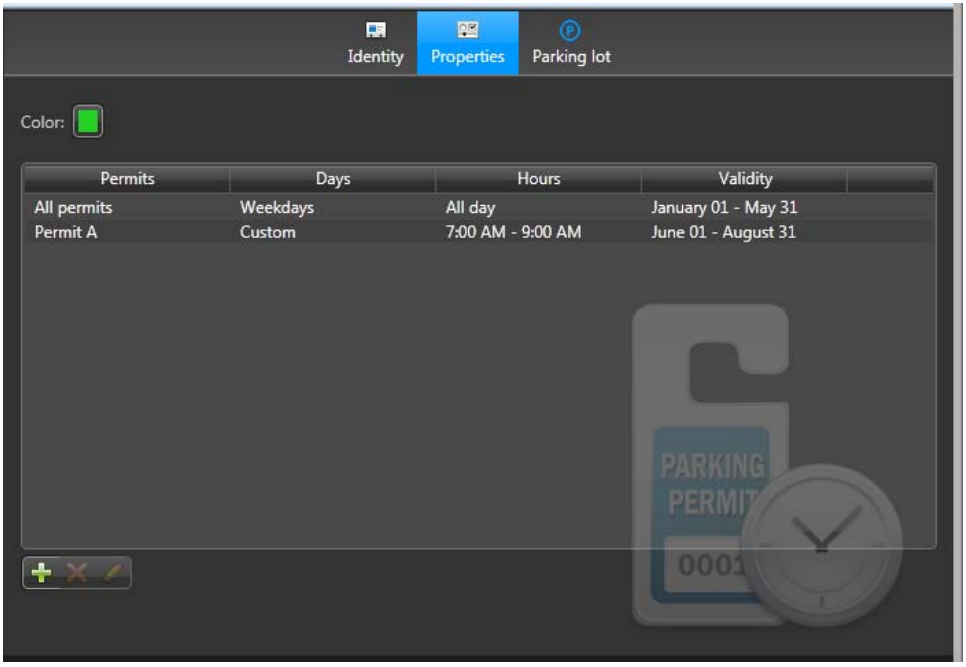
Before you begin: See "Create a permit restriction" on page 219.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, click **LPR** > **Permit restrictions**.

3 Select the permit restriction you want to configure, then click **Properties**.

The **Properties** page appears.

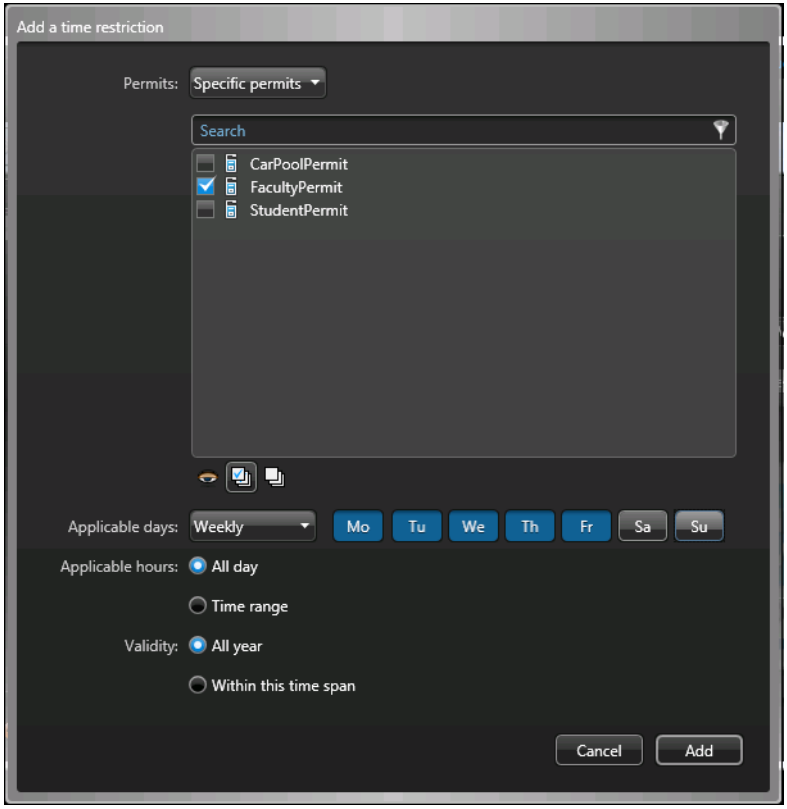


4 Click the **Color** icon to assign a color to the permit restriction.

This will be the color of the permit hit screen in Patroller and Security Desk, as well as the plate reads due for enforcement on the Patroller map.

5 Click the create button ( ) to define a time restriction, and apply it to one or more permits.

The **Time restriction** window appears.



6 From the **Permits** drop-down list, select which permits the restriction applies to:

- *Everyone.* Parking is available to everyone, regardless of whether they have a permit or not. No restriction is enforced during the specified time period. This restriction is used in conjunction with other restrictions as a temporary override. For example, if a university is hosting a football game, parking would be made available to everyone during the game instead of specific permit holders.
- *No permit.* Only vehicles without permits can park. For example, you can use this type of restriction to reserve a zone for visitors parking. A plate read that matches any of the permits downloaded to the Patroller raises a hit.
- *All permits.* Only vehicles with a permit can park. A plate read that does not match any of the permits downloaded to the Patroller raises a hit.

- *Specific permits.* Only vehicles having one or more of the specified permits can park. A plate read that does not match any of the specified permits raises a hit.

When multiple time restrictions apply at a given time, conflicts are resolved by evaluating the restrictions in the following order: 1. *Everyone*, 2. *No permit*, 3. *All permits*, 4. *Specific permits*.

Moreover, a hit is raised when a matched permit is not valid (either not yet effective or already expired).

7 In **Applicable days**, select the days of week when parking is allowed.
- *Always.* Seven days a week.
- *Weekly.* Monday to Friday.
- *Weekend.* Saturday and Sunday.
- *Custom.* Select the days that apply.

8 In **Applicable hours**, select the times during the day when parking is allowed.

9 In **Validity**, select the dates during the year when parking is allowed.

10 Click **OK**.

The permit restriction entity is configured and enabled in Security Center.

After you are done: See "Configure parking lots in Security Center" on page 223.

Configure parking lots in Security Center

You need to configure an enforcement area (i.e. parking lot) for each enforcement rule (i.e. overtime rule or permit restriction) you create. This combination of enforcement rule and parking lot creates the parking zone that is displayed in Patroller.

You create parking lots in Security Center Config Tool by drawing a polygon around the parking lot's geographical location on the map.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, click **LPR** > **Overtime rules** or **Permit restrictions**.

3 Select the overtime rule or permit restriction you want to configure, then click **Parking lot**.

The map appears.

NOTE This map is for an overtime rule, but the same steps apply for permit restrictions.

4 Zoom in to the area of the map where your parking lot is located.

Make sure the entire parking lot is visible on the map, and that you are in **Aerial** view.

5 Click the create button, enter the name and numbers of spaces in your parking lot, then click **OK**.

The cursor changes to crosshairs.

This name will appear in Patroller along with the *Overtime rule* or *Permit restriction* name, to display an enforcement zone. For more information on how zones work in University Parking Enforcement, see "About parking lots and zones in Patroller" on page 22.

TIP Choose a name that describes where the parking lot is. This makes it easier to select the parking zone in Patroller when multiple zones are available.

6 On the map, click to create the first corner of the polygon, then move the crosshairs to the next corner.

A thick blue line appears, joining the point you just clicked on the map and where the crosshairs are.

7 Click again to mark the second corner of the polygon.

8 Continue this process until you returned to the initial position, then click on the starting corner to close the polygon.

9 Click **Apply**.

10 (Optional) To edit the parking lot's name or number of spaces, click the edit button, then click the parking lot.

NOTE If you want to change the shape of the polygon, you have to delete the parking lot and create a new one. You can't directly edit the polygon shape.

11 (Optional) To delete the parking lot, click the delete button, then click the parking lot.

The parking lot appears as a filled polygon with a thick blue border on the map. The name of the parking lot and its number of spaces are written in the center.

After you are done: See "Configuring Patroller for City and University Parking Enforcement" on page 244.

Calibrating the Navigator box for wheel imaging

The Navigator box provides the positioning and odometry accuracy needed for a City Parking Enforcement with Wheel Imaging installation.

Before you can use the Navigator box, you need to calibrate it for use with the Patroller vehicle. Navigator box calibration is a two-part procedure. You perform the initial calibration with the IO Services software installed with Patroller, and then you use the Genetec oscilloscope application to filter out the vehicle's random engine noise.

This section includes the following topics:

About the Navigator box

The AutoVu Navigator box provides Patroller with more accurate geographic coordinates than a standard GPS device. It is required for City Parking Enforcement with Wheel Imaging systems.

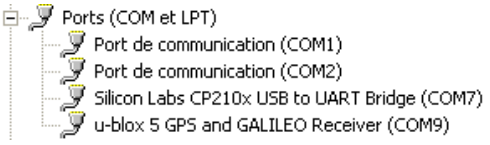
The Navigator box comes with a GPS receiver that receives satellite positioning information, but it *also* taps into the vehicle's odometer readings and has an internal gyroscope. This provides greater accuracy than GPS alone. For example, drive through a long tunnel and you'll lose the GPS satellite signal, but the Navigator box still knows how far and how fast you're driving (odometry signal), and if you change direction (gyroscope).

In City Parking Enforcement with Wheel Imaging, you need the Navigator box to know if the parked vehicle has moved even a small distance. GPS alone cannot provide an accurate enough reading to be able to enforce this rule.

The Navigator box is installed in the vehicle, and is connected to the vehicle's odometry signal (usually by tapping the vehicle speed sensor), and to the in-vehicle computer. Some calibration is required.

Before you begin Navigator box calibration

Before you begin, you'll need to perform the following tasks:

	Task	More information
❑	Install the Navigator box in the vehicle.	See Chapter 8, "Installing mobile AutoVu hardware" on page 65.
❑	Install AutoVu Patroller on the in-vehicle computer.	See "Installing AutoVu Patroller" on page 87.
❑	Start Patroller.	Patroller must be running to access IO Services. Go to **Start** > **All Programs** > **Genetec AutoVu X.Y**, then start **Patroller**.
❑	Find the COM Ports of the Navigator box and its GPS receiver. You'll need this information to log on to the oscilloscope, and to enter in Patroller Config Tool.	Go to Windows Device Manager, expand **Ports (COM and LPT)**, and look for the following: • **Navigator box port.** Seen by Windows as *Silicon Labs CP210x USB to UART Bridge*. • **GPS Antenna port.** Seen by Windows as *u-blox 5 GPS and GALILEO Receiver*. **EXAMPLE** In the example below, the Navigator box is on COM Port 7, and its GPS Antenna is on COM Port 9. 
❑	Turn on the GPS and Navigator box in Patroller Config Tool, then specify the COM Ports they are using.	1 Open Patroller Config Tool. 2 Go to **Navigation** > **GPS**, turn on **GPS**, then enter the **Port** number. 3 Go to **Navigation** > **Odometry**, turn on **NavBox**, then enter the **Port** number.
❑	Copy the oscilloscope application to the in-vehicle computer.	The oscilloscope application is available on the USB key included with the Navigator box. **NOTE** If you don't have the USB key, contact your Genetec representative for more information on how to get the oscilloscope application.

Calibrating the Navigator box using the oscilloscope

Oscilloscope calibration is the first of a two-part calibration procedure for the Navigator box. In this procedure, you'll use the oscilloscope software (the scope) to fine-tune the Navigator box to filter out the vehicle's random engine noise.

The vehicle's engine activity is represented by an analog signal wave. The peaks and valleys of the wave represent both real vehicle movement, and noise (vehicle running but idle). You need to calibrate the Navigator box so that it can identify which parts of the analog signal wave represent vehicle movement, and which parts represent noise.

To do this, you'll use the scope to capture a sample signal, then you'll analyze the signal to determine the proper sensitivity setting for the Navigator box.

IMPORTANT This procedure is best performed with two people: one to drive the Patroller vehicle, and the other to use the scope.

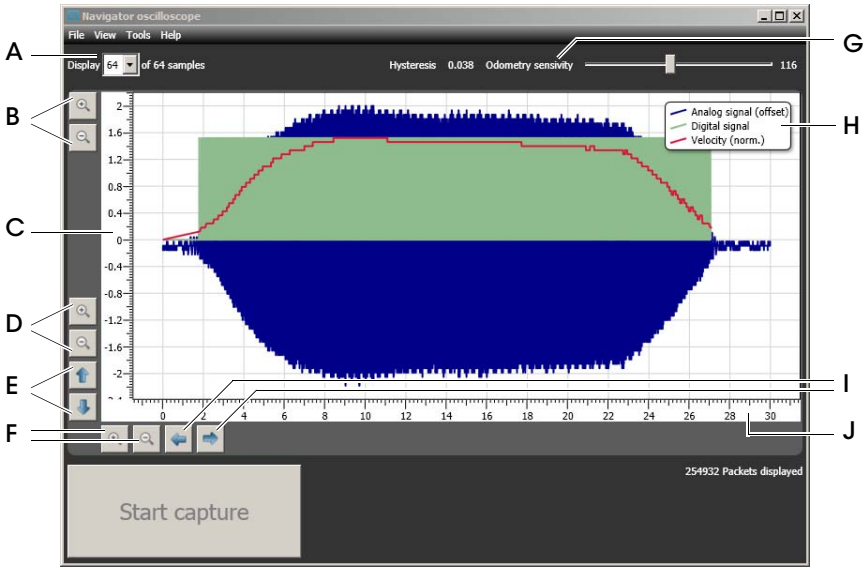
Before you begin: Perform the tasks in "Before you begin Navigator box calibration" on page 226.

This section includes the following topics:

About the oscilloscope user interface

This topic describes the main controls you'll use to analyze a sample signal after you import it. A 30 second sample is used as an example.

NOTE By default, only the **Analog signal (offset)** is shown. The offset makes it visually easier to perform the calibration. You can display the true analog signal (with the real voltage values) from the **View** menu.



A	Sampling rate	The rate at which digital values are sampled from the analog signal. • When capturing, display **1 of 64** to minimize CPU effort. • When analyzing, display **64 of 64** to get a clearer signal.
B	Zoom in/out	General zoom in/out. Not specific to either the Y-axis or X-axis. If you have a wheel mouse, you can also use the wheel to zoom in/out.
C	Y-axis	Displays voltage.
D	Zoom in/out (Y-axis)	Zoom in to the y-axis to focus on a smaller unit of voltage.
E	Scroll up/down	Scroll the signal vertically.
F	Zoom in/out (X-axis)	Zoom in to the x-axis to focus on a smaller unit of time.
G	Odometry sensitivity	Slide left/right to adjust the digital signal line.

H	Signal views	• **Display analog signal (not shown in example).** The analog signal represents vehicle engine activity. This view displays the analog signal with its true voltage values. You don't need this signal to perform the calibration, but it can be useful as a reference. • **Display analog signal (offset).** Same as the analog signal but with an offset to zero voltage. Use this view for calibration. • **Display digital signal.** The digital signal represents the Navigator box. Adjusting the sensitivity setting will move the digital signal line, and tell the Navigator box which part of the analog signal to "trigger" on (i.e. which part of the analog signal represents true vehicle movement). • **Display normalized velocity.** Represents the vehicle's velocity. Use this as a reference to see when the vehicle was accelerating, decelerating, or stopped.
I	Scroll left/right	Scroll the signal horizontally.
J	X-axis	Displays time.

Capture a sample signal

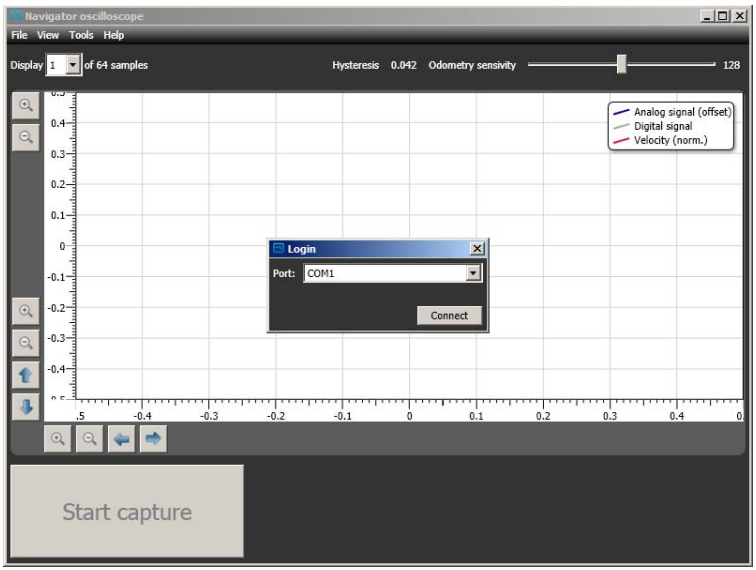
To capture a sample signal, you'll perform three basic driving scenarios. You'll speed up from a complete stop, travel at a constant speed, and then slow down to a complete stop.

Before you begin: Close Patroller. The scope cannot connect to the Navigator box's COM Port if Patroller is running.

1 Stop the vehicle, but keep the engine running.

2 Double-click *Oscilloscope.exe*.

The main window and **Login** dialog box appear.



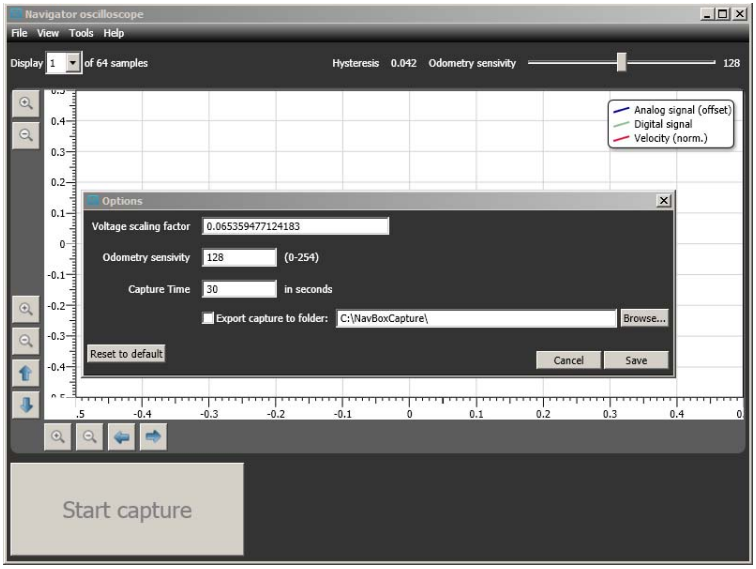
3 In the **Login** dialog box, select the Navigator box's COM Port from the drop-down list, then click **Connect**.

For more information on the Navigator box's COM Port, see "Before you begin Navigator box calibration" on page 226.

4 From **Display X of 64 samples**, select **1**.

5 Click **Tools** > **Options**.

The *Options* window appears.



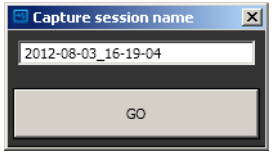
6 Configure the following, then click **Save**:

- *Voltage scaling factor.* Do **not** adjust this setting.
- *Odometry sensitivity.* Do **not** adjust this setting.
- *Capture time.* Enter the duration of the sample capture. Best practice is a 30-second sample. For example, you can speed up for 10 seconds, drive at a constant speed for the next 10 seconds, then slow down to a complete stop for the last 10 seconds.
- *Export capture to folder.* Specify where to save the sample file.

7 From the main window, click **Start capture**.

TIP If the **Start capture** button is unavailable, it means you're not connected to the correct COM port. Go to **File** > **Reconnect**, and connect to the Navigator box's COM Port.

8 The *Capture session name* dialog box appears.



9 Enter a filename.

The default filename is the current date and time (YYYY-MM-DD_hh-mm-ss). You can add to the name, or change it if you choose.

10 Name the file, click **GO**, then start driving as follows:

a Speed up gradually for 10 seconds until you reach approximately 40 km/h.

b If available, activate the vehicle's cruise control.

c Drive at a constant speed for 10 seconds.

d Slow down gradually for 10 seconds, until you come to a complete stop.

The 30 seconds capture ends. You have now captured a sample signal of the vehicle's engine.

After you are done: See "Analyze the sample signal" on page 232.

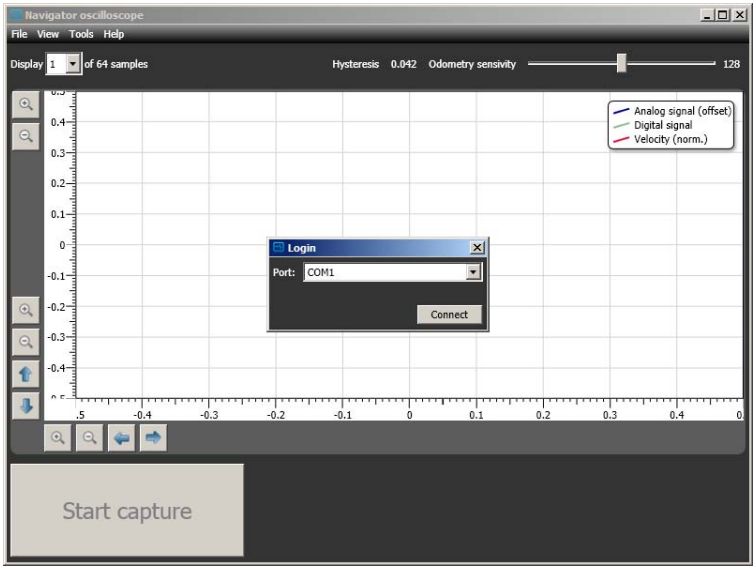
Analyze the sample signal

To determine the proper sensitivity setting, you'll need to analyze the sample signal you captured. First you'll learn how to differentiate between vehicle movement and noise. Then you'll adjust the scope's sensitivity setting so that the digital signal (which represents the Navigator box) "triggers" at the correct part of analog signal, the part that represents vehicle movement.

To perform the analysis, you need only the oscilloscope software, and access to the *.raw* data files from your capture session. You don't have to be connected to the Navigator box to perform the analysis. You can even use another computer with a larger screen if you choose.

1 Double-click *Oscilloscope.exe*.

The main window and **Login** dialog box appear.



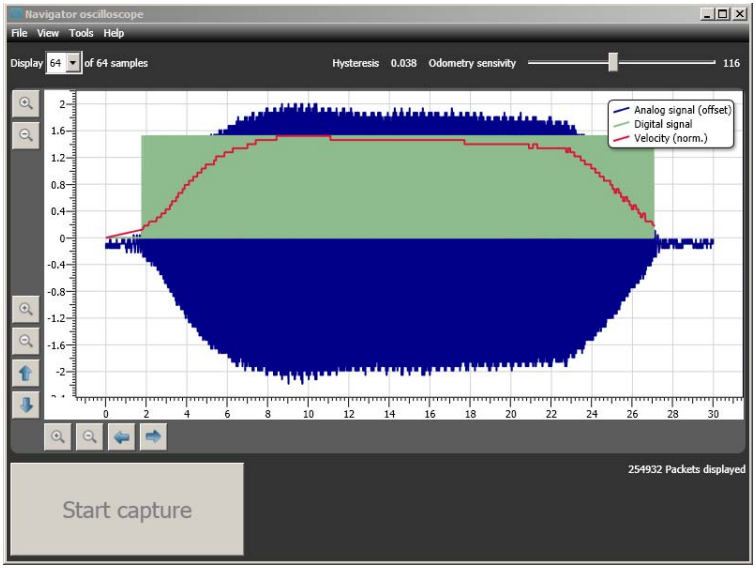
2 Close the **Login** dialog box.

3 From the **Display X of 64 samples** list, select **64**.

4 Go to **File** > **Import capture**, and select the *.raw* file you want to analyze.

The sample signal appears.

NOTE This sample signal is an example only. The signal from your Patroller vehicle may look different.



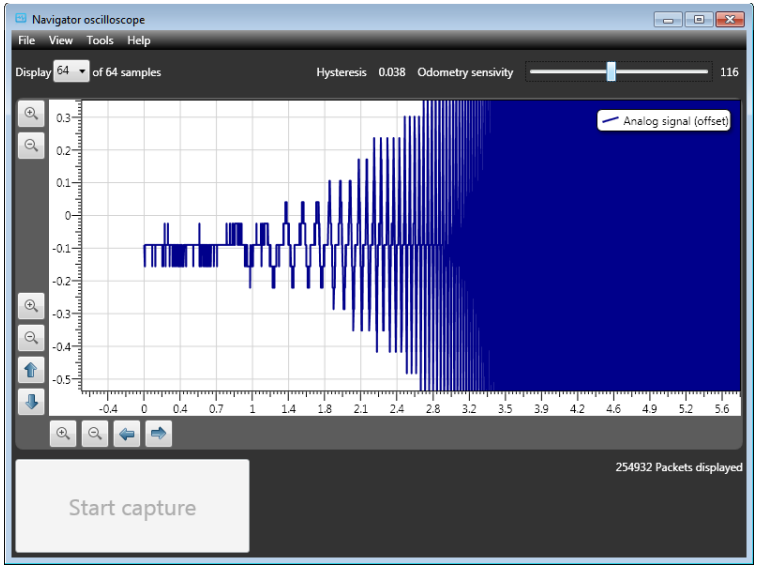
5 From the **View** menu, clear all options except **Display analog signal (offset)**.

The analog signal represents the vehicle's engine activity. Displaying the analog signal alone will help you identify noise in the signal.

6 Zoom in to display the first five or six seconds of the signal.

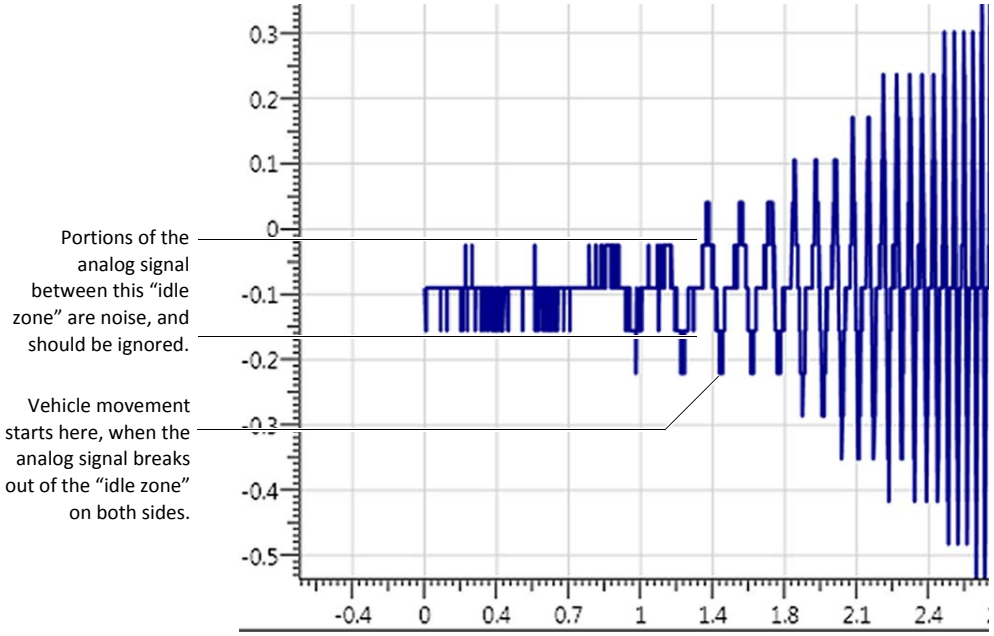
This is the best part of the signal to look for noise because you can see when the vehicle first started moving.

When zoomed in with only the **Analog signal (offset)** showing, the sample signal looks like this:



As you can see, the analog signal shows activity at zero seconds even though the vehicle was idle at that point. This represents noise. You want the Navigator box to ignore any part of the analog signal at this voltage.

An even closer look shows which part of the signal should be ignored.

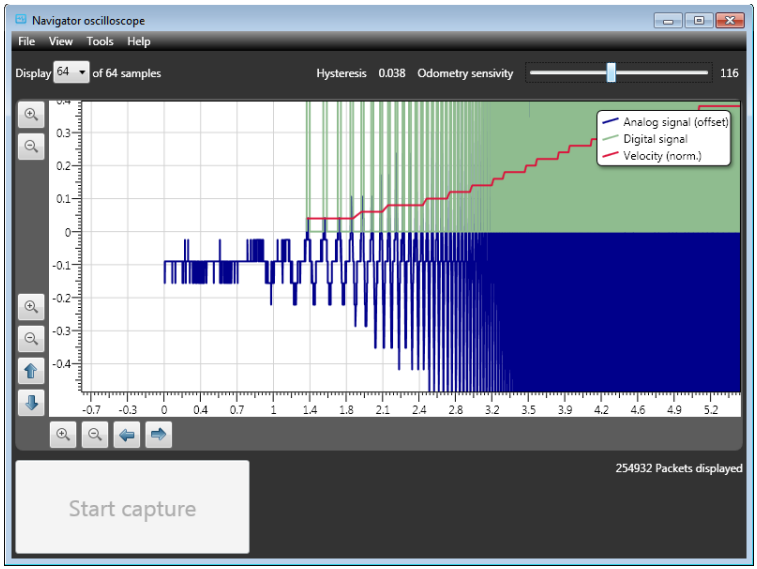


The vehicle only started moving approximately 1.4 seconds into the capture. That is the point where the analog signal broke out of the "idle zone".

Now that you know what part of the signal to ignore (idle zone), you need to configure the Navigator box to ignore it.

7 From the **View** menu, select **Display digital signal**, and **Display normalized velocity**.

With the digital signal and velocity showing, and the **Odometry sensitivity** at 116, the sample signal looks like this:

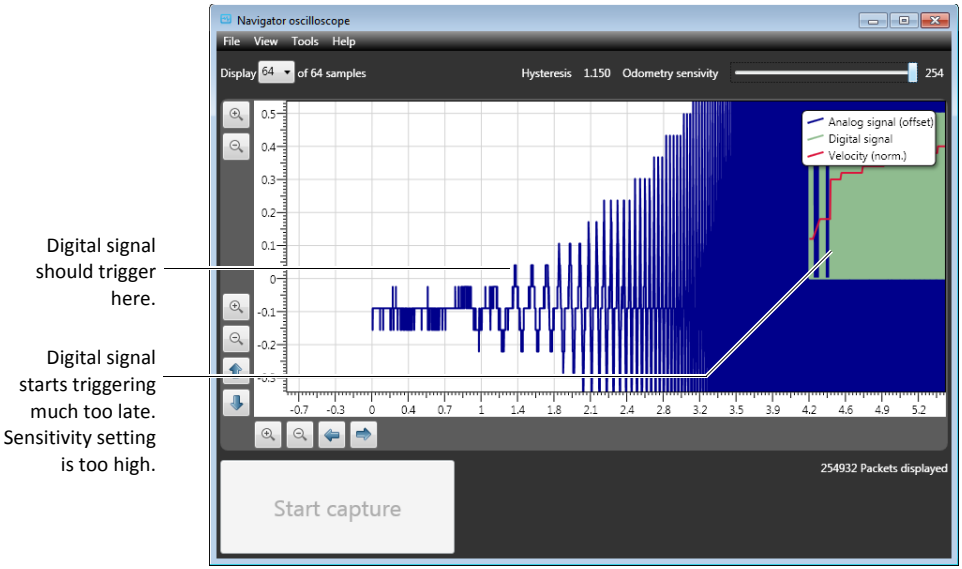


8 Drag the **Odometry sensitivity** slider left or right to adjust the starting position of the digital signal (which represents the Navigator box).

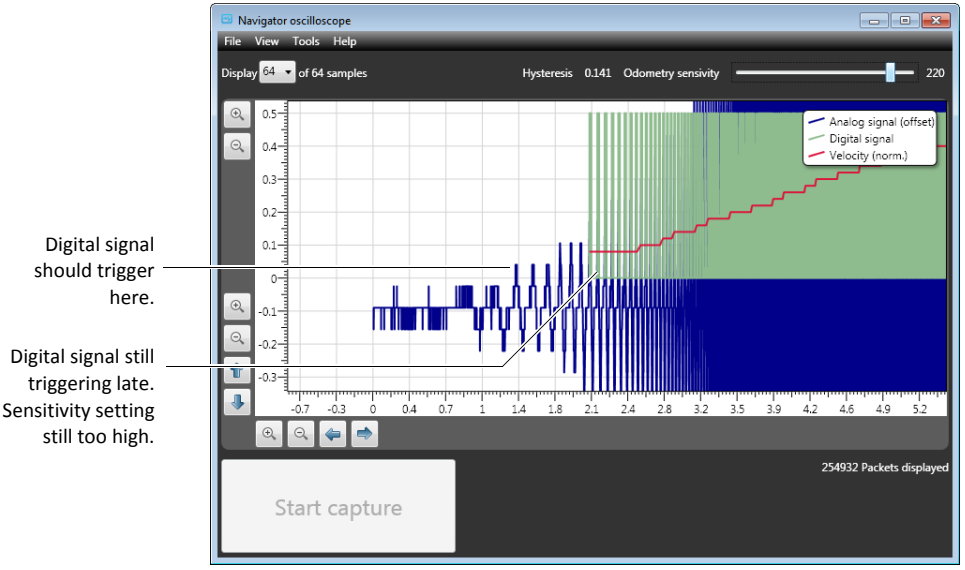
You want the digital signal to start where the analog signal breaks out of the idle zone you identified in Step 6. You are looking for the highest possible sensitivity setting that satisfies that condition.

Here are some examples of what the sample signal we are using looks like at different sensitivity settings:

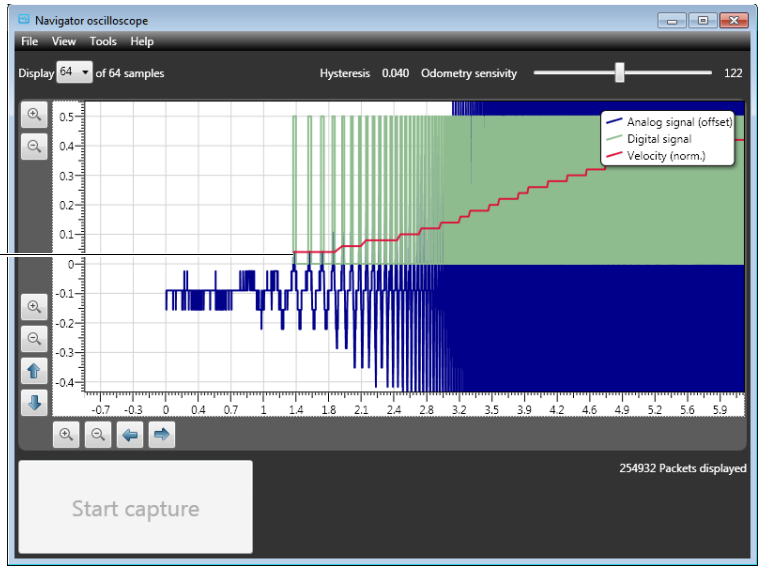
EXAMPLE Odometry sensitivity at 254 (maximum). Much too high. The digital signal (Navigator box) is triggering way too late.



EXAMPLE Odometry sensitivity at 220. Better, but still too high. The digital signal is triggering closer to the correct wave of the analog signal, but not close enough.



EXAMPLE Odometry sensitivity at 122. This setting is just right for the sample signal we are using. This is the highest sensitivity setting we could reach, and have the digital signal trigger at the correct point of the analog signal.



A sensitivity setting of 122 is perfect for the sample signal we are using in this procedure.

To confirm this setting, you can also perform this procedure using the end of the signal (when the vehicle was slowing down to a complete stop).

9 Open Patroller Config Tool, go to **Navigation** > **Odometry**, and enter the sensitivity number in the **Sensitivity** field.

10 Click **Apply**.

The Navigator box is properly calibrated. It will filter out random engine noise, and trigger on the parts of the analog signal that represent vehicle movement.

After you are done: See "Calibrate Navigator box using IO Services" on page 239.

Calibrate Navigator box using IO Services

This procedure is the second of a two-part calibration procedure for the Navigator box. You'll use the IO Services application installed with Patroller to determine the number of wheel ticks (ticks) your Patroller vehicle generates per meter travelled.

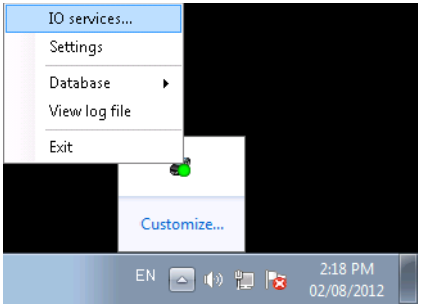
A “tick” is a pulse generated by the vehicle, typically by the transmission or drive shaft, whose frequency is proportional to the vehicle’s velocity. Because all vehicles have a different tick frequency, you’ll calibrate the Navigator box to know your vehicle’s specific tick frequency.

IMPORTANT This procedure is best performed with two people: one to drive the Patroller vehicle, and the other to use IO Services.

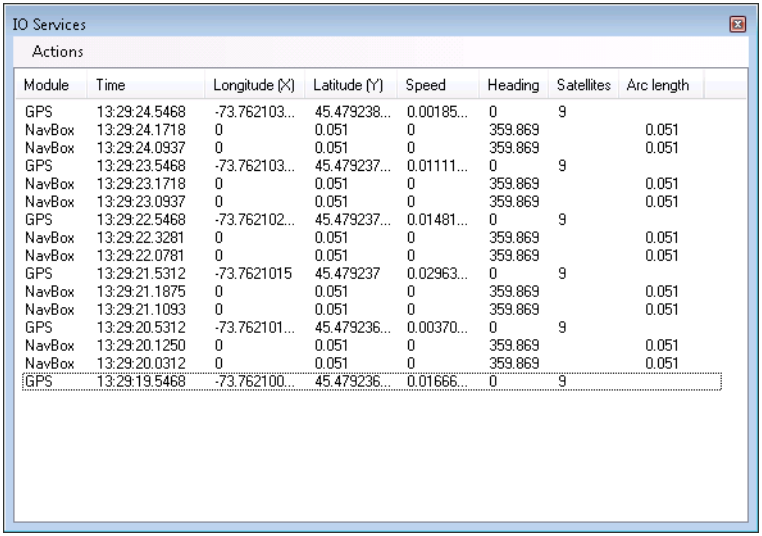
Before you begin: Perform the tasks in "Before you begin Navigator box calibration" on page 226.

1 Stop the vehicle, but keep the engine running.

2 On the in-vehicle computer, in the Windows system tray, right-click the Patroller icon and click **IO Services**.

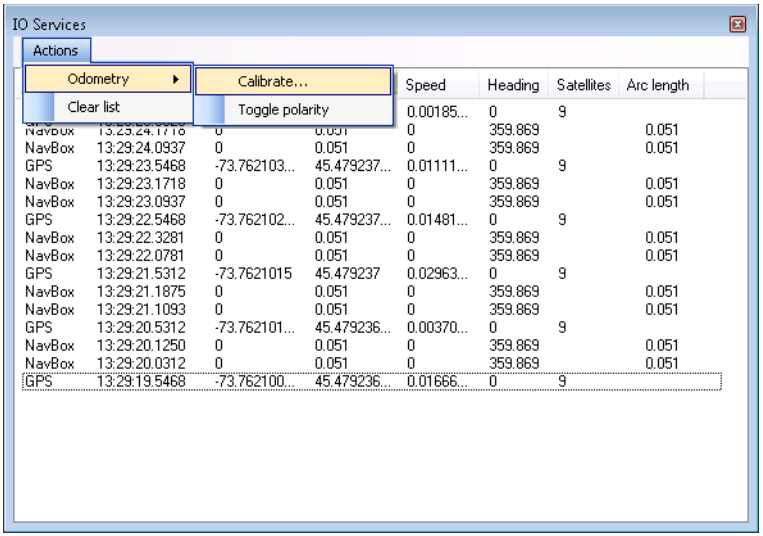


The **IO Services** window appears.

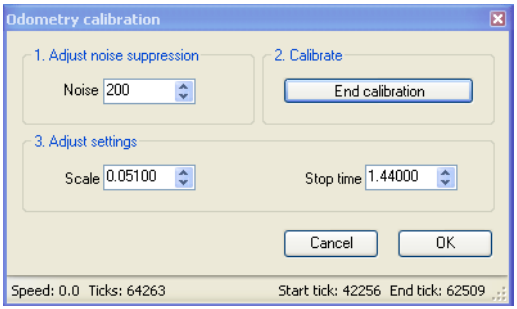


Module	Time	Longitude (X)	Latitude (Y)	Speed	Heading	Satellites	Arc length
GPS	13:29:24.5468	-73.762103...	45.479238...	0.00185...	0	9	
NavBox	13:29:24.1718	0	0.051	0	359.869		0.051
NavBox	13:29:24.0937	0	0.051	0	359.869		0.051
GPS	13:29:23.5468	-73.762103...	45.479237...	0.01111...	0	9	
NavBox	13:29:23.1718	0	0.051	0	359.869		0.051
NavBox	13:29:23.0937	0	0.051	0	359.869		0.051
GPS	13:29:22.5468	-73.762102...	45.479237...	0.01481...	0	9	
NavBox	13:29:22.3281	0	0.051	0	359.869		0.051
NavBox	13:29:22.0781	0	0.051	0	359.869		0.051
GPS	13:29:21.5312	-73.7621015	45.479237	0.02963...	0	9	
NavBox	13:29:21.1875	0	0.051	0	359.869		0.051
NavBox	13:29:21.1093	0	0.051	0	359.869		0.051
GPS	13:29:20.5312	-73.762101...	45.479236...	0.00370...	0	9	
NavBox	13:29:20.1250	0	0.051	0	359.869		0.051
NavBox	13:29:20.0312	0	0.051	0	359.869		0.051
GPS	13:29:19.5468	-73.762100...	45.479236...	0.01666...	0	9	

3 Click **Actions** > **Odometry** > **Calibrate**.



The **Odometry calibration** window appears.



4 At the bottom of the dialog box, verify the **Ticks**.

The ticks should not be changing at this time because the vehicle is stopped.

5 Do one of the following:

- If the ticks are *not* changing, continue to Step 6.
- If the ticks *are* changing, modify the **Adjust noise suppression** value until they are no longer changing, then continue to Step 6.

The number of ticks should not change when the vehicle is stopped.

6 Start driving until you reach approximately 40 km/h, then activate the cruise control.

NOTE If your vehicle doesn't have cruise control, try to drive at a constant speed for an accurate reading.

7 Take note of the number on the vehicle's odometer, or reset the vehicle's trip meter. You'll need to enter the distance you travelled as part of the calibration.

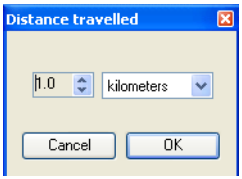
8 Click **Start calibration**.

9 Drive a distance of least one kilometer.

Best practice: To get the most accurate odometry reading, drive two to four kilometers.

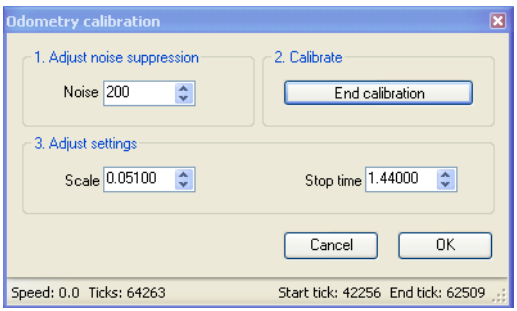
10 Pull to the side of the road, stop the vehicle, then click **End Calibration**.

The **Distance travelled** dialog box appears.



11 Enter the distance you travelled, then click **OK**.

The **Odometry calibration** window appears.



12 From the **Odometry calibration** window, take note of the value in the **Scale** field.

The "Scale" is the metres the vehicle travelled per tick. You'll need to enter this scale value in Patroller Config Tool

13 Click **OK**.

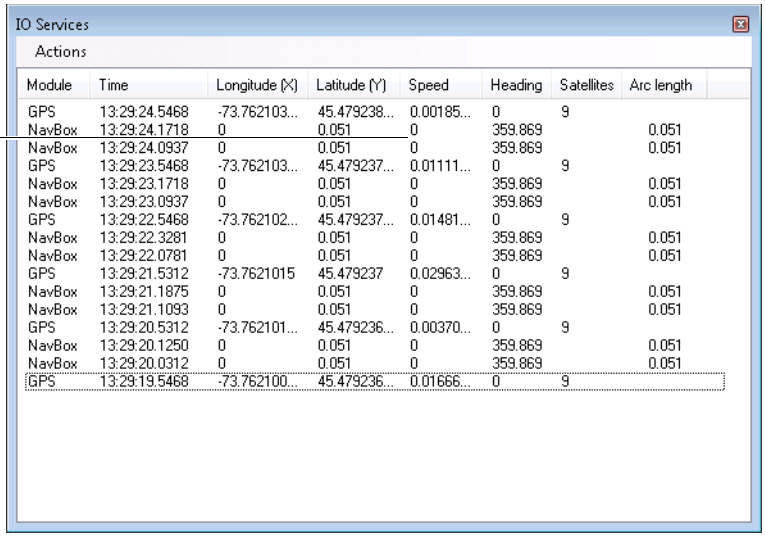
14 Validate the calibration:

a Start driving.

b From the IO Services window, see if the **Speed** field matches your vehicle's actual speedometer within 5 km/h.

If properly calibrated, the **Speed** should match your vehicle's speed within 5 km/h.

In this example, the speed is zero because the vehicle is not moving.



Module	Time	Longitude (X)	Latitude (Y)	Speed	Heading	Satellites	Arc length
GPS	13:29:24.5468	-73.762103...	45.479238...	0.00185...	0	9	
NavBox	13:29:24.1718	0	0.051	0	359.869		0.051
NavBox	13:29:24.0937	0	0.051	0	359.869		0.051
GPS	13:29:23.5468	-73.762103...	45.479237...	0.01111...	0	9	
NavBox	13:29:23.1718	0	0.051	0	359.869		0.051
NavBox	13:29:23.0937	0	0.051	0	359.869		0.051
GPS	13:29:22.5468	-73.762102...	45.479237...	0.01481...	0	9	
NavBox	13:29:22.3281	0	0.051	0	359.869		0.051
NavBox	13:29:22.0781	0	0.051	0	359.869		0.051
GPS	13:29:21.5312	-73.7621015	45.479237	0.02963...	0	9	
NavBox	13:29:21.1875	0	0.051	0	359.869		0.051
NavBox	13:29:21.1093	0	0.051	0	359.869		0.051
GPS	13:29:20.5312	-73.762101...	45.479236...	0.00370...	0	9	
NavBox	13:29:20.1250	0	0.051	0	359.869		0.051
NavBox	13:29:20.0312	0	0.051	0	359.869		0.051
GPS	13:29:19.5468	-73.762100...	45.479236...	0.01666...	0	9	

If the speed in IO Services matches your vehicle's speed within 5 km/h, continue to Step 15. If not, you need to repeat the calibration procedure.

15 Open Patroller Config Tool, go to **Navigation** > **Odometry**, enter the scale number from Step 12 in the **Scale** field, then click **Apply**.

Navigator box calibration using IO Services is complete.

After you are done: See "Configuring Patroller for City and University Parking Enforcement" on page 244.

Configuring Patroller for City and University Parking Enforcement

This section describes the settings and procedures required to configure Patroller for City Parking Enforcement (with and without wheel imaging), and for University Parking Enforcement.

This section includes the following topics:

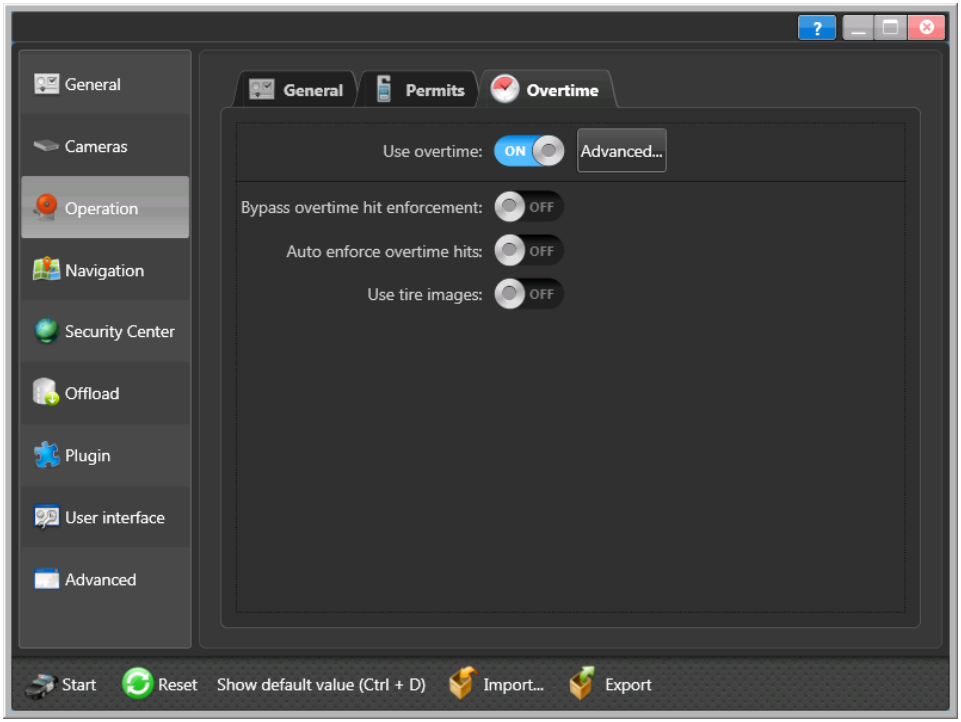
Configure Patroller overtime settings

To use overtime rules, you need to enable overtime and configure the overtime settings in Patroller Config Tool.

1 Open Patroller Config Tool.

2 Go to **Operation> Overtime**.

NOTE The **Overtime** page below is for a City Parking Enforcement system. It includes all the possible overtime configuration options.

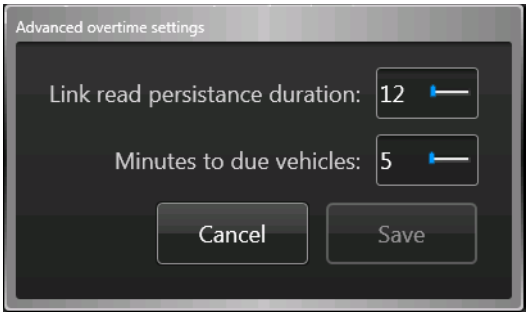


3 (*City Parking Enforcement* and *University Parking Enforcement*) Turn on **Use overtime**, then configure the following:

- *Bypass hit enforcement.* Turn this off if you want Patroller users to indicate whether or not they enforced the hit after accepting it. Turn it on to bypass enforcement. When turned on, Patroller automatically enforces hits after they are accepted.
- *Auto enforce overtime hits.* Turn this on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction. If you've configured a hit accept or hit reject survey, it is ignored when this option is enabled.

4 (*City Parking Enforcement* and *University Parking Enforcement*) Click **Advanced**.

The **Advanced overtime settings** window appears.



From the **Advanced overtime settings** window, configure the following, then click **Save**:

- *Link read persistence duration.* Enter the amount of time that a plate read stored in the Patroller database is considered to be a "time 1" read for a particular overtime rule.

  For example, let's say you enter 8 hours, which is a typical Patroller's shift. You start your shift and select *OT_Rule1*. You do your first pass and read plate *ABC123* at 9:00 A.M. This is now "time 1" for the rest of the day (until 5:01 P.M.). Even if you close and restart Patroller, the "time 1" for plate *ABC123* for *OT_Rule1* will be 9:00 A.M. If you start Patroller after the duration (8 hours in this example), the 9:00 A.M. read is no longer considered to be a "time 1" read.
- *Minutes to due vehicles.* Enter the amount of time before the vehicles are due for enforcement. This value determines the *Show Due* functionality in Patroller. The default value is 5 minutes.

5 (*City Parking Enforcement with Wheel Imaging* only) Turn on **Use tire images**, then go to "Configuring Patroller wheel imaging settings" on page 248.

6 Click **Apply**.

Overtime rules are now enabled and configured in Patroller.

After you are done: If applicable, see "Configuring Patroller wheel imaging settings" on page 248.

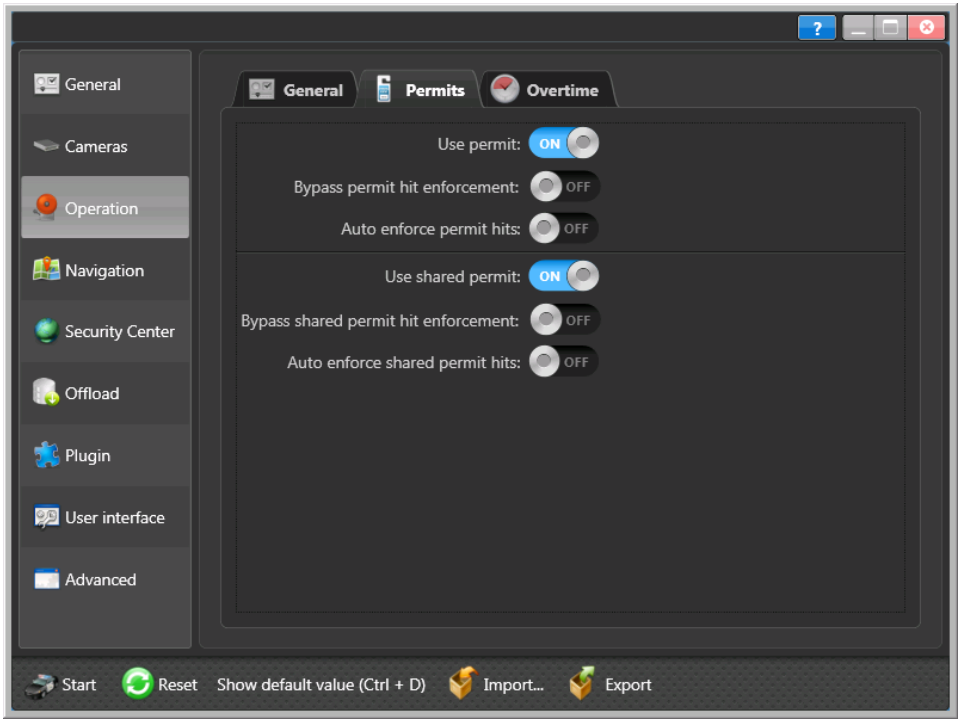
Configure Patroller permit settings

To use permits and shared permits, you need to enable them and configure their settings in Patroller Config Tool.

1 Open Patroller Config Tool.

2 Go to **Operation** > **Permits**.

NOTE The **Permits** page below is for a University Parking Enforcement system. It includes all the possible permit configuration options.



3 (*City Parking Enforcement* and *University Parking Enforcement*) Turn on **Use permit**, then configure the following:

- *Bypass permit hit enforcement.* Turn this off if you want Patroller users to indicate whether or not they enforced the hit after accepting it. Turn it on to bypass enforcement. When turned on, Patroller automatically enforces hits after they are accepted.
- *Auto enforce permit hits.* Turn this on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction. If you've configured a hit accept or hit reject survey, it is ignored when this option is enabled.

4 (*University Parking Enforcement* only) Turn on **Use shared permit** (if you're using them), then configure the following:

- *Bypass shared permit hit enforcement.* Turn this off if you want Patroller users to indicate whether or not they enforced the hit after accepting it. Turn it on to bypass enforcement. When turned on, Patroller automatically enforces hits after they are accepted.
- *Auto enforce shared permit hits.* Turn this on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction. If you've configured a hit accept or hit reject survey, it is ignored when this option is enabled.

5 Click **Apply**.

Permits and shared permits are now enabled and configured in Patroller.

Configuring Patroller wheel imaging settings

If you have a City Parking Enforcement with Wheel Imaging system, you need to configure Patroller to grab wheel images from the installed tire cameras.

Before you begin: Configure the general overtime settings. See "Configure Patroller overtime settings" on page 245.

This section includes the following topics:

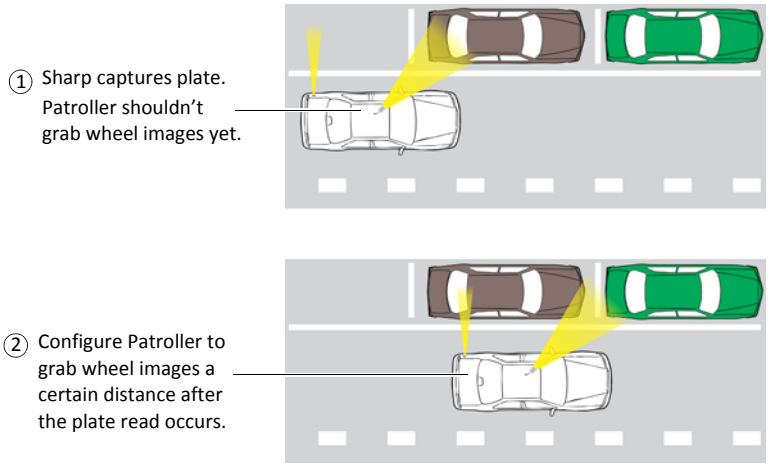
About Patroller wheel imaging settings

In City Parking Enforcement with Wheel Imaging, Patroller uses wheel images taken by "tire cameras" to provide additional evidence of whether or not a parked vehicle has moved.

The tire cameras are always on (when the vehicle is running), but Patroller only needs images of parked vehicles' wheels, not random images from the side of the road. You'll configure Patroller to save (or "grab") only the images it needs from the tire cameras. You need to grab just enough images to prove the offense.

A plate read from the Sharp tells Patroller it should start grabbing tire images. However, since the Sharp and the tire cameras are typically installed on opposite ends of the Patroller vehicle, plate reads occur *before* the parked vehicle's wheels come into view of the tire camera. You need to configure Patroller to account for this delay, so that it doesn't grab useless images.

EXAMPLE In the following diagram, you can see that the vehicle's wheels aren't in the tire camera's field of view when the plate read occurs.



The "when" to grab wheel images is expressed in Patroller by distance rather than time. Since you don't drive at exactly the same speed every time you patrol, a time value (e.g. start grabbing images 1.2 seconds after a plate read) would never be accurate. Instead, you'll specify how *far*, not how *long*, after the plate read Patroller should start grabbing wheel images.

Based on the initial distance, you'll also configure Patroller so that it knows how many images to grab, and when to stop, assuming there isn't another vehicle to initiate a new plate read.

NOTE For 45-degree angled parking, please note the following:

- You'll only be able to capture the rear wheel's tire image. The front wheel will either be out of the tire camera's range, or blocked from view because of the angle of the vehicle.
- Depending on how vehicles are parked, a long vehicle can visibly block the rear wheel of the vehicle behind it.
- If you are *exclusively* doing 45-degree angled parking, you can adjust the angle of the tire camera so that it is facing backwards at about 45 degrees. This way the tire camera will be facing the parked vehicle's wheel when it passes.

  In this case however, the quality and size of the wheel image will be lower because the image is captured from slightly farther away than a parallel parked vehicle.
- If you're doing *both* parallel and 45-degree parking, keep the tire camera at a 90 degree angle, but note that the wheel images for the 45-degree parked vehicles will be skewed because they are captured at an angle.

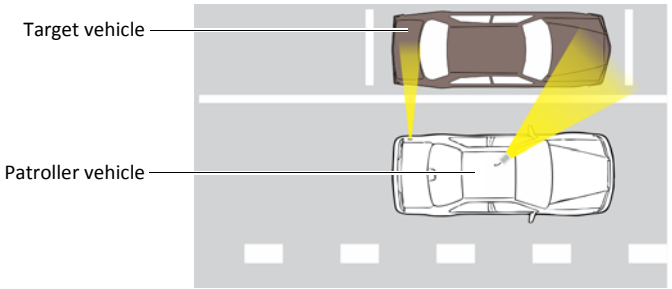
Measure the Tire cam-to-plate distance

This section explains how to measure the distance between the tire camera and the license plate to determine when Patroller should start grabbing wheel images from the tire camera. You need to be in the Patroller vehicle and parked next to a "target" vehicle to perform this procedure.

NOTE This procedure is the same for parallel or 45-degree parking, but the distance is less for 45-degree parking because of the parked vehicle's angle.

Before you begin: Patroller must be installed on the in-vehicle computer, and you must have a tape measure available.

1 Park the Patroller vehicle next to the target vehicle. Keep the engine running.



2 Start Patroller, then tap **Video**.

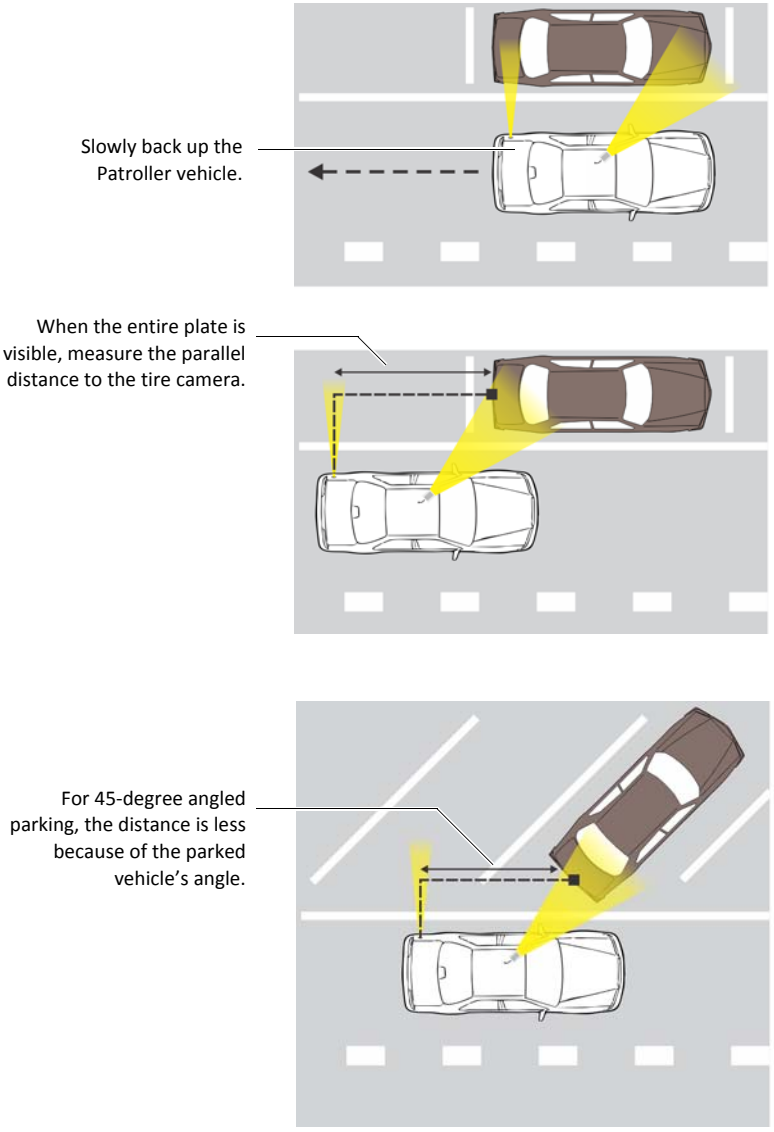
The video window appears showing the available Sharps and tire cameras.

3 Select the Sharp camera (if you have more than one) aimed at the target vehicle, then tap LPR to see the LPR camera's feed.

The LPR camera's video feed appears.

4 Put the Patroller vehicle in reverse, then slowly back up until you see the target vehicle's entire plate in the LPR video feed. Stop the vehicle.

5 Using your tape measure, measure the *parallel* distance (in metres) from the tire camera's field of view to the target vehicle's license plate.



6 Write down the distance you measured.

You'll need to enter the distance in Patroller Config Tool. The distance is used by Patroller to know when to start grabbing tire images after a plate read.

After you are done: See "Configure Patroller wheel imaging settings" on page 252

Configure Patroller wheel imaging settings

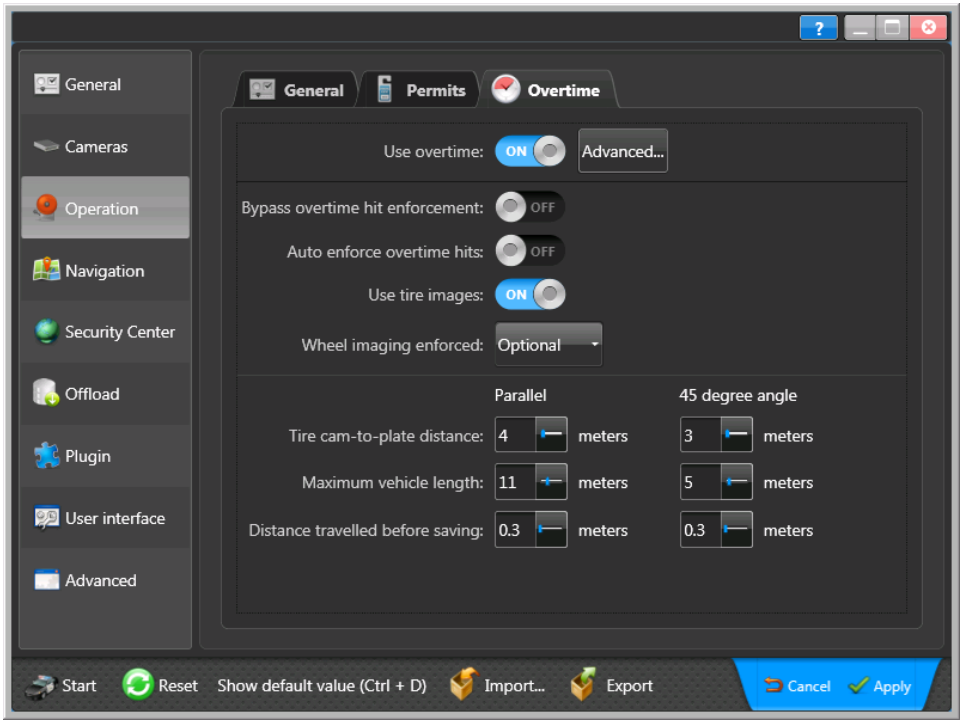
This section describes how to configure Patroller for wheel imaging. You'll enter the required settings for Patroller to know when to grab wheel images from the tire cameras.

Before you begin: You'll need the Tire cam-to-plate distance for this procedure. See "Measure the Tire cam-to-plate distance" on page 250.

1 Open Patroller Config Tool.

2 Go to **Operation**> **Overtime**, turn on **Use overtime**, then turn on **Use tire images**.

The **Overtime** page appears with the wheel imaging settings displayed.



3 Configure the following:

- *Wheel imaging enforced.* Select **Mandatory** or **Optional** from the drop-down list. If you select optional, Patroller users can enforce a hit without confirming wheel images.
- *Tire cam-to-plate distance.* This distance tells Patroller how far to travel (after the initial plate read) before it starts grabbing wheel images. For 45-degree parking, enter a greater distance to account for the tire camera facing backwards at 45 degrees.

  For more information on how to obtain this value, see "Measure the Tire cam-to-plate distance" on page 250.

- *Maximum vehicle length.* This distance tells Patroller to stop grabbing wheel images when, after capturing a license plate read, it travels *Maximum Vehicle Length* without capturing a new license plate read. For 45-degree parking, enter a smaller distance because the angle of the parked vehicle makes it appear smaller to the tire camera.

  TIP The distance you enter should be based on the general size of the vehicles in your patrol area. For example, vehicles in Europe tend to be smaller than in the United States.

- *Distance travelled before saving.* When grabbing wheel images, this distance tells Patroller how often to grab an image. For example, the default 0.3 meters means that an image is grabbed every 30 centimeters.

  NOTE You should not need to change the default value of 0.3 meters. It should be adequate for any parking enforcement scenario.

4 Click **Apply**.

Patroller is configured for wheel imaging.

EXAMPLE Here is an example of how all these settings work together:

1 The Sharp reads a parked vehicle's plate.
2 After the Patroller vehicle travels 4 meters (if **Tire cam-to-plate distance** = 4), Patroller starts grabbing wheel images from the tire camera.
3 Patroller grabs an image every 0.3 meters (if **Distance travelled before saving** = 0.3).
4 Unless the Sharp reads a new plate, Patroller keeps grabbing images until it travels 11 meters (if **Maximum vehicle length** = 11) past the initial read.

After you are done: You'll most likely need to perform some trial and error testing before fully deploying your AutoVu system in the field. As a result, you may need to adjust these settings.

Configure Navigator box settings

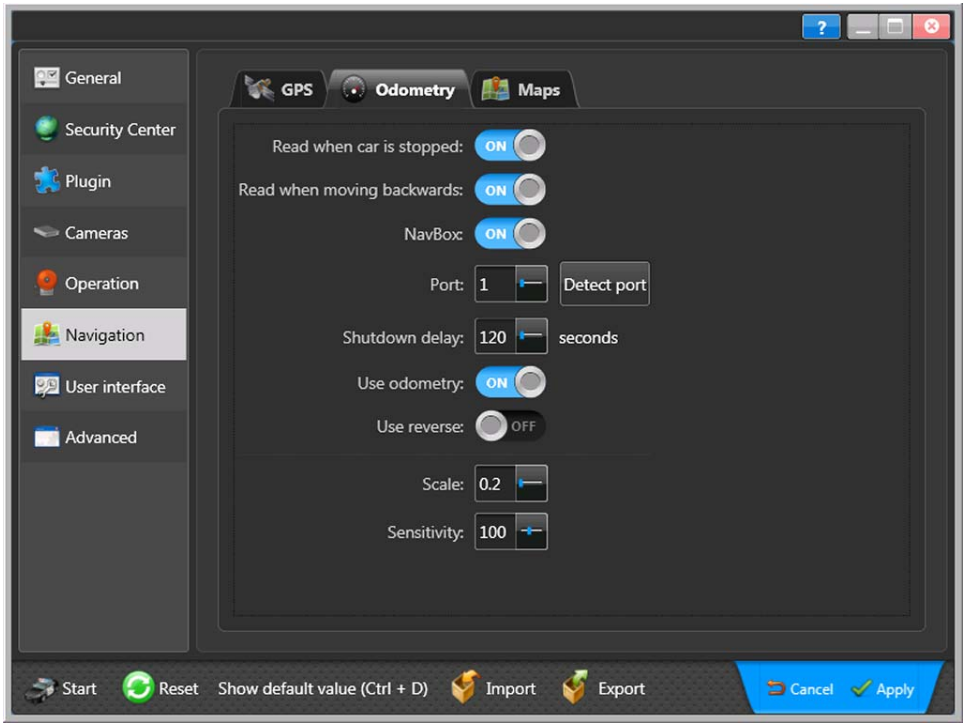
If you use City Parking Enforcement with Wheel Imaging, you need to enable the Navigator box and enter its COM port, as well as configure the odometry-related settings you obtained by calibrating the Navigator box.

Before you begin: See "Calibrating the Navigator box for wheel imaging" on page 225.

1 Open Patroller Config Tool.

2 Go to **Navigation** > **Odometry**.

The **Odometry** page appears.



3 Configure the following:

- *Read when car is stopped.* Specify whether or not to continue reading plates when the Patroller vehicle is stopped. In parking enforcement, Patroller vehicles may stop and reverse frequently.
- *Read when moving backwards.* Specify whether or not to continue reading plates when the Patroller vehicle is in reverse. In parking enforcement, Patroller vehicles may stop and reverse frequently.

4 Turn on **NavBox**, then configure the basic settings:

- *Port.* Specify the COM port number of the Navigator box device as seen in Windows Device Manager. The name of the device in Device Manager is *Silicon Labs CP210x USB to UART Bridge*. Click **Detect port** to confirm the port number.
- *Shutdown delay.* Specify the number of seconds to wait after the vehicle's ignition is turned off before shutting down the in-vehicle computer. To disable this feature, enter "0".

5 Turn on **Use odometry**, then configure the odometry-related settings:

- *Use reverse.* Turn this setting on to reverse the odometry polarity to negative. When calibrating the Navigator box, you may encounter negative signal ticks from the vehicle's

engine. This depends entirely on the make and model of the vehicle. If you see negative ticks while calibrating the Navigator box, use this option to reverse the polarity, which will display the ticks as positive.

- *Scale*. This value is provided by the IO Services software during Navigator box calibration. This number is equivalent to the meters travelled per tick, a tick being one complete revolution of the vehicle's wheel.
- *Sensitivity*. This value is provided by the Navigator oscilloscope software during Navigator box calibration. This number adjusts the sensitivity of the Navigator box so it doesn't mistake random engine noise for a tick, a tick being one complete revolution of the vehicle's wheel.

6 Click **Apply**.

The Navigator box and Patroller odometry settings are configured.

After you are done: You need to configure the settings for the GPS antenna connected to the Navigator box. See "Configure GPS settings" on page 190.

17

Additional configuration for Mobile License Plate Inventory (MLPI) systems

This section includes the additional configuration tasks that apply to AutoVu Mobile License Plate Inventory systems.

This section includes the following topics:

Configuring parking facilities in Security Center

This section explains how to create and configure a parking facility for a AutoVu Mobile License Plate Inventory system. You'll learn how to define a parking facility by creating sectors and rows for the purpose of tracking the location of vehicles.

This section includes the following topics:

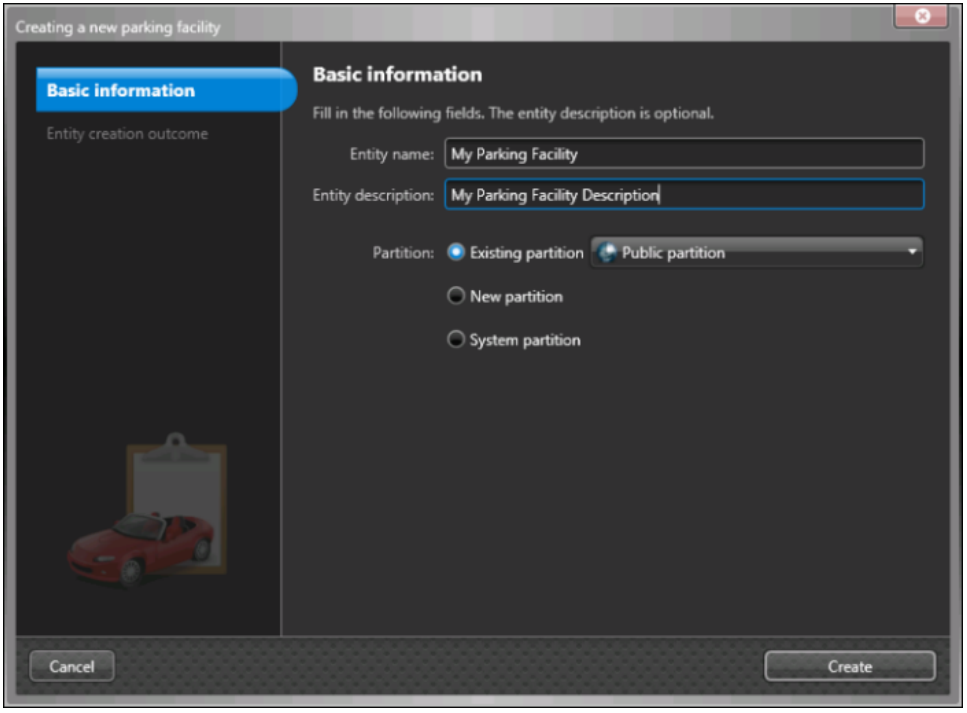
Create a parking facility

You create a parking facility entity in Security Center Config Tool. After you create the entity, you'll configure its settings for your parking scenario.

1 Log on to Security Center Config Tool.

2 From the Security Center Config Tool Home page, click **LPR** > **Parking facilities**, then click the Create (+) button that appears.

The entity creation wizard appears.



3 Enter the required information:

- *Entity name.* In Mobile License Plate Inventory, this name will appear in Patroller on the parking zone selection page.
- *Entity description.* You can add a longer description for the parking facility. This field does not appear in Patroller.
- *Partition.* The public partition is selected by default. For more information on creating and managing partitions, see the *Security Center Administrator Guide*.

4 Click **Create**.

The parking facility appears in a flat list view that displays all the facilities on your system.

After you are done: See "Configure a parking facility" on page 258.

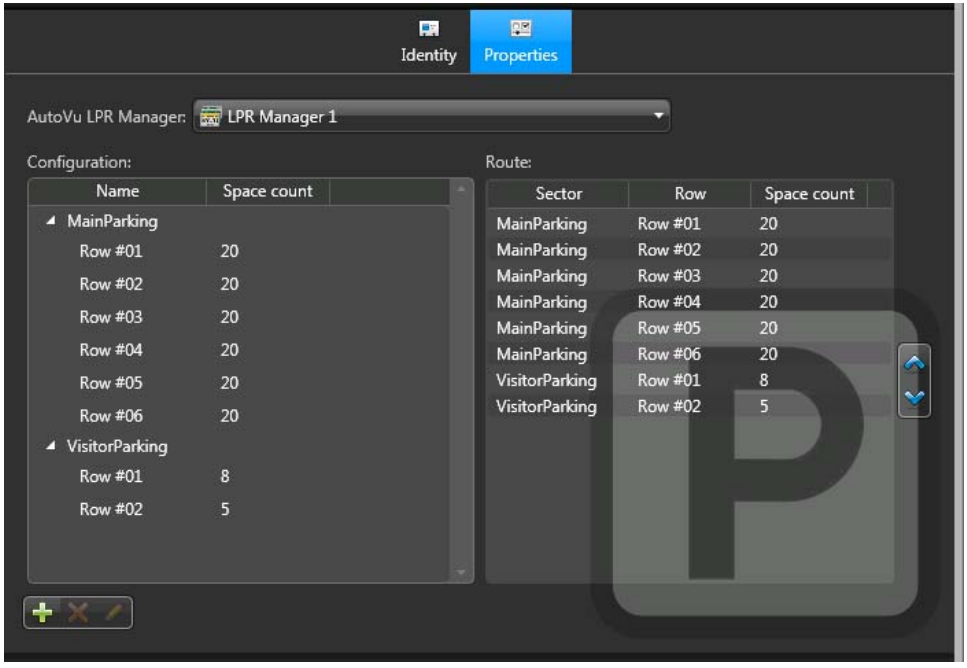
Configure a parking facility

After you have created a parking facility entity in Security Center Config Tool, you need to configure its sectors and rows for the license plate collection route.

Before you begin: See "Create a parking facility" on page 257.

1 Log on to Security Center Config Tool.
2 From the Security Center Config Tool Home page, click **LPR** > **Parking facilities**.
3 Select the facility you want to configure, then click **Properties**.

The **Properties** page appears.



4 From the **AutoVu LPR Manager** drop-down list, select the LPR Manager that will create and manage the license plate inventory for the selected parking facility.

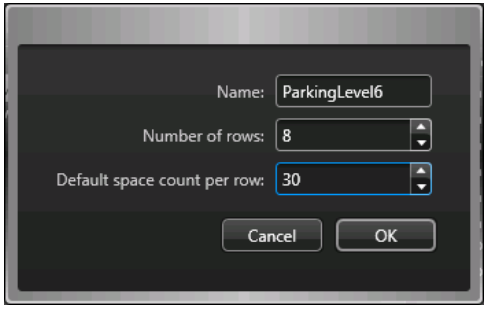
Only offloads from MLPI Patrollers managed by the same LPR Manager are used to build the inventory for this parking facility. An MLPI Patroller offload can include the vehicle inventory for multiple parking facilities, but only the reads tagged for this parking facility are used to build the inventory.

IMPORTANT Make sure to set the *Read retention period* of the LPR Manager long enough for the period of time you want to keep your inventories. The default retention period is 90 days. For more information on the LPR Manager database retention periods, see "General settings" on page 286.

5 Under **Configuration**, click the Create (+) button to add a new sector.

The parking space of a parking facility is divided into sectors (or levels in the case of a parking garage) for ease of reference. Each sector contains *x* number of rows.

The section creation dialog box appears.

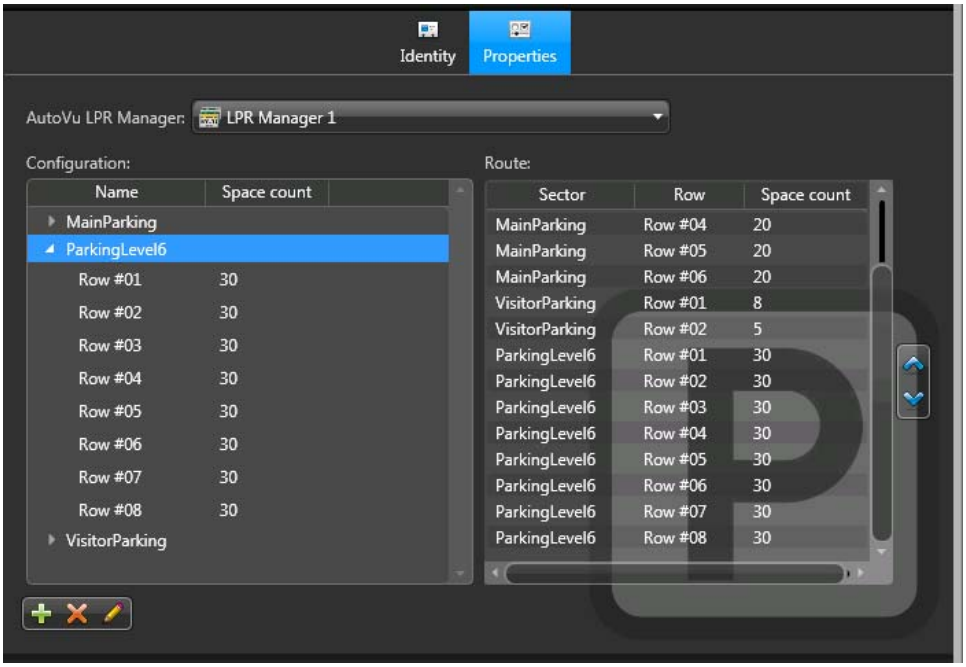


6 Enter the **Name** of the sector (or level if you have a parking garage).

7 Enter the **Number of rows** in the sector.

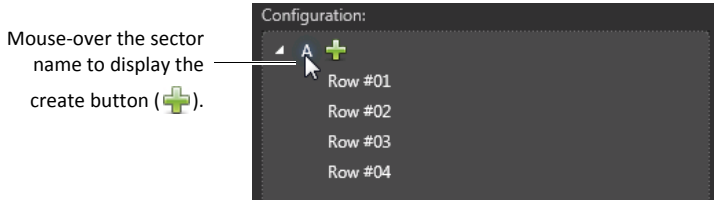
8 Click **OK**.

The sector you created appears under the **Configuration** and **Route** sections.



9 (Optional) Add rows to a sector:

a Under **Configuration**, mouse-over the sector name, then click the Create (+) button that appears.

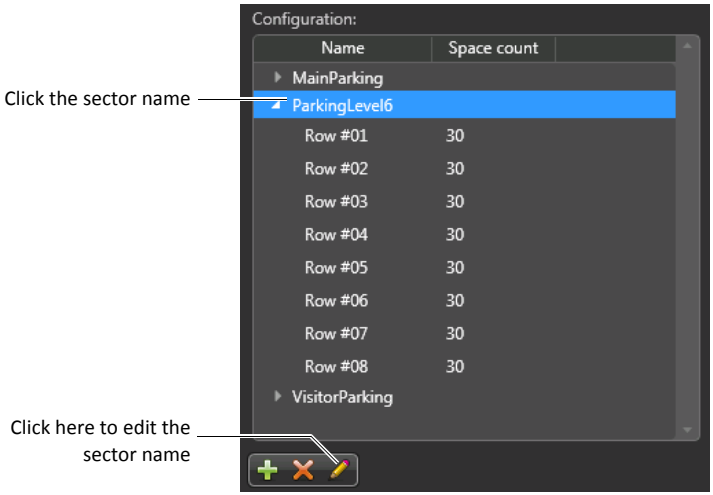


b Enter the **Number of rows** to add, then click **OK**.

c Click **Apply**.

10 (Optional) Rename a sector:

a Under **Configuration**, select the sector name you want to rename, then click the Edit ( ) button.

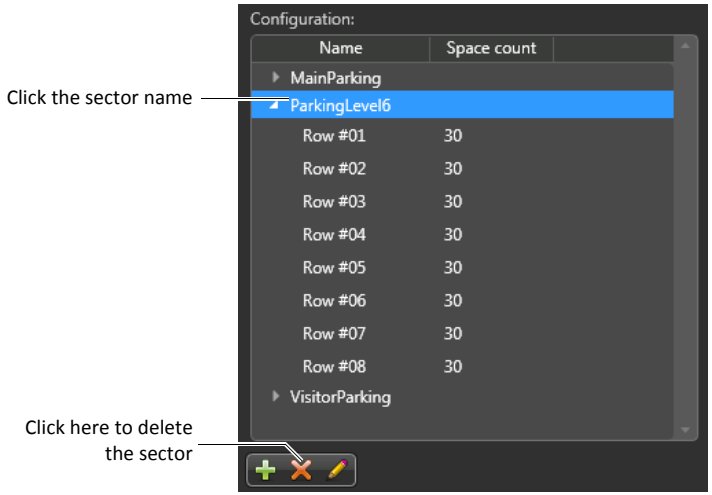


b Enter the new name, and click **OK**.

c Click **Apply**.

11 (Optional) Delete a sector:

a Under **Configuration**, select the sector name you want to delete, then click the Delete ( ) button.



b Click **Apply**.

12 (Optional) Under **Route**, click the up ( )and down ( ) arrows to change the order of sectors and rows in the route.

This is the plate collection route to be followed by the MLPI units responsible for collecting the license plates for the inventory. The route is downloaded by the Patrollers and handheld devices assigned to this parking facility.

NOTE Only one route may be defined per parking facility, but each MLPI device can start its sweeping round at a different point in the route. The route forms a closed circuit.

After you are done: In Patroller Config Tool, turn on the setting Read when car is stopped. Since you do not use a GPS or Navigator box in an MLPI deployment, Patroller cannot detect vehicle movement. By turning this setting on, Patroller will always read plates.

About the Genetec approved handheld computer

This section includes the following topics:

What is the Genetec approved handheld computer

The Genetec approved handheld computer is a rugged device with an integrated camera that lets you manually collect license plate information and export it to Security Center.

Compatibility

The handheld computer is supported in Security Center version 4.0 and later.

Requirements

To perform the procedures in this document, you'll need the following:

- Handheld computer with eyeWARE installed.
- Genetec Security Center 4.0 or later with an AutoVu license that includes the *xml Import* module.
- Xml Import module options set to use the *ReadTemplate.xml* file.

  ReadTemplate.xml is used to import reads from the handheld computer into Security Center. For more information on configuring the xml Import module, see "XML import" on page 295.
- Parking facility entity configured in Security Center.

  The Parking facility entity represents the parking facility you wish to create an inventory for. Before AutoVu MLPI Patrollers can collect license plate reads for a parking facility inventory, the Parking facility entity needs to be configured into sectors and rows using Security Center Config Tool. For more information, see "Configuring parking facilities in Security Center" on page 257.
- The MLPI application folder needs to be copied to the handheld computer. For more information, see "Copy the MLPI application folder to the handheld computer" on page 264.
- The zones.xml file from the AutoVu root folder needs to be copied to the MLPI application folder. See "Copy the zones.xml folder" on page 265.

Copy the MLPI application folder to the handheld computer

This section includes the following topics:

About the MLPI application folder

There are two versions of the AutoVu MPLI application folder: *MLPISmartDevice12* and *MLPISmartDevice20*. The folder you copy to the Genetec approved handheld computer depends on which SDK the handheld uses.

For example, if the handheld uses SDK version 1.2, you must copy the *MLPISmartDevice12* folder. If the handheld uses SDK version 2.0, then you must copy the *MLPISmartDevice20* folder.

The *MLPISmartDevice12* and *MLPISmartDevice20* folders are located in the *Tools* folder on your installation CD: \Patroller_vxxx_Full\Tools.

The application folder includes the following files:

- *ApplicationConfiguration.xml*. Application settings.
- *genetec.c2t*. Custom eyeWARE configuration file.
- *Genetec.LicensePlateManagement.MLPI.SmartDevice.exe*. The application file.
- *ReadTemplate.xml*. Template used to export MLPI reads from handheld units and import them into Security Center.
- *twotecheyewarelibraryce.dll*. Reference library.
- *twotechlibraryce.dll*. Reference library.

Copy the MLPI application folder

To copy the MLPI application folder:

1. Navigate to the *SystemCF* folder on the handheld computer (*Computer\Hydrus Luna\SystemCF*).
2. Create a new folder with a meaningful name, such as: MLPI.
3. Copy the application folder (MLPISmartDevice12 or MLPISmartDevice20) from your Security Center server to the folder you created on the handheld computer in Step 2.

   NOTE You can also copy the application folder to a mini USB drive that is compatible with the handheld computer and run the application from there.
4. (Optional) Modify the value of the DefaultPlateState. This value of the plate state that appears in the application when the user enters the plate information.

Open the ApplicationConfiguration.xml file in a text editor, and modify the value of the DefaultPlateState (default is QC).

```
<ApplicationConfiguration>
  <DefaultPlateState>QC</DefaultPlateState>
</ApplicationConfiguration>
```

Copy the zones.xml folder

You need to copy your latest <GUID>_zones.xml file from your AutoVu Root folder to the file system folder of the Genetec approved handheld computer (*Computer\Hydrus Luna\SystemCF*). <GUID> is a globally unique identifier of the zone file (for example, dd9f4ea7-2aed-44c0-a0a9-cb01282b9a53_zones.xml).

NOTE The <GUID>_zones.xml file is located in the Root folder that is set in Security Center Config Tool. For more information about configuring the Root folder settings, see "Configure LPR Manager root folder" on page 119.

Part VI

Interface references

This part describes the buttons and options in the three applications you use to configure an AutoVu system: Security Center Config Tool, Patroller Config Tool, and the Sharp Portal.

This part includes the following chapters:

18

Security Center Config Tool reference

This section describes the main Security Center Config Tool components used to configure an AutoVu fixed or mobile system. It describes the LPR-related entity types, the LPR Manager role, and the LPR administration task.

NOTE This reference is an abridged version of the main Security Center reference section found in the *Security Center Administrator Guide*.

This section includes the following topics:

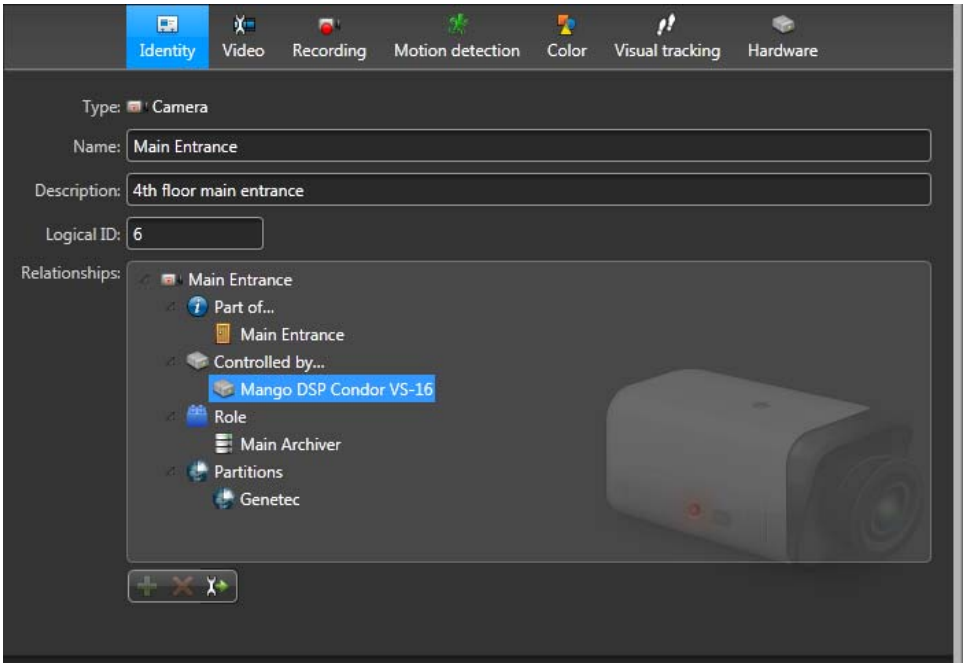
Common configuration tabs

Some of the configuration tabs are commonly used by the majority of Security Center entities. The following tabs are covered in this section:

Identity	Name, description, logical ID, and relationships of the selected entity with other entities in the system.
Cameras	Cameras associated to the selected entity.
Custom fields	Custom fields for the selected entity.
Location	Time zone and geographical location for the selected entity.

Identity

The *Identity* tab provides descriptive information on the entity and lets you jump to the configuration page of related entities. The sample screen shot below is that of a camera entity.



Standard information

All entity types share the following standard attributes:

- **Type.** Entity type.
- **Name.** Entity's given name. The entity name is editable, except in the following cases:
  - *Server entities.* The entity name corresponds to the machine name and cannot be changed.
  - *Federated entities.* The entity name belongs to the original system and cannot be changed on the federation.
- **Description.** Optional descriptive text.
- **Logical ID.** Logical IDs are unique numbers assigned to entities for ease of reference in the system (mainly for CCTV keyboard operations).

  NOTE A logical ID must be unique across all entities of the same group. Entity types that are likely to be referenced within the same context are put in the same group. For example, cameras and public tasks belong to the same functional group, therefore, a camera and a public task may not have the same logical ID, but a camera and a camera sequence may.

  TIP You can view and edit the logical IDs of all entities in the system from one place. For more information, see System – General settings – "Logical ID" in the *Security Center Administrator Guide*.

- **Relationships.** List of relationships between this entity and other entities on the system.

  You can use the command buttons found at the bottom of the relationship list to manage the relationships of this entity with other entities in the system.

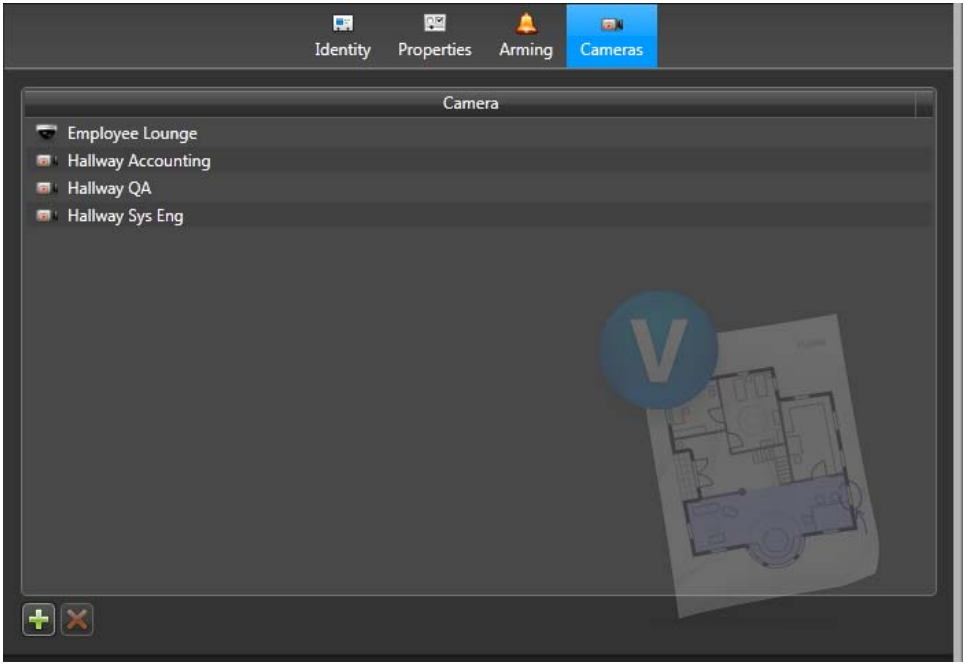
  - Select a relationship group, and click  to add a new relationship.
  - Select a related entity, and click  to remove the relationship.
  - Select a related entity, and click  to jump to its configuration page.

Specific information

Certain entity types may show additional information in this tab. For example, see Video unit – "Identity" in the *Security Center Administrator Guide*.

Cameras

The *Cameras* tab allows you to associate cameras to the entity so that when it is viewed in Security Desk, the cameras are displayed instead of the entity icon. The sample screen shot below is that of a virtual zone entity.

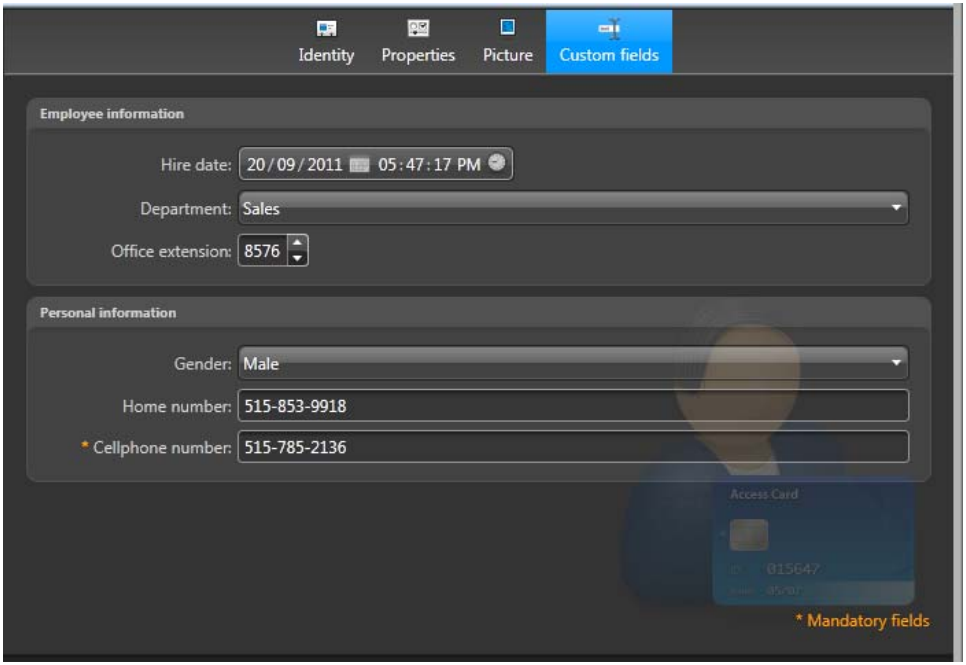


From this tab you can perform the following actions:

- To add a camera, click .
- To remove the selected camera, click .

Custom fields

The *Custom fields* tab lets you view and modify the custom fields defined for this entity. The sample screen shot below is that of a cardholder entity.



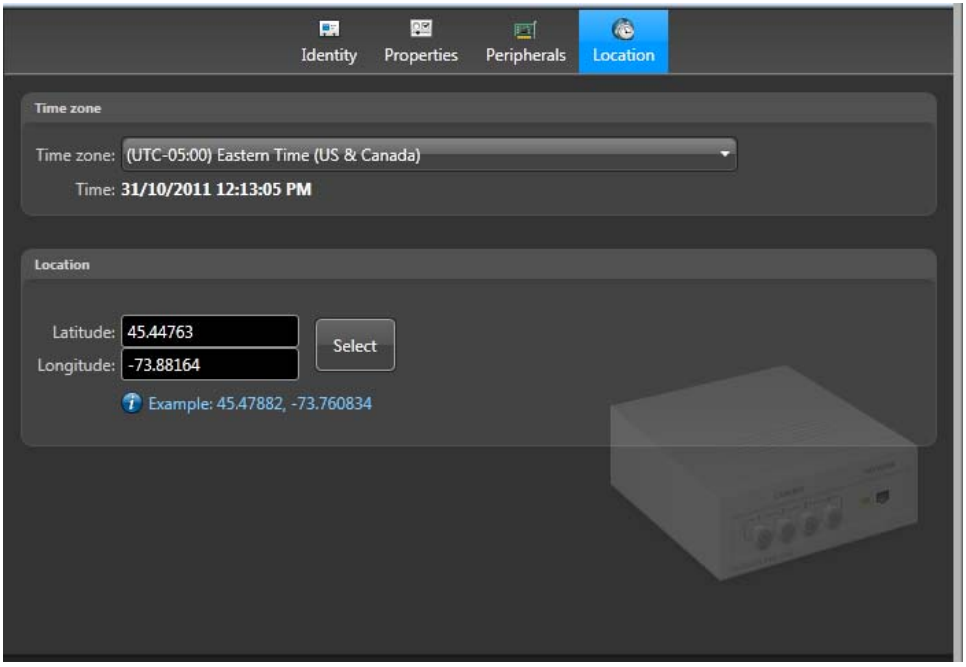
In the above example, five custom fields have been defined for the cardholder entity, separated in two groups:

- Employee information
  - Hire date
  - Department
  - Office extension
- Personal information
  - Gender
  - Home number
  - Cellphone number (flagged as mandatory)

For information on defining custom fields, see System– General settings – “Custom fields” in the *Security Center Administrator Guide*.

Location

The *Location* tab provides information regarding the time zone and the geographical location of the entity. The sample screen shot below is that of a video unit entity.



Time zone

The time zone is used to display the entity events in the entity's local time zone. In Security Center, all times are stored in UTC in the databases, but are displayed according to the local time zone of the entities. The local time of the entity is displayed below the time zone selection.

Location

The geographical location (latitude, longitude) of the entity has several different uses:

- For video units, it is used for the automatic calculation of the time the sun rises and sets on a given date. A typical application is for the system to record video only during daytime (for cameras placed outside), or to adjust the brightness of the camera based on daytime and nighttime. For more information, see "Schedule" in the *Security Center Administrator Guide*.
- For fixed LPR units that are not equipped with a GPS receiver, the geographical location is used to plot the LPR events (reads and hits) associated to the LPR unit on the map in Security Desk. For more information, see Hits and Reads investigation tasks in the *Genetec Security Desk User Guide*.

LPR

The *LPR* task allows you to configure the general settings for LPR (license plate recognition) and the related entities such as LPR Manager roles, LPR units, hotlists, permits, overtime rules, and so on, that are not found in the *Logical view*.

System: AutoVu IP license plate recognition

License option: AutoVu

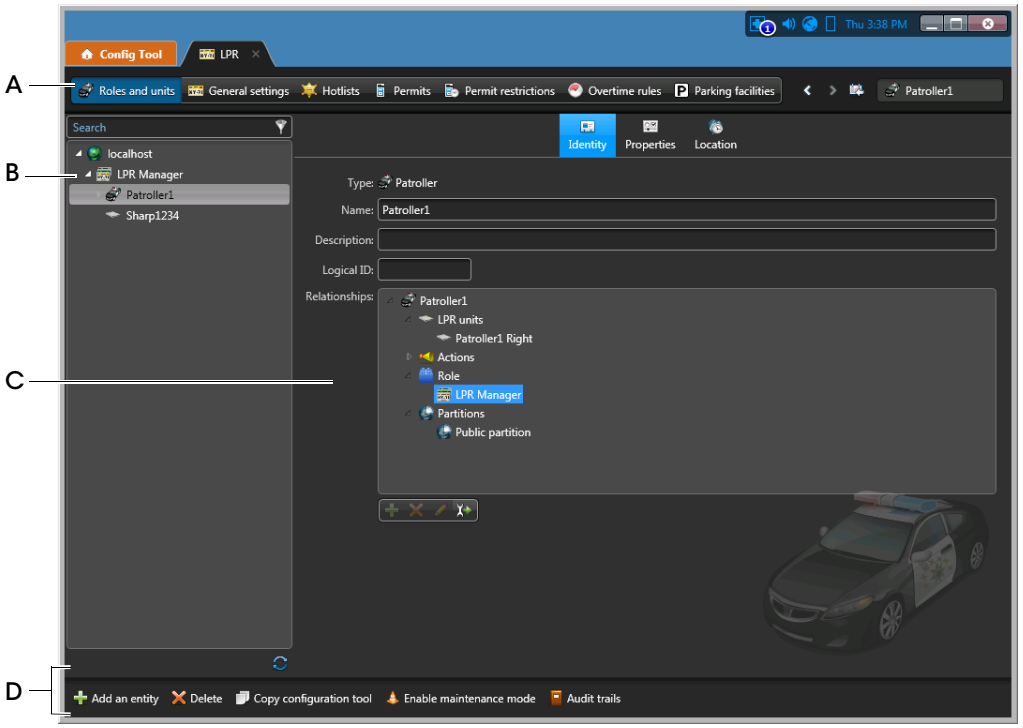
Category: Administration

The *LPR* task includes the following views:

	Roles and units	Shows the LPR Manager roles and the LPR and Patroller units they control as a hierarchy. For more information, see: • "LPR Manager" on page 284. • "LPR unit" on page 327. • "Patroller" on page 330.
	Hotlists	Lists all hotlists in alphabetical order. For more information, see "Hotlist" on page 304.
	Overtime rules	Lists all overtime rules in alphabetical order. For more information, see "Overtime rule" on page 319.
	Parking facilities	Lists all parking facilities in alphabetical order. For more information, see "Parking facility" on page 324.
	Permit restrictions	Lists all permit restrictions alphabetical order. For more information, see "Permit restriction" on page 315.
	Permits	Lists all permits in alphabetical order. For more information, see "Permit" on page 311.
	General settings	Lets your configure the general settings pertaining to license plate recognition and the generation of LPR hits.

Roles and units

The *LPR – Roles and units* view shows the LPR Manager roles and the units they control in a hierarchy.



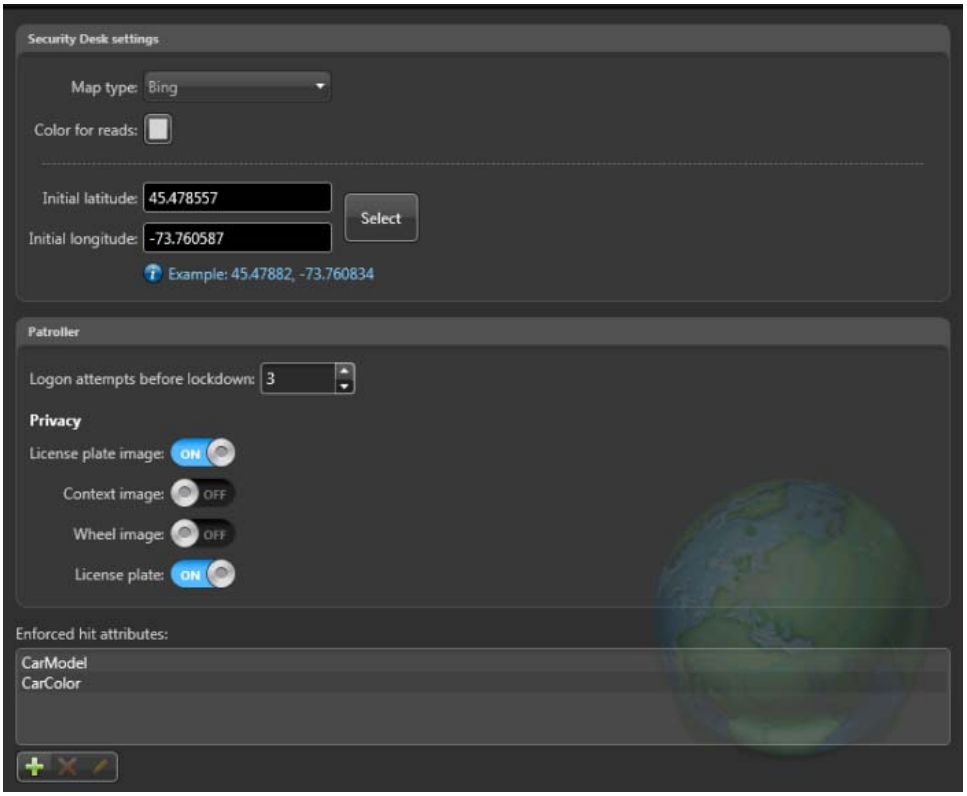
A	Selected view (*Roles and units*).
B	Select an entity to configure.
C	Configuration pane of the selected entity.
D	See “Contextual command toolbar” in the *Security Center Administrator Guide*.

General settings

The *General settings* view includes the following settings pages:

Applications

The *Applications* tab lets you configure how Security Desk displays maps in the Monitoring and Route playback tasks. You can also limit the number of logon attempts in Patroller, enforce Patroller privacy settings, and set the attributes a Patroller user must enter when enforcing a hit.

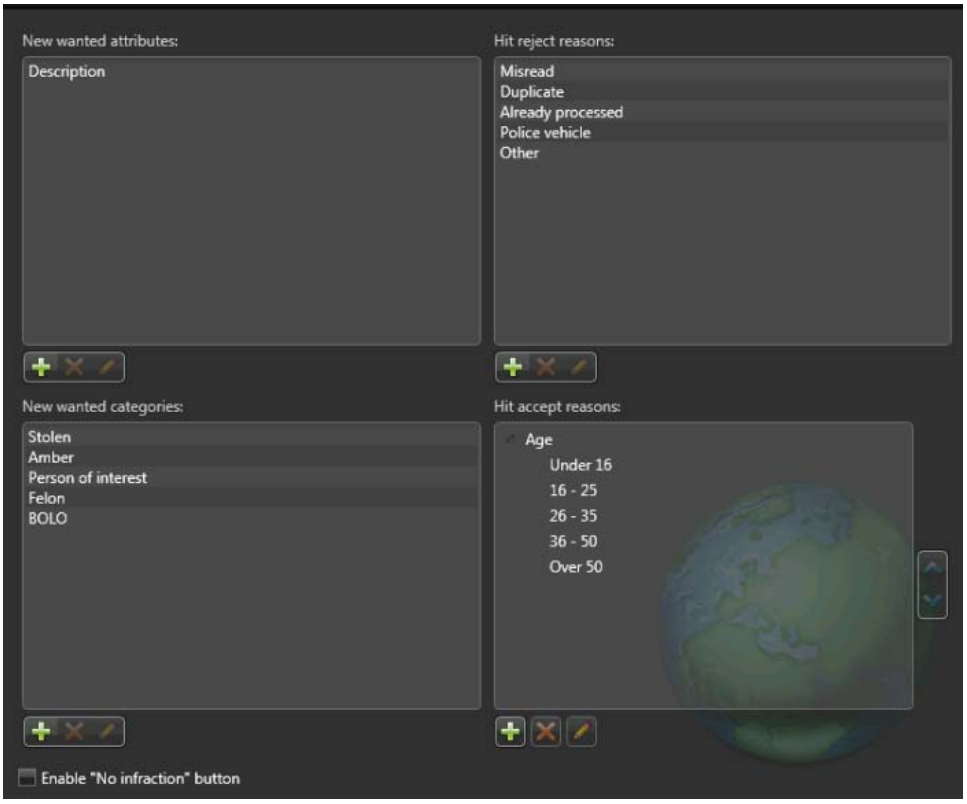


- **Map type.** Display-only field showing the type of map system supported by your Security Center license. The choices are Bing, MapInfo, and None.
- **Color for reads.** Click to select the color used to show license plate reads on maps.
- **Initial longitude/latitude.** Set the default starting location for map view in Security Desk. You can type the coordinates in the fields or click Select and zoom in on a location and click Select. A red pushpin appears to indicate the selected position.
- **Logon attempts before lockdown.** You can specify the number of unsuccessful logon attempts a Patroller can make before the account is locked out. For example, if the limit is set to 3, Patroller users have three attempts to log on to Patroller with their username and password. On the fourth attempt, their accounts will be locked and they won't be able to logon. Users with locked accounts must contact their administrators in order to have the password reset. Patroller must be connected to the Security Center server for the password to be reset.
- **Privacy.** You can configure Patroller to obscure plate numbers, or exclude plate, context, or wheel images from reads and hits so that the information is not stored in the LPR Manager database. These settings allow you to comply with privacy laws in your region:
  - *License plate, context, or wheel images.* When switched to **On**, images are not sent to Security Center or included in offloaded data.
  - *License plate.* When switched to **On**, the plate number text string is replaced by asterisks (*) when sent to Security Center or in the offloaded data.

  At the hotlist level, you have the option of overriding these privacy settings for the purpose of sending an email with real data to a specific recipient (see "Advanced" on page 308).
- **Enforced hit attributes.** Create text entry fields that Patroller users must enter text in when they enforce a hit. The information from the enforced hit text fields can be queried in the Security Desk hits report.

Hotlist

The *Hotlist* tab allows you to define the customized attributes, reasons, and categories that will appear in Patroller when the user adds a New wanted entry, or rejects or accepts a hit. The settings are downloaded to Patroller along with the selected hotlists when Patroller connects to Security Center. These settings are also available as filter options for hit reports in Security Desk.



- **New wanted attributes.** A new wanted is a hotlist item that is manually entered by the Patroller user. The new wanted attributes are attributes other than the standard ones (plate number, plate issuing state, category) that the Patroller user is asked to specify when entering a new wanted item in the Patroller. One category is pre-configured for you when you install Security Center.

  For more information, see "Configuring New wanted attributes and categories" on page 207.

- **New wanted categories.** List of hotlist categories that a Patroller user can pick from when entering a new wanted item. The category is the attribute that says why a license plate number is wanted in a hotlist. Several categories are pre-configured for you when you install Security Center.

  For more information, see "Configuring New wanted attributes and categories" on page 207.

NOTE BOLO is an acronym for "be on the lookout", sometimes referred to as an all-points bulletin (APB).

- **Hit reject reasons.** List of reasons for rejecting hotlist hits. These values also become available as Reject reason filter options for generating hit reports in Security Desk. Several categories are pre-configured for you when you install Security Center.

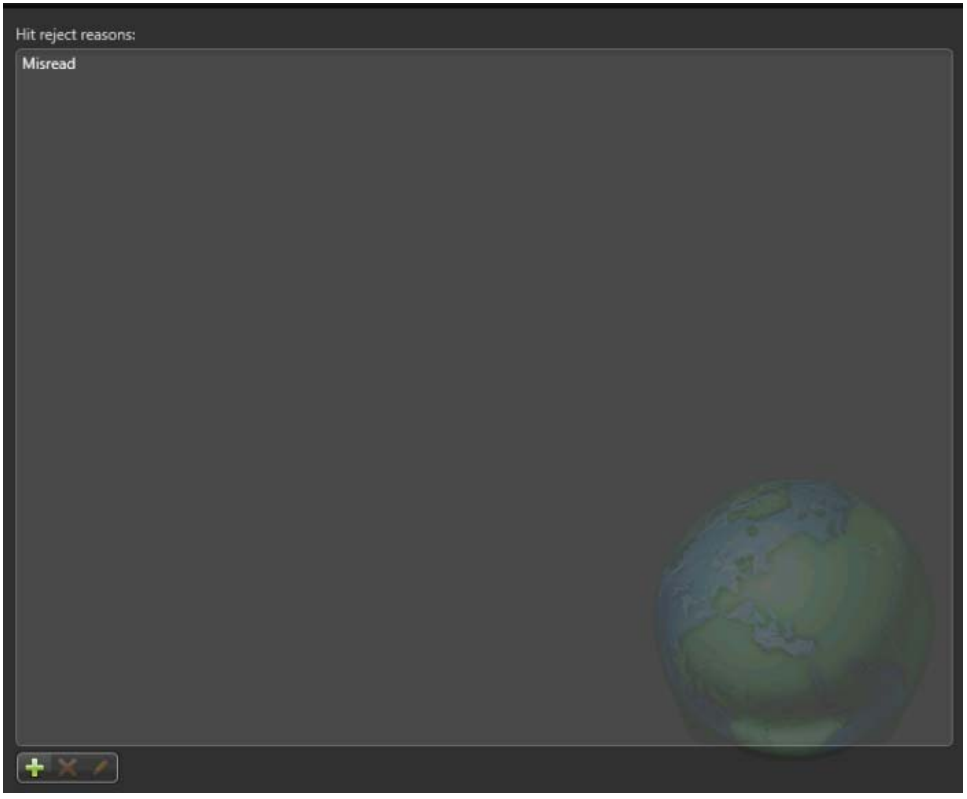
  For more information, see "Configure hit accept and hit reject reasons" on page 206.
- **Hit accept reasons.** Create a survey that contains information Patroller users must provide when they accept a hit. The information from the hit survey can be queried in the Security Desk Hit report. There are no pre-configured categories for this option. The category you see above is an example only.

  For more information, see "Configure hit accept and hit reject reasons" on page 206.
- **Enable "No infraction" button.** Select this option to enable the **No infraction** button in the Patroller hit survey. This button allows the Patroller user to skip the hit survey after enforcing a hit.

Overtime rule

The *Overtime rule* tab allows you to define the custom reject reasons for overtime hits. The values defined here are downloaded to Patrollers and are available as Reject reason filter options for generating hit reports in Security Desk.

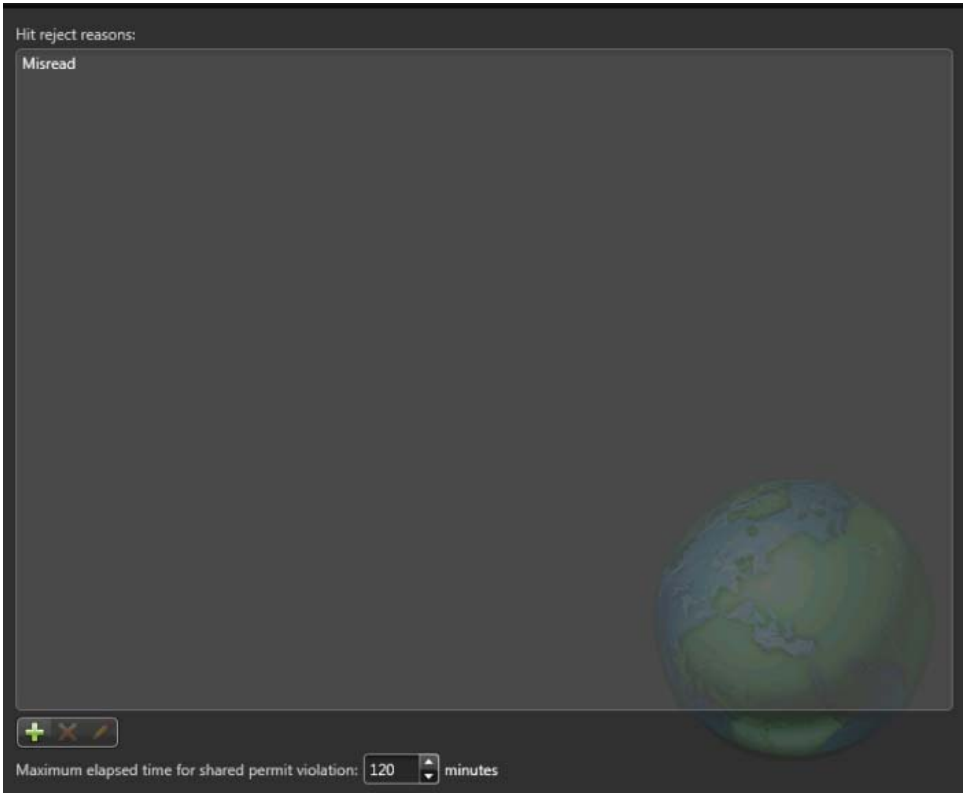
One category is pre-configured for you when you install Security Center.



Permit

The *Permit* tab allows you to define the custom reject reasons for permit hits, and to select the minimum elapsed time for shared permit violations (University Parking Enforcement only). The values defined here are downloaded to Patrollers and are available as Reject reason filter options for generating hit reports in Security Desk.

One category is pre-configured for you when you install Security Center.



- **Hit reject reasons.** List of reasons for rejecting permit hits or shared permit hits. These values also become available as Reject reason filter options for generating hits reports in Security Desk.
- **Maximum elapsed time for shared permit violation.** This parameter defines the time period used by University Parking Enforcement Patrollers to generate shared permit hits. A shared permit hit is generated when two vehicles sharing the same permit ID are parked in the same parking zone within the specified time period.

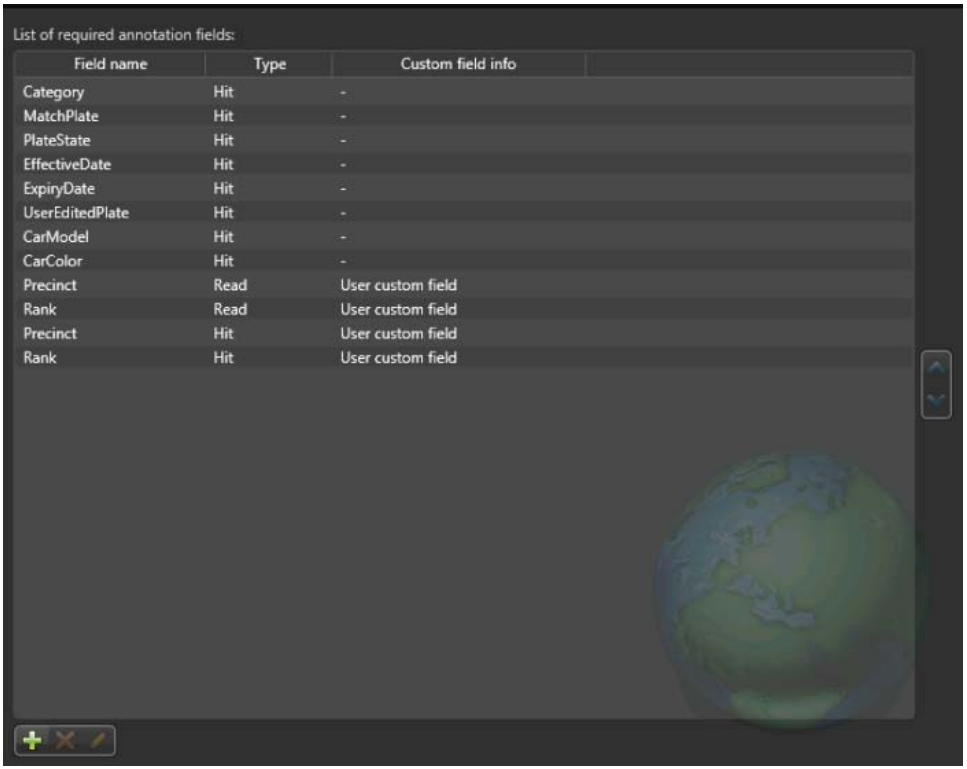
  For example, let's say you're using the default 120 minutes (two hours), and license plates ABC123 and XYZ456 are sharing the same parking permit. If Patroller reads plate ABC123

at 9:00 A.M., and then reads plate XYZ456 at 11:01 A.M., Patroller does **not** raise a hit because the time exceeds the 120 minutes.

Annotation fields

The *Annotation fields* tab allows you to define additional selectors to appear in Security Desk *Reads* or *Hits* report. To be valid, the selector must relate exactly to the information contained in the actual read or hit.

EXAMPLE If you configure *CarModel* and *CarColor* as an Enforced hit attribute (see "Applications" on page 275), the Patroller user will be asked to enter the car's model and color when enforcing a hit, and the information will be stored with the hit. Specifying *CarColor* as an *Annotation* field will allow the values entered by the user to be displayed in a *Hits* report.

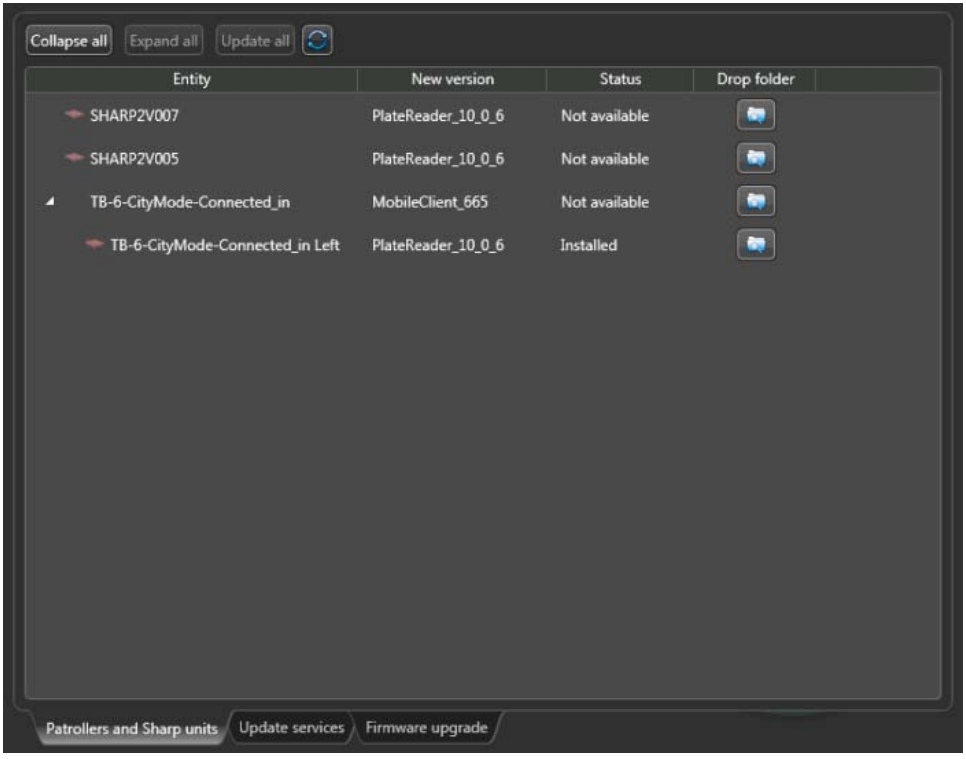


You can also add user custom fields to annotation fields in order to associate a user's metadata with individual reads and hits. This allows you to query and filter for the user custom fields in Security Desk *Reads* and *Hits* reports.

Updates

The *Updates* tab allows you to update Patrollers and Sharp units with hotfixes or new sound files for hit alerts. You can also update services on Sharp units, and upgrade Sharp firmware. Before you can send updates, you need to receive the updates from Genetec and place them in the *Updates* folder under the LPR *Root folder*.

For more information, see "Updating AutoVu with hotfixes or service packs" on page 105.



- **Collapse all.** Collapses all items in the **Entity** field.
- **Expand all.** Expands all items in the **Entity** field.
- **Update all.** Update all units that are controlled by the currently-selected LPR Manager. This button updates only the units on the current tab. For example, if you're on the *Patroller and Sharp units* tab, you'll update all Patrollers and Sharp units on the list.
- **Status.** Shows the status of the update. The possible statuses are:
  - *Not available.* Updater service is not supported (for example, Sharp versions 1.5 and 2.0 with less than 512 MB RAM).
  - *Entitled.* The client machine can receive the update.
  - *Synchronizing.* The client machine has started synchronizing with the server.

  - *Synchronized.* All update files have been successfully downloaded to the client machine. The client machine is waiting for the update to be applied.
  - *Installing.* Client machine has accepted the update, and has started replacing outdated files with new files.
  - *Installed.* The new updates have successfully been applied to the client machine.
  - *Uninstalling.* The update is being removed from the client machine.
  - *Uninstalled.* The update has been successfully removed from the client machine.
  - *Error.* An error occurred in the update process.
- **Drop folder.** Opens the required folder for you to copy the update file. For example, clicking the drop folder icon for a Patroller entity opens *C:\Genetec\AutoVu\RootFolder\Updates\Patroller* (default location).

  NOTE If Security Center is running on a computer that doesn't have access to the server computer, clicking the drop folder opens the *My Documents* folder on the local machine.
- **Patrollers and Sharp units.** Displays the Patrollers and Sharp units (fixed and mobile) that are eligible for an update.
- **Update services.** Displays the Sharp services that are eligible for an update.
- **Firmware upgrade.** Displays the Sharp units that are eligible for a firmware upgrade.

LPR Manager

The *LPR Manager* stores all LPR data (reads, hits, images, vehicle status, GPS data, and so on) collected from the LPR units (fixed Sharps) and Patrollers that it manages into a central database for data mining and reporting. The LPR Manager is also responsible for updating fixed Sharps and Patrollers in the field with hotfixes, hotlist updates, and so on.

Multiple instances of this role can be created on the system to provide scalability and partitioning. For example, different fleets of Patrollers can be managed by different LPR Managers, fixed Sharp units can be managed by different LPR Managers, and so on.

System: AutoVu IP license plate recognition

Tasks: LPR – Units, or System – Roles

	Identity	Name, description, logical ID, and relationships of this entity with other entities in the system.
	Properties	General parameters within which this role should operate.
	Resources	Server and database configuration for this role.

Related topics:

- "Hotlist" on page 304
- "LPR unit" on page 327
- "Overtime rule" on page 319
- "Parking facility" on page 324
- "Patroller" on page 330
- "Permit" on page 311
- "Permit restriction" on page 315

Properties

The *Properties* tab is used to configure the general LPR Manager settings and optional AutoVu features. The availability of certain features depends on your Security Center license.

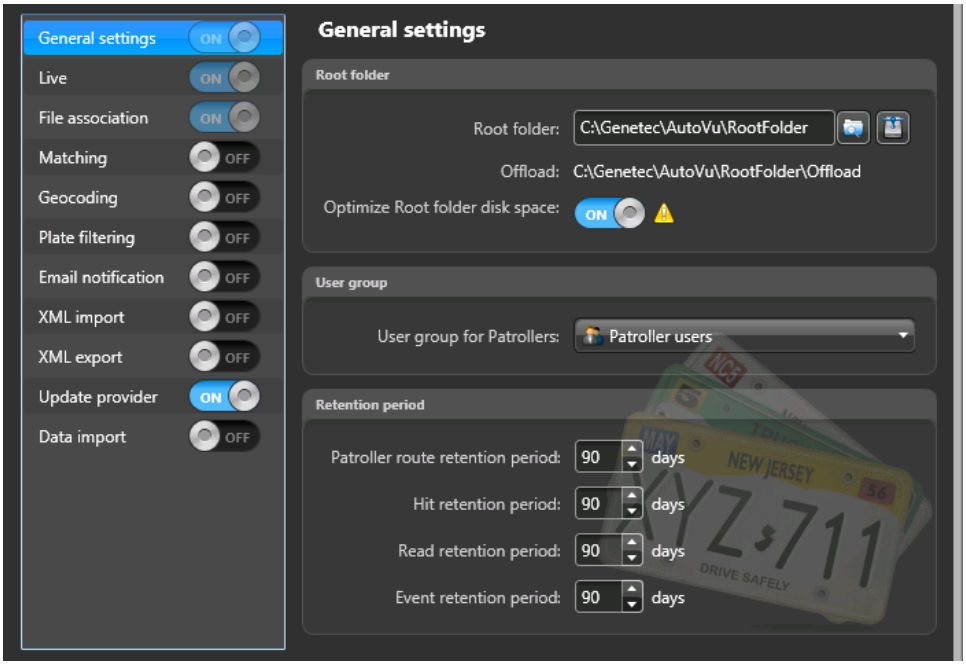
This section includes the following topics:

General settings

Use the *General settings* to configure the *Root folder* for the LPR Manager, the user group for the Patrollers, and how long the data from the LPR Manager is kept in the database.

IMPORTANT Please read the following before you configure the LPR Manager General settings.

- If you are using SQL Server Express Edition, the database might be full before the retention period ends. Contact GTAP to help you evaluate whether SQL Server Express meets the requirements of your AutoVu system.
- If your computer is hosting more than one LPR Manager, each LPR Manager must have a different root folder.



- **Root folder.** The main folder on the computer hosting the LPR Manager. This is where all the configuration files are created, saved, and exchanged between the LPR Manager and the Patroller units it manages.

  Whenever you create a new LPR Manager role, the root folder is created automatically on your computer at the location *C:\Genetec\AutoVu\RootFolder*. If you create multiple LPR Managers, new folders will be created for you at the same location. For example, if you have three LPR Managers created, the folders *RootFolder1*, *RootFolder2*, and *RootFolder3* will be created under the folder *C:\Genetec\AutoVu*.

  The LPR Manager root folder includes the following subfolders:

  - *ManualTransfer*. Contains the configuration and data files to transfer to Patroller manually using a USB key or similar device.

- *Offload.* Contains the LPR data offloaded by Patroller.
- *Rules.* Contains the delta files used by Security Center to transfer hotlist and permit list changes. Do **not** copy or move anything in this folder.
- *Updates.* This folder appears when you first turn on the Update provider (see "Update provider" on page 301). It contains Security Center and Patroller hotfixes, as well as Sharp service and firmware updates. Patroller hotfixes are automatically downloaded to Patroller whenever Patroller is connected to Security Center. Mobile Sharp units are updated through Patroller, and fixed Sharp units are updated through the network.

- **Optimize Root folder disk space.** (Windows Vista or later only) Enables the use of symbolic links to reduce disk utilization when the same file is replicated in multiple folders, such as when you have large hotlists and/or permit lists associated to individual Patroller units. This reduces the Root folder's overall disk space, and optimizes file transfer performance to the Patroller in-vehicle computer.

  IMPORTANT If your root folder is on a network drive, the Genetec Server service must be configured to run using a domain user and not a local user.

  To use this feature, the server machine must be running Windows Vista or later, otherwise hotlists and permits will be copied as usual (duplicate copies on disk). The client machine must also be running Windows Vista or later, otherwise the client won't be able to access the files inside the root folder.

  After enabling this option in Security Center, you also must enable it in Windows on your server and client machines (you'll need administrator rights).

  On both the server and client machines, open Windows Command Prompt, and then type the following:

  - *To enable symbolic links.* Type `fsutil behavior set SymlinkEvaluation R2R:1`
  - *To disable symbolic links.* Type `fsutil behavior set SymlinkEvaluation R2R:0`.

- **User group for Patrollers.** List of users (and their passwords) who are allowed to log on to the Patrollers managed by the LPR Manager. This list is downloaded to the Patrollers.

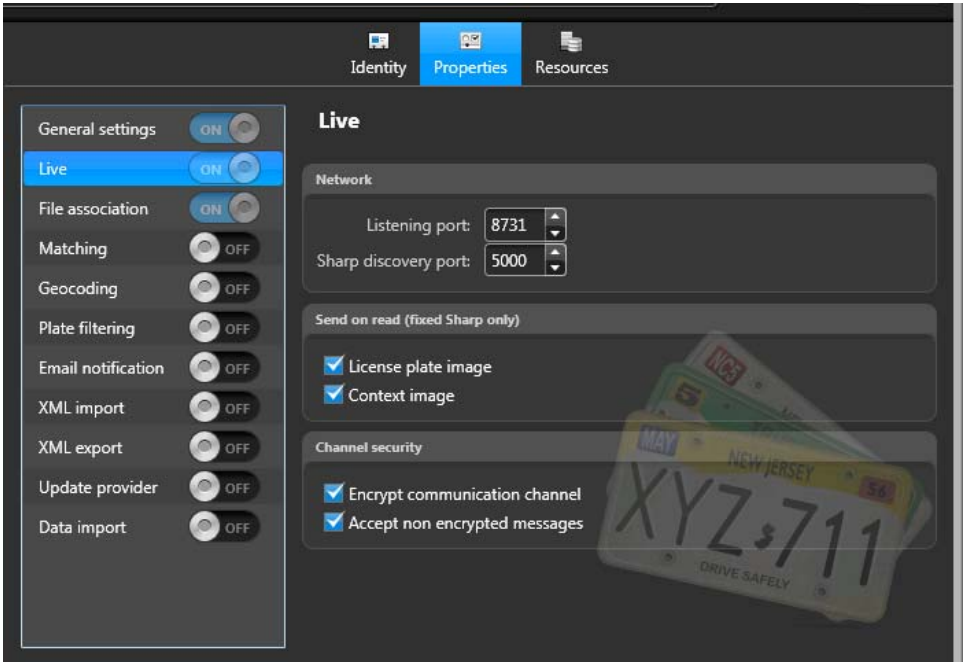
  In Patroller Config Tool, if the Patroller *Logon type* is *Secure name* or *Secure name and password*, the Patroller user will be required to enter the username and password configured in Security Center. If secure logon names are in use, when a read or a hit occurs, in Security Desk you can view who was driving the vehicle.

- **Database retention periods.** Specify how many days of LPR-related data Security Center can query. The default is 90 days, and the maximum is 2000 days. LPR data that is older than the value(s) you specify will not appear in Security Center queries and reports (Hit reports, Read reports, and so on).
  - *Patroller route retention period.* Number of days Patroller route data (GPS positions) can be queried.
  - *Hit retention period.* Number of days hit data can be queried.
  - *Read retention period.* Number of days license plate reads can be queried.

- *Event retention period.* Number of days the LPR events *License plate read* and *License plate hit* can be queried.

Live

The *Live* settings are used to configure how data is transferred between Security Center and Patroller.



- **Listening port.** Port used to listen for connection requests coming from fixed Sharps and Patrollers. After the connection is established, the LPR Manager can receive live updates from the LPR units it manages.
- **Sharp discovery port.** Port used by the LPR Manager to find fixed Sharp units on the network. The same port number must be used in the *Discovery port* setting on the Sharp.

  IMPORTANT Each LPR Manager must use a unique discovery port.
- **Send on read (fixed Sharp only).** For each plate read, choose which Sharp images are sent to Security Center. These images are displayed in Security Desk when monitoring LPR events.
  - *License plate image.* Include the high resolution close-up image of the license plate along with the plate read data.
  - *Context image.* Include the wide angle context image of the vehicle along with the plate read data.

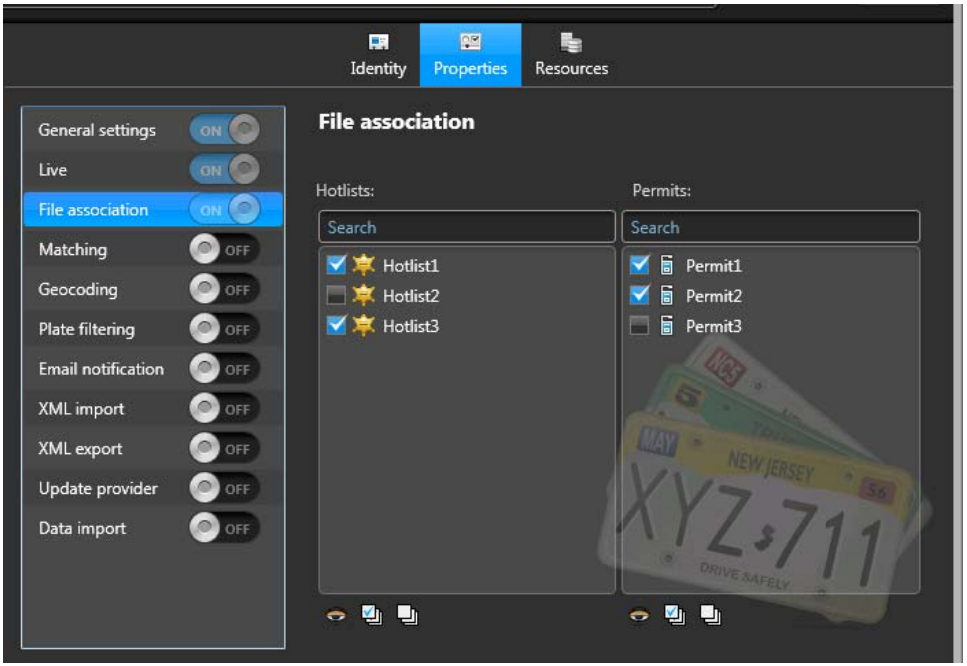
- **Channel security.** Encrypt communication between Security Center and Patroller.

  IMPORTANT Encryption must be enabled both in the Security Center Config Tool and in Patroller Config Tool (see "Security Center" on page 359).

  - *Encrypt communication channel.* Encrypt communication between Patroller and Security Center.
  - *Accept non encrypted messages.* Security Center will accept incoming connections from Patrollers that do not have the encryption option enabled.

File association

The *File association* settings specify which hotlists and permits are active and managed by the LPR Manager.



- **Hotlists.** A list of all the hotlists in Security Center. Choose which hotlists you want the LPR Manager to manage. The LPR Manager then sends the hotlists to the Patrollers it manages, or matches the hotlists against the reads collected from fixed Sharp units to produce hits. When you create a new hotlist, it is automatically added to this list and enabled for all the LPR Managers on your system.
- **Permits.** A list of all the permits in Security Center. Choose which permits the LPR Manager manages. The LPR Manager sends these permit lists to Patrollers. Only Patrollers configured for parking enforcement require permits. When you create a new permit, it is automatically added to this list and enabled for all the LPR Managers on your system.

NOTE You can also associate permits to individual Patrollers, and hotlists to individual Patrollers or Sharp units. For more information, see "Patroller" on page 330, and "LPR unit" on page 327.

Matching

The *Matching* settings are used to enable matching between hotlists and fixed Sharp units. You use these settings when you want to configure event-to-actions in Security Desk that trigger on "match" or "no match" events.

- **Matching.** Enables matching between fixed Sharp units and hotlists. When matching is enabled, you can configure event-to-actions in Security Desk that trigger when the Sharp reads a plate that is on a hotlist you've activated in File association.
- **Generate "No match" events.** Security Center generates "no match" events when a plate is *not* found on a specific hotlist. You can then configure event-to-actions in Security Desk based on "No match" events.

  You would typically use "No match" events as part of an access control scenario. For example, you can associate a hotlist to a specific Sharp unit that is monitoring access to a parking lot or similar location. In this scenario, a Security Center event-to-action for a "License plate hit" grants the vehicle access (opens a gate, raises a barrier, and so on), and an event-to-action for a "No match" could trigger an alarm, or send an email to security personnel.

Reverse geocoding

The *Reverse geocoding* feature converts the raw GPS data (longitude, latitude) from Patrollers into street addresses. The street addresses are then saved along with the reads in the LPR Manager database.

NOTE You need geocoding if your Patrollers are equipped with GPS but no maps.

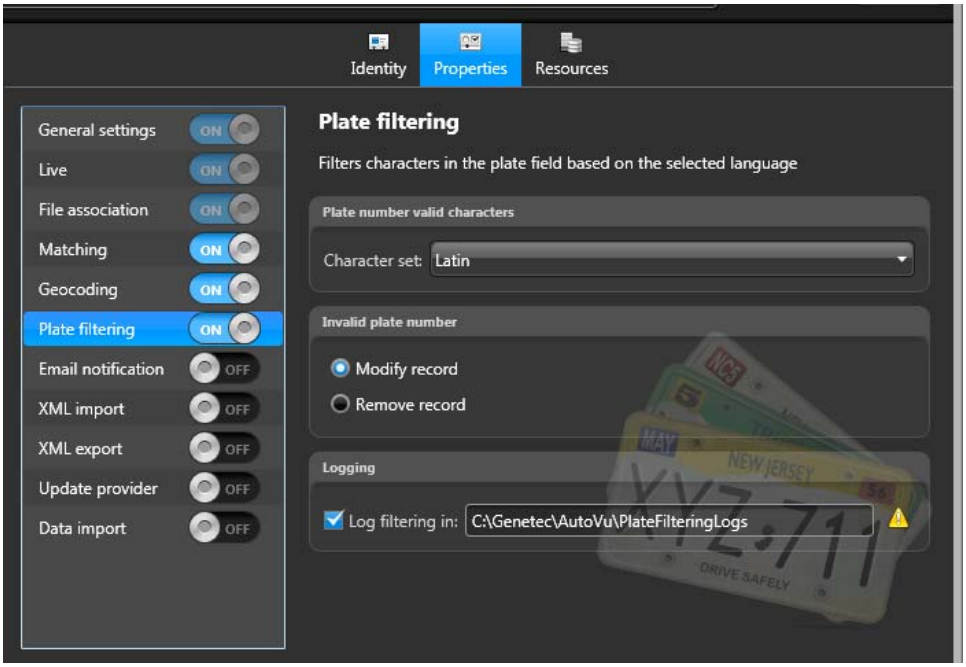
- **Map type.** Displays the map type set in the Security Center license.
- **Maps and data folder.** Location of the folder where the map files are found. This folder must be on the same computer where the LPR Manager is installed.

IMPORTANT After March 15th, Genetec will no longer support Bing as the default mapping solution. However, you can continue to use Bing for mapping and reverse geocoding by obtaining your own Bing license from Microsoft. For more information, see "Using Bing for mapping and reverse gecoding" on page 98.

Plate filtering

The *Plate filtering* settings determine what to do when a hotlist or permit list is modified. The LPR Manager can detect if the new or modified lists include entries that contain invalid (non-alphanumeric) characters. You can configure the LPR Manager to either delete the invalid entries completely, or to delete only the invalid characters within the entries. You can also save

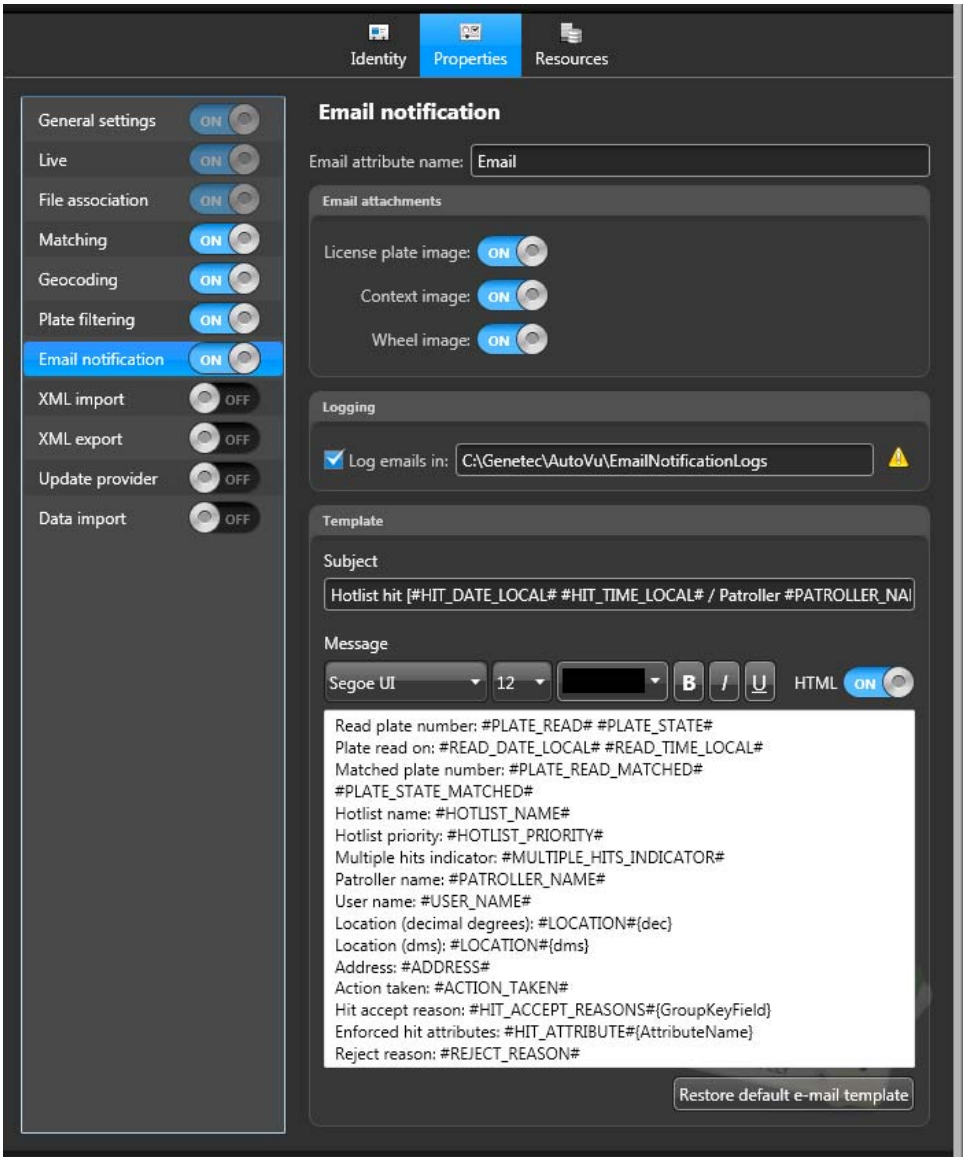
logs of the filtering process to view detailed information about how many invalid entries were deleted or modified. This option is enabled by default when you install Security Center or create a new LPR Manager role.



- **Plate number valid characters.** Select the types of characters to filter on (Latin, Arabic, Japanese, or Cyrillic).
- **Invalid plate number.** Configure how the LPR Manager handles invalid records:
  - *Modify record.* (Default setting). Removes any non-alphanumeric characters from the plate number. For example, the plate number "ABC#%3" becomes "ABC3".
  - *Remove record.* Deletes the entry from the list entirely.
- **Logging.** Select **Log filtering in**, and then specify where you want the log file to be saved. The destination folder you choose must be accessible to the computer hosting the LPR Manager role.

Email notification

The *Email notification* setting turns on email notifications for hotlist hits, and lets you customize the look and contents of the email message. You can configure email notification at the hotlist level (any hit from a hotlist), or at the individual license plate level (a hit from a specific plate). For more information, see "Configuring email notifications for hotlist hits" on page 122.



- **Annotation email address.** Used for email notification at the individual license plate level. Type the name of the hotlist attribute related to email notification. For example, if you added an "Email" attribute on the hotlist entity's Properties page, type the exact same name here. The names must match exactly.
- **Email components.** Choose the LPR data you want to attach to the notification email, and whether to hide the license plate numbers in the message body.
  - *License plate image.* High resolution close-up images of the license plate.
  - *Context image.* A wider angle color image of the vehicle.
  - *License plate.* Replaces the read plate number, and the matched plate number in the email with asterisks (*).
- **Log emails in.** Select the check box to log hotlist hit notification emails. Type the full path to the log file.
- **Template.** Customize the email. Do any of the following:
  - Edit the email's subject line or message body.
  - Switch between plain text and HTML.
  - Add formatting (bold, italics, and so on).
  - Right-click in the message body for a menu of quick tags that you can use to add more information to the email.
  - Restore the default email template at any time.

XML import

The *XML import* settings are used to import data from third-party applications into the LPR Manager database. When you turn this setting on, Security Center creates an *XML import* entity, and then associates the imported data with this entity. In Security Desk, you can then filter on the *XML import* entity when running hit or read reports.

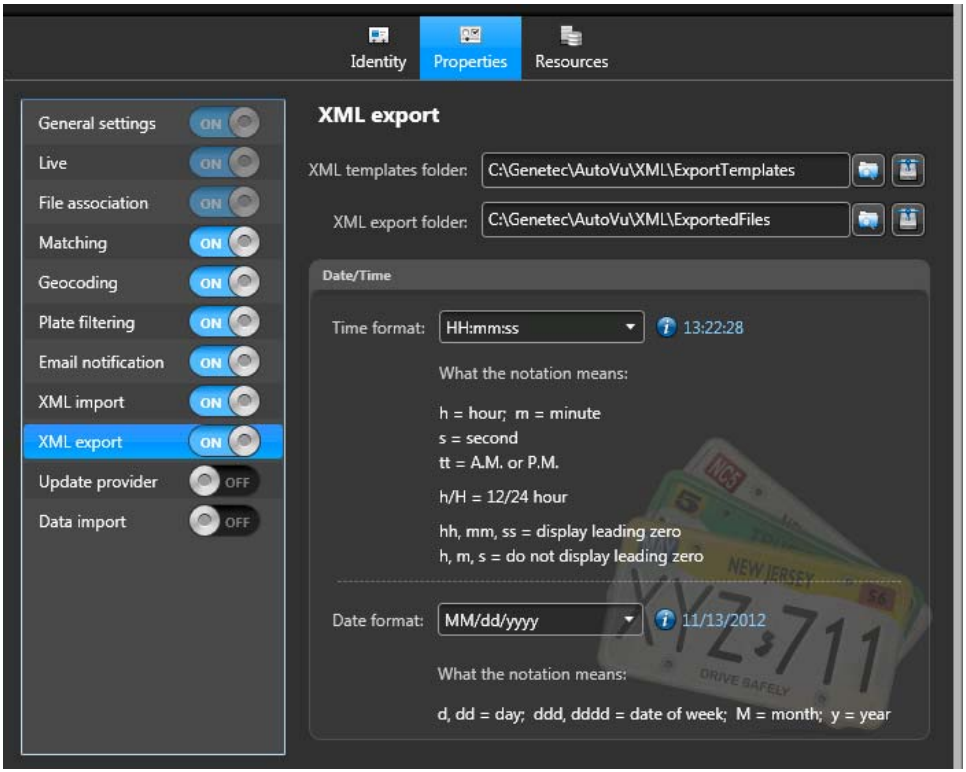
NOTE The LPR data imported cannot be displayed in a live Security Desk monitoring task, but it is matched against loaded Hotlists. You can then generate a hit report to see the data.

- **XML template file.** Specify where the XML template file is located. You'll find a default template in the Security Center installation package in *Tools\LPR\XMLTemplatesSamples*.
- **XML data folder.** Specify the folder that contains the XML data files for Security Center to import.
- **Supported XML hashtags.** The following XML hashtags are supported. Each hashtag must have an opening and closing XML tag (for example, to use the tag *#CONTEXT_IMAGE#* you must write *<ContextImage>#CONTEXT_IMAGE#</ContextImage>* in the XML):
  - *#GUID#*. Unique identifier of the LPR event. If this value is not included, a value will be created by default.
  - *#Time_Zone#*. Name of the time zone where the read occured. The format must conform to the *TimeZoneInfo.Id Property* of the .NET Framework. If this value is not included, or if it is invalid, the time zone of the LPR Manager role is used.

- *#DATE_LOCAL#, #DATE_UTC#, #TIME_LOCAL#, #TIME_UTC#.* Date and time (local or UTC) of the LPR event. You must specify a format for these hashtags (for example, #DATE_LOCAL#{yyyy/MM/dd}). For more information about which formats to use, see the MSDN article at http://msdn.microsoft.com/en-us/library/8kb3ddd4.aspx. If these hashtags are not included, UTC dates and times are used as a baseline for calculating the local time. If an error occurs, the time the LPR Manager role imported the data is used.
- *#PLATE_IMAGE#, #CONTEXT_IMAGE#.* The plate and context images as Base64-encoded images.
- *#PLATE_READ#.* License plate as read by the Sharp.
- *#PLATE_STATE#.* License plate's issuing state or province, if read.
- *#RULE_ID#, #LOT_ID#.* Unique identifiers of parking lots and facilities. These are typically used for MLPI deployments. If these hashtags are not included, the *Guid.Empty* is used.
- *LATITUDE#, #LONGITUDE#.* Latitude and longitude of the event. This must be formatted in decimal degrees.
- *#CUSTOM_FIELDS#.* You can import other fields with this hashtag by using the *key=value* format. Format the key as *#CUSTOM_FIELDS#{KEY}*.

XML export

The *XML export* settings are used to send LPR Manager reads and hits to third-party applications. Reads and hits are sent live as they occur.



- **XML templates folder.** Specify where the XML templates folder is located. You'll find default templates in the Security Center installation package in *Tools\LPR\XMLTemplatesSamples*. There are XML templates for each type of LPR event (plate reads, hotlist hits, overtime hits, permit hits, and shared permit hits).
- **XML export folder.** Specify the folder that contains the XML files exported by the LPR Manager.
- **Time format.** Enter the time format used in the exported files. As you set the time format the information field displays what the time format will look like in the XML file.
  To identify the units of time, use the following notation:

Notation	Description
h	Hour
m	Minute

s	Second
:	Must use a colon (:) between the hour, minute, and second units.
hh,mm,ss	Display time with leading zero. For example: 03:06:03 represents 3 hours 6 minutes 3 seconds.
h,m,s	Display without leading zero. For example: 3:6:3 represents 3 hours 6 minutes 3 seconds.
tt	Include A.M. or P.M. If using a 12-hour clock, you might want to use A.M. or P.M. notation. Unit can be preceded with or without a space. For example, HH:mm:ss tt displays 17:38:42 PM.
Lowercase h	12-hour clock.
Uppercase H	24-hour clock.

- **Date format.** Enter the date format used in the export files.
  To identify the units of a date, use the following notation:

Notation	Description
M	Month in numerals
MM	Month in numerals with leading zero.
MMM	Month abbreviation. For example Apr for April.
y	Year without century. For example, yy displays 11 for 2011.
yyy	Year with century. For example, yyyy displays 2011
d	Date
dd	Date with leading zero.
ddd	Day of week three letter abbreviation. For example, ddd displays Wed for Wednesday.
dddd	Day of week. For example, dddd displays Wednesday.
Delimiters	Can use space or dash (-) between units in the date.
Example	dddd MM dd, yyy displays Wednesday April 06, 2011.

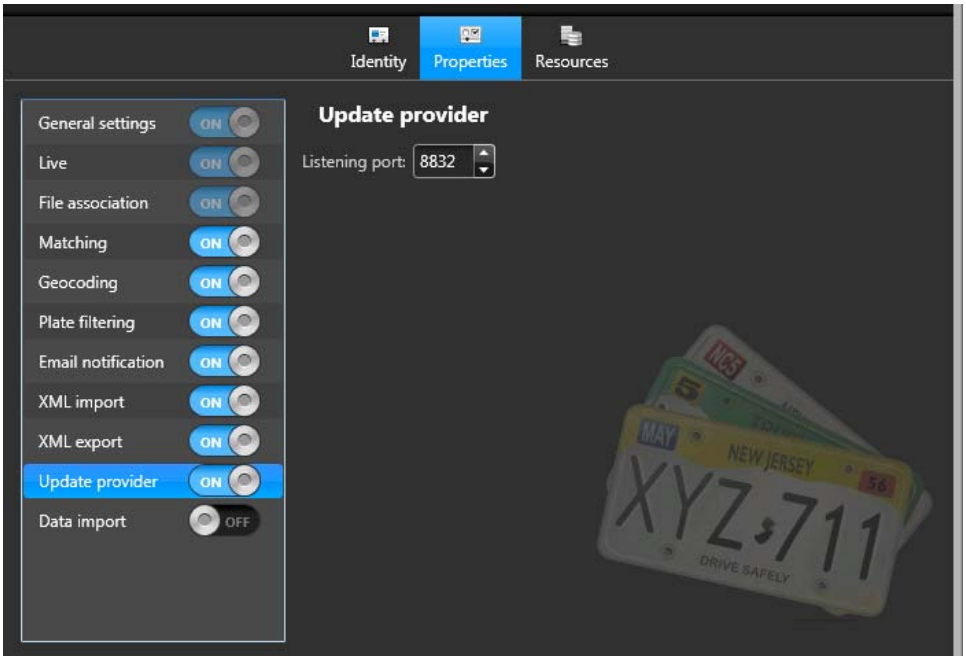
- **Supported XML hashtags.** The following XML hashtags are supported. Each hashtag must have an opening and closing XML tag (for example, to use the tag *#CONTEXT_IMAGE#* you must write *<ContextImage>#CONTEXT_IMAGE#</ContextImage>* in the XML).
  - *#ATTRIBUTES#*. Generate all Read and Hit attributes.

- *#CAMERA_NAME#* . Identifies which camera unit in a SharpX - Multi 2-port, or 4-port system was responsible for a particular plate read.
- *#CONTEXT_IMAGE#*. Context image (Base64-encoded JPEG).
- *#DATE_LOCAL#*. Local date of the LPR event.
- *#ELAPSED_TIME#*. For an overtime hit, this tag indicates the time difference between the two plate reads (displaying the number of days is optional).
- *#FIRST_VEHICLE#*. For a shared permit hit, this tag generates the content specified in *ReadTemplate.xml* for the first vehicle seen.
- *#FIRST_VEHICLE_FROM_STREET#*. For an overtime hit, this tag retrieves the attribute *From street* from the first plate read.
- *#FIRST_VEHICLE_TO_STREET#*. For an overtime hit, this tag retrieves the attribute *To street* from the first plate read.
- *#HOTLIST_CATEGORY#*. Category field of the hotlist that generated the hit.
- *#GUID#*. Unique identifier of the LPR event.
- *#INVENTORY_LOCATION#*. For MLPI installations, the location of the vehicle inventory.
- *#ISHIT#*. This tag indicates if the LPR event is a hit.
- *#LATITUDE_DEGREE#*. Latitude of the LPR event (in degrees).
- *#LATITUDE_DMS#*. Latitude of the LPR event (in degrees, minutes, and seconds).
- *#LATITUDE_MINUTE#*. Latitude of the LPR event (in minutes).
- *#LATITUDE_SECOND#*. Latitude of the LPR event (in seconds).
- *#LONGITUDE_DEGREE#*. Longitude of the LPR event (in degrees).
- *#LONGITUDE_DMS#*. Longitude of the LPR event (in degrees, minutes, and seconds).
- *#LONGITUDE_MINUTE#*. Longitude of the LPR event (in minutes).
- *#LONGITUDE_SECOND#*. Longitude of the LPR event (in seconds).
- *#MATCHED_PLATE#*. License plate against which the hit was generated.
- *#ORIGINAL#*. For an overtime hit, this tag generates the content specified in *ReadTemplate.xml* for the first read of a given plate.
- *#OVERVIEW_IMAGE#*. Overview image (Base64-encoded JPEG).
- *#PARKING_LOT#*. The parking lot or parking facility name given in Security Center.
- *#PATROLLER_ID#*. Unique identifier of the Patroller unit.
- *#PATROLLER_NAME#*. The Patroller name as defined in Patroller Config Tool.
- *#PERMIT_NAME#*. Name of the permit that generated the LPR event.
- *#PLATE_READ#*. License plate as read by the Sharp.
- *#PLATE_IMAGE#*. License plate image (Base64-encoded JPEG).
- *#READ#*. Embed the contents of the *ReadTemplate.xml* inside another XML template (useful for hits).

- *#REJECT_REASON#.* The reason given by the Patroller user for rejecting a hit. Reject reasons must first be configured in Security Center.
- *#SECOND_VEHICLE#.* For a shared permit hit, this tag generates the content specified in *ReadTemplate.xml* for the second vehicle seen.
- *#SECOND_VEHICLE_FROM_STREET#.* For an overtime hit, this tag retrieves the attribute *From street* from the second plate read.
- *#SECOND_VEHICLE_TO_STREET#.* For an overtime hit, this tag retrieves the attribute *To street* from the second plate read.
- *#SHARP_NAME#.* Name of the Sharp that read the plate.
- *#STATE#.* License plate's issuing state or province, if read.
- *#TIME_LOCAL#.* Local time.
- *#USER_ACTION#.* User action related to the LPR event.
- *#USER_ID#.* Unique identifier of the Security Center user that is logged on to Patroller.
- *#USER_NAME#.* The username of the Security Center user that is logged on to Patroller.
- *#VEHICLE#.* Same as #READ#.
- *#ZONE_COLOR#.* Color of the zone associated to the LPR event.
- *#ZONE_ID#.* The unique identifier of the zone associated to the LPR event.
- *#ZONE_NAME#.* Name of the zone associated to the LPR event.

Update provider

Turn on the *Update provider* to create the required sub-folder in the LPR Root folder that will receive the update files. Also, you need to specify the **Listening port** used for Patroller and Sharp updates. The LPR Manager will use this port to update Patrollers and Sharps with new hot fixes, hit alert sounds, hotlists, firmware and so on.



- **Listening port.** This is the port Security Center uses to send updates to Patrollers and connected Sharp units, as well as to fixed Sharps on the network. Make sure to use the same port number in Patroller Config Tool (see "Security Center" on page 359), and in the Sharp Portal (see "Extension" on page 379).

Data import

The *Data* import settings are used to import data from AutoVu 4.3 systems. The LPR Manager connects to the AutoVu Gateway 4.3 database and imports all mobile data into the LPR Manager database so that the data can be viewed with Security Desk.

IMPORTANT Before you turn on Data import, configure the AutoVu Gateway database server and database name.

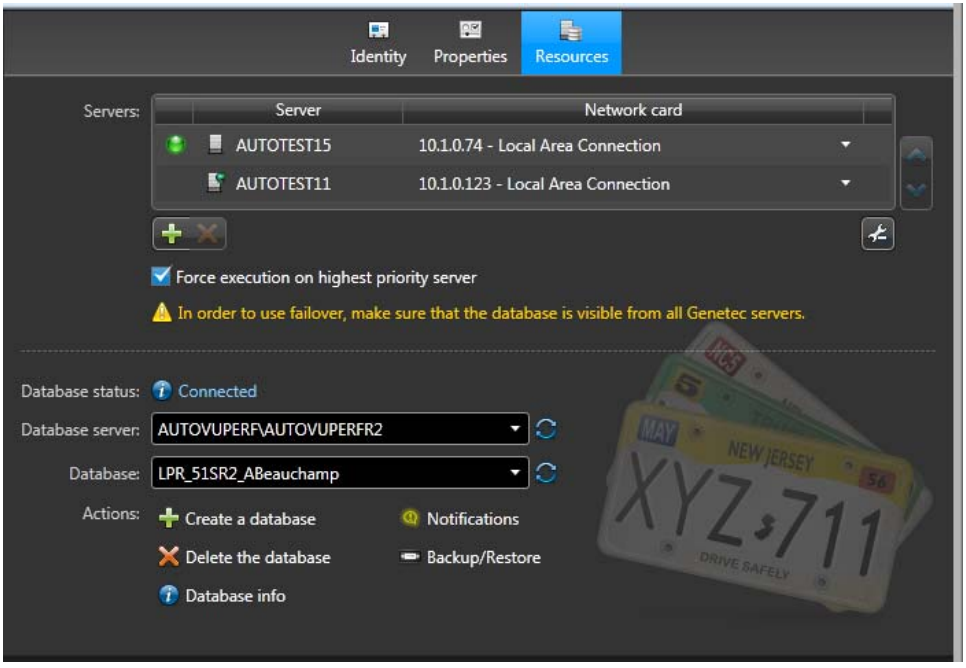
NOTE Please note the following about importing the AutoVu Gateway 4.3 database into Security Center:

- The first time you run the migration, the LPR Manager will import everything that is in the existing Back Office database up until the retention period specified in the General settings.
- It takes approximately one hour for every 2.5 GB of data to transfer. For example, if you have 100 GB of data, the data import process will take approximately 40 hours.
- After the first batch of data is imported, the import process will resume every 12 hours. In the mean time, the old system can operate as usual.
- As data from the legacy system is imported into Security Center, you'll see the Patroller and LPR units appear under the LPR Manager.
- For information on how to migrate to Security Center 5.0 from AutoVu 4.3, see the *Security Center Installation and Upgrade Guide*.

- **Data server.** Name of the data server used by the legacy AutoVu Gateway.
- **Database.** Name of the legacy AutoVu Gateway database.

Resources

The *Resources* tab allows you to configure the servers and database assigned to this role.



Servers

All server management principles are the same for the LPR Manager role as with any other Security Center role.

For more information, see the *Security Center Administrator Guide*.

Database

All database management principles are the same for the LPR Manager role as with any other Security Center role.

NOTE When backing up (or restoring) the database to a network drive, you must manually enter the network path (for example, \\<*MyNetworkDrive*>\<*Backup DB folder*>\. For more information, see the *Security Center Administrator Guide*.

Hotlist

The *hotlist* entity defines a list of wanted vehicles. Each vehicle in the list is identified by a license plate number, the license plate issuing state (or province, or country), and the reason why the vehicle is wanted (for example, Stolen, Wanted felon, Amber alert, VIP, and so on). Additional vehicle information can include the model, the color, and the vehicle identification number (VIN).

Hotlists are used by both the AutoVu Patroller and the AutoVu LPR Manager role to check against license plates captured by LPR units to identify vehicles of interest.

The hotlist entity is a type of hit rule. A hit rule is a method used by AutoVu to identify vehicles of interest. Other types of hit rules include *overtime*, *permit*, and *permit restriction*. When a plate read matches a hit rule, it is called a hit. When a plate read matches a plate on a hotlist, it is called a hotlist hit.

System: AutoVu IP license plate recognition

Task: LPR – Hotlists

	Identity	Name, description, logical ID, and relationships of this entity with other entities in the system.
	Properties	Configure the basic parameters of the hotlist, including: assigning priority to a hotlist, and the location and attributes of the hotlist data file.
	Advanced	Configure the advanced parameters of the hotlist, including: assigning color, sound, email address for notifications, and enabling hotlist and permit editor support.
	Custom fields	Custom field values for this hotlist.

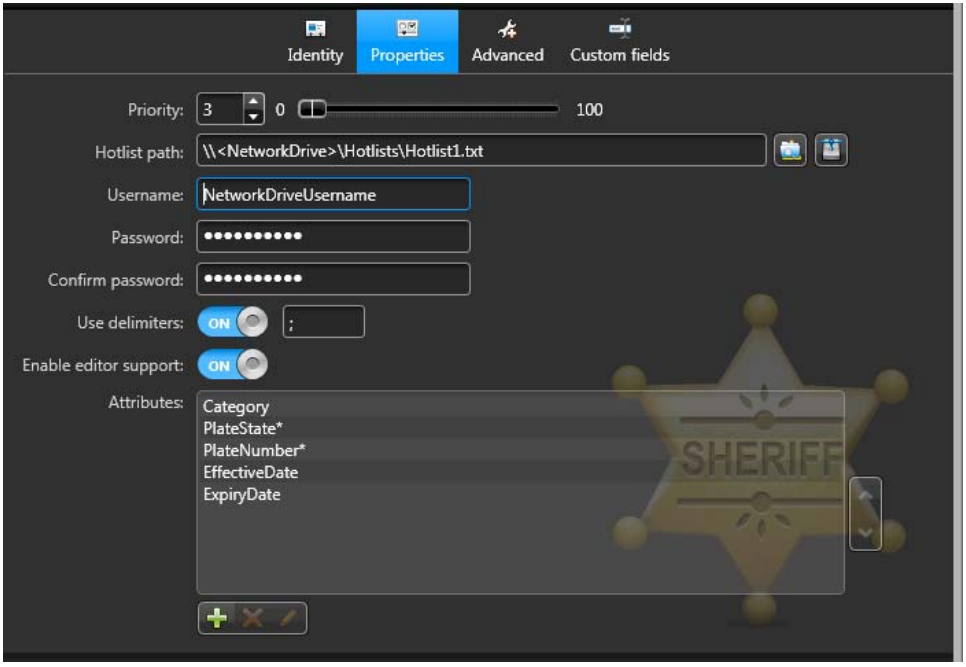
Related topics:

- "LPR Manager" on page 284
- "LPR unit" on page 327

Properties

The *Properties* tab is where you configure the basic properties of the hotlist (hotlist priority, hotlist path, attributes, and so on). These settings tell Security Center how to parse the hotlist file into the format required by the Patroller and the LPR Manager to identify plates read by Sharp units.

For more information on how to configure hotlists, see "Configuring hotlists" on page 120.



- **Priority.** Choose a hotlist priority. Zero (0) is the highest priority setting and 100 is the lowest priority setting. This setting is used to resolve conflicts when a plate read matches more than one hotlist, in which case the hotlist with the highest priority is displayed first in the list of hotlist matches.
- **Hotlist path.** Type the path or browse to the hotlist text file. Every hotlist entity in Security Center must be associated with a text file containing the actual hotlist data; that is, license plate numbers and other related vehicle information. The associated text file is typically created by a third party system (e.g. Notepad for *.txt* files, or Excel for *.csv* files).

  The source text file can be located on the LPR Manager computer's local drive (for example, the C drive), or on a network drive that is accessible from the LPR Manager computer. If you start typing a path to a network drive, the **Username** and **Password** fields appear and you'll need to type the username and password to access the network drive.
- **Use delimiters.** Tells Security Center that the fields in the hotlist file are of variable length and indicates the character used to separate each field in the file. By default, **Use delimiters**

is set to **On**, and the delimiter specified is a **semi-colon** (;). If your hotlist file is made up of fixed length fields, set **Use delimiters** to Off.

Security Center supports the following delimiters:

- Colon (:)
- Comma (,)
- Semi-colon (;)
- Tab (Tab)

If your hotlist file uses Tab as a delimiter (i.e. the "Tab" key on your keyboard), type the word "TAB" as the delimiter character.

IMPORTANT Security Center considers one Tab space to be a valid delimiter. Do not use more than one Tab space to align columns in your hotlist file or Security Center may not be able to parse the hotlist.

- **Enable editor support.** Allow a user to edit the hotlist or permit list using the Hotlist and permit editor task.

  IMPORTANT Please note the following about the Hotlist and permit editor:

  - A user must be granted the privilege to use the Hotlist and permit editor.
  - Only the first 100,000 rows of a hotlist are loaded into the Hotlist and permit editor.
  - If an error occurs while the hotlist is being loaded, the loading process is cancelled and an error message is displayed. However, you will not lose any of the data loaded before the error occurred, and you can still edit the data loaded into the editor.
- **Attributes.** Tells Security Center the name and order of the fields in the source text file. From the Attributes area, you can add, delete, or edit the data fields (attributes). Security Center includes the following default attributes:
  - *Category.* (Mandatory field) Reason why a license plate number is wanted. For example: Scofflaw, Stolen, Amber alert, Wanted felon, and so on. When a hit occurs, this field is displayed on the hit screen in Patroller and Security Desk.
  - *PlateState.* (Mandatory field) Issuing state (or province, or country) of the license plate. Patroller uses the PlateNumber to match against a plate read. When a hit occurs, this field is displayed on the hit screen in Patroller and Security Desk.
  - *PlateNumber.* (Mandatory field) The license plate number.

  The following fields are shown by default, but are optional. If there is no start or end date for the hotlist, you can delete these fields, or simply leave them blank.

  - *EffectiveDate.* Date at which the hotlist starts to be effective.
  - *ExpiryDate.* Date after which the hotlist is no longer valid.

  IMPORTANT Please note the following about hotlist attributes.

  - The hotlist text file must include Category, PlateState, and PlateNumber fields. For this reason, these fields already appear in the attribute list and cannot be deleted from the list.
  - There cannot be any spaces within an attribute name.

- You can have a maximum of two wildcard characters (asterisk *) in a PlateNumber.

- **Add () or Edit () a hotlist attribute.** Configure the following:
  - *Name.* Name of the field. It may contain spaces. Only the three compulsory fields, Category, PlateState and PlateNumber cannot be renamed.
  - *Value.* The default value is interpreted differently depending on whether delimiters are used or not.
    - If delimeters are in use, the default value is written into this field. Fields already populated will be overwritten.
    - If delimeters are not in use, and if the field is empty, the default value is written into this field. Fields already populated will not be overwritten.
  - *Is mandatory.* A mandatory attribute cannot be blank in the source file. For example, if you add a mandatory attribute called *CarColor*, the column for *CarColor* in the source file must have text in it.
  - *Fixed length.* This option is enabled only if you chose to use fixed length data fields. Indicate the start position of the field in the file record and its length. The position of the first character is zero (0).
  - *Date format.* Specify a time format if the field contains a date or time value. All standard date and time format strings used in Windows are accepted. If nothing is specified, the default time format is "yyyy-MM-dd".
  - *Translate.* You can apply an optional transformation to the values read from the data file. Use this feature to shorten certain values to save space on the Patroller or to enforce spelling consistency.

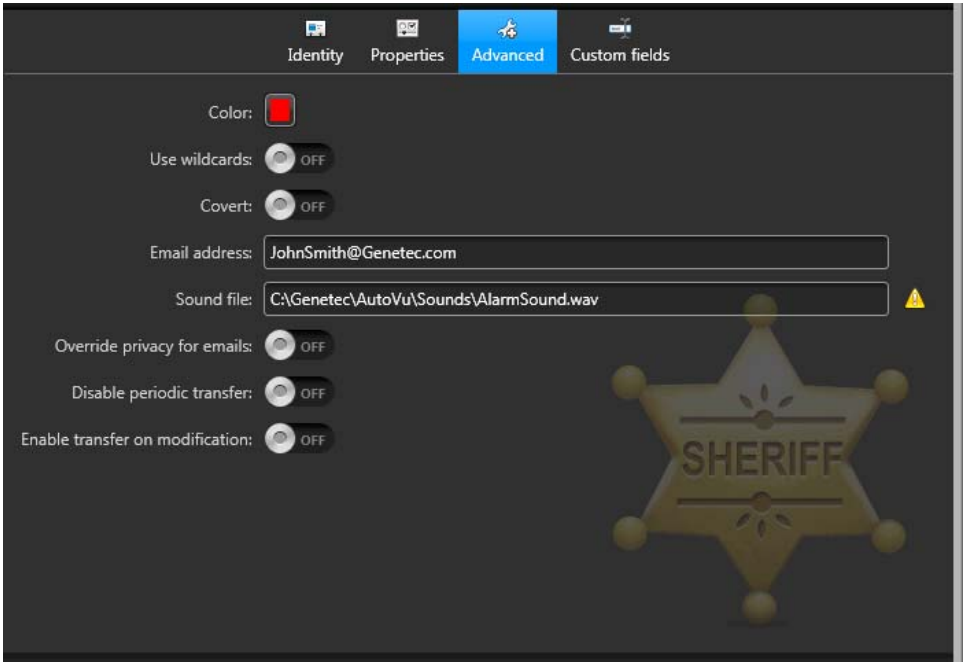
  For example, the following is what you may find in a variable field length data file using a semicolon (;) as delimiter and using the fields: *Category, PlateState, PlateNumber, CarMake,* and *CarColor.*

```
AMBER;QC;DEF228;TOYOTA COROLLA;GREEN
STOLEN;QC;345ABG;HONDA CIVIC;BLUE
STOLEN;QC;067MMK;FORD MUSTANG;YELLOW
STOLEN;QC;244KVF;LEXUS IS350;SILVER
```

Advanced

The *Advanced* tab is where you configure the advanced properties of the hotlist (the color, sound, download frequency, and so on). These properties are not required for all hotlists, but allow you to customize certain hotlists for specific scenarios.

For more information on how to configure hotlists, see "Configuring hotlists" on page 120.



- **Color.** Assigns a color to a hotlist. When you choose a color, the map symbol that marks the location of the hotlist hit in Security Desk and Patroller, as well of the Hotlist Hit and Review Hits screen in Patroller, appears in that color.
- **Use wildcards.** Indicates that the hotlist contains wildcards (partial license plate numbers). You can have a maximum of two wildcard characters (asterisk *) in a PlateNumber.

  Wildcard hotlists are used in situations where witnesses did not see, or cannot remember a complete license plate number. This allows the officer to potentially intercept vehicles associated with a crime, which otherwise would not have been detected using standard hotlists.

  Best practice: If using a wildcard hotlist, use the following best practices:
  - Do not use more than one wildcard hotlist per Patroller.
  - By default, hotlists are applied at the LPR Manager level. Use only one wildcard hotlist per LPR manager role.
  - Limit the number of entries to 100 plates.

NOTE If using wildcard hotlists, please note the following:

- An asterisk (*) in the data file indicates a wildcard.
- Only the PlateNumber field accepts wildcard characters. If the asterisk is found in any other field, it is considered as a normal character.
- The PlateNumber field is limited to two wildcard characters.
- If you select **Use wildcards**, Patroller ignores all hotlist entries that do not contain a wildcard, or that contain more than two wildcard characters.
- It is the number of wildcards in the PlateNumber field, and not the location of the wildcard, that determines how many mismatched characters are allowed before a match can occur.
- The position of the wildcards cannot be enforced because, typically, when witnesses report a partial plate number, they do not remember the position of the characters they missed. The sequence of the normal characters in the PlateNumber is respected, such that the three patterns "S*K3*7", "**SK37", and "SK37**" are equivalent.

  EXAMPLE If a wildcard hotlist contains the PlateNumber entry S*K3*7:

  - Plate reads NSK357 and ASDK37 will generate a hit because both reads have no more than two mismatched characters (in red) and the sequence "SK37" is respected.
  - Plate read SUKA357, will not generate a hit because it contains three mismatched characters (in red).
  - Plate read SKU573 read will not generate a hit because the sequence of characters SK37 is not found in the read.

- **Covert.** Set the hotlist to a covert hotlist. When you choose this setting, Patroller users are not alerted when a hit occurs. Only users with sufficient privileges can view covert hits in Security Desk.
- **Email address.** Set hotlist email notifications. When the hotlist you're configuring generates a hit, Security Center sends an email to the address you specify.

  IMPORTANT For this feature to work, the *SMTP configuration* must be set up in the Server Admin and the Email notification option must switched to ON in the Config Tool's LPR Manager **Properties** tab.

- **Sound file.** This indicates which sound Patroller should play when a hotlist hit occurs. If you leave this field blank, Patroller plays its default sounds. The path (you must include the filename) indicates the file's location on the Patroller in-vehicle computer. You can copy sound files to the in-vehicle computer manually, or use the Security Center updater service to push new sound files to Patroller as you would a hotfix. Only *.wav* files are supported.

  For more information, see "Updating Patroller with new sound files" on page 111.

- **Override privacy for emails.** Bypasses any privacy settings you applied at the Directory level (see "Applications" on page 275), and sends an email with real LPR data to the Email address you specified for this particular hotlist.

- **Disable periodic transfer.** Turns off periodic transfer of hotlist modifications to the Patroller computer. When this setting is off, hotlist changes are only downloaded to Patroller when the user logs on to the application. This option requires a wireless connection between Patroller and Security Center.
- **Enable transfer on modification.** Transfer hotlist modifications to Patroller as soon as they occur. For example, you can use this option on a hotlist to force Patroller to query for changes more frequently than the periodic transfer period (which applies to all hotlists). This can be useful for Amber alerts because they can be added to a specific hotlist and sent to a Patroller almost immediately. This option requires a continuous wireless connection between Patroller and Security Center.

Permit

The *Permit* entity defines a single parking permit holder list. Each permit holder is characterized by a Category (whose value is the same as the name of the Permit entity), a license plate number, a license issuing state (or province, or country), an optional permit validity range (effective date and expiry date), and an optional Permit ID.

Permits are used by AutoVu Patrollers configured for either city or university parking enforcement.

The permit entity belongs to a family of methods used by AutoVu to identify vehicles of interest, called hit rules. Other types of hit rules include *hotlist*, *overtime*, and *permit restriction*. When a plate read matches a hit rule, it is called a hit. When a read fails to match any permit loaded in the Patroller, it generates a permit hit.

System: AutoVu IP license plate recognition

Task: LPR – Permits

	Identity	Name, description, logical ID, and relationships of this entity with other entities in the system.
	Properties	Configuring the parsing of the source permit data file for this entity.
	Custom fields	Custom field values for this permit.

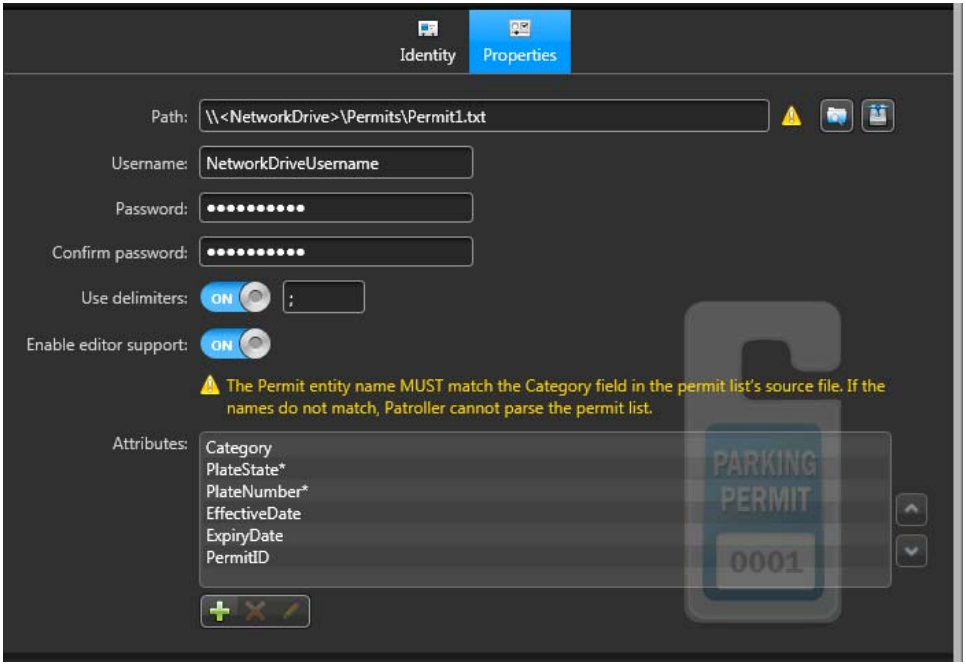
Related topics:

- "Hotlist" on page 304
- "Patroller" on page 330
- "Overtime rule" on page 319
- "Permit restriction" on page 315

Properties

The permit *Properties* tab is used to configure the parsing of the source permit data file.

For more information on how to configure permits, see "Configuring permits and permit restrictions in Security Center" on page 215.



- **Path.** Type the path or browse to the permit text file. Every permit entity in Security Center must be associated with a text file containing the actual permit data; that is, license plate numbers and other related vehicle information. The associated text file is typically created by a third party system (e.g. Notepad for *.txt* files, or Excel for *.csv* files).

  The source text file can be located on the LPR Manager computer's local drive (for example, the C drive), or on a network drive that is accessible from the LPR Manager computer. If you start typing a path to a network drive, the **Username** and **Password** fields appear and you'll need to type the username and password to access the network drive.
- **Use delimiters.** Tells Security Center that the fields in the permit list file are of variable length and indicates the character used to separate each field in the file. By default, **Use delimiters** is set to **On**, and the delimiter specified is a **semi-colon** (;). If your permit list file is made up of fixed length fields, set **Use delimiters** to Off.

  Security Center supports the following delimiters:

  - Colon (:)
  - Comma (,)

- Semi-colon (;)
- Tab (Tab)

If your permit list file uses Tab as a delimiter (i.e. the "Tab" key on your keyboard), type the word "Tab" as the delimiter character.

IMPORTANT Security Center considers one Tab space to be a valid delimiter. Do not use more than one Tab space to align columns in your file or Security Center may not be able to parse the permit list.

- **Enable editor support.** Allow a user to edit the hotlist or permit list using the Hotlist and permit editor task.

  IMPORTANT Please note the following about the Hotlist and permit editor:

  - A user must be granted the privilege to use the Hotlist and permit editor.
  - Only the first 100,000 rows of a list are loaded into the Hotlist and permit editor.
  - If an error occurs while the hotlist is being loaded, the loading process is cancelled and an error message is displayed. However, you will not lose any of the data loaded before the error occurred, and you can still edit the data loaded into the editor.
- **Attributes.** Tells Security Center the name and order of the fields (attributes) in the source text file. You can add, delete, or edit the fields.

  IMPORTANT There cannot be any spaces within an attribute name.

  - *Category.* (Mandatory field) The name of the parking permit. This field in the permit list's source text file *must* match the permit entity name for the entry to be downloaded to Patroller.

    This field allows you to use one permit list for several permit entities on your system, provided you create permit entities for each permit category in your permit list.

    EXAMPLE Here is a simple permit list with three different permit categories (*Students*, *Faculty*, and *Maintenance)*.

    You can use this same permit list for three different permit entities. Create a *Students* permit entity, a *Faculty* permit entity, and a *Maintenance* permit entity, and then point all of them to the same source text file. Security Center will extract the license plates (and related information) whose category is the same as the name of the permit entity.

    IMPORTANT The permit entity name *must* match the category name exactly.

  - *PlateState.* (Mandatory field) Issuing state (or province, or country) of the license plate.
  - *PlateNumber.* (Mandatory field) The license plate number.

  The following fields are shown by default, but are optional.

- *EffectiveDate.* Date from which the particular permit on the list starts to be effective.
- *ExpiryDate.* Date after which the particular permit on the list is no longer valid.
- *PermitID.* (*University Parking Enforcement* only) Used when multiple entries in a permit list share the same permit (e.g. car pool permits). Can be used to identify the number of the permit issued to the vehicle whose license plate is identified in *PlateNumber*. In the case of shared permits, normally up to four separate vehicles would all have the same permit number.

- **Add () or Edit () a permit attribute.** Configure the following:
  - *Name.* Only the three compulsory fields, *Category*, *PlateState,* and *PlateNumber* cannot be renamed. Names may contain spaces.
  - *Value.* The default value is interpreted differently depending on whether delimiters are used or not.
    - If delimiters are in use, the default value is written into this field. Fields already populated will be overwritten.
    - If delimiters are not in use, and if the field is empty, the default value is written into this field. Fields already populated will not be overwritten.
  - *Is mandatory.* A mandatory attribute cannot be blank in the source file. For example, if you add a mandatory attribute called *CarColor*, the column for *CarColor* in the source file must have text in it.
  - *Fixed length.* This option is enabled only if you chose to use fixed length data fields. Indicate the start position of the field in the file record and its length. The position of the first character is zero (0).
  - *Date format.* Specify a time format if the field contains a date or time value. All standard date and time format strings used in Windows are accepted. If nothing is specified, the default time format is "yyyy-MM-dd".

    For example, the following is what you may find in a variable field length data file using a semicolon (;) as delimiter and using the fields: *Category*, *PlateState*, *PlateNumber*, *EffectiveDate*, *ExpiryDate*, and *PermitID*.

    ```
    MyPermit;QC;DEF228;2012-01-31;2012-05-31;PermitID_1
    MyPermit;QC;345ABG;2012-01-31;2012-07-25;PermitID_2
    MyPermit;QC;067MMK;2012-03-31;2012-09-11;PermitID_1
    MyPermit;QC;244KVF;2012-01-31;2012-03-31;PermitID_3
    ```
  - *Translate.* You can apply an optional transformation to the values read from the data file. Use this feature to shorten certain values to save space on the Patroller or to enforce spelling consistency.

Permit restriction

The *permit restriction* entity defines where and when permit holders can park. Different time restrictions can be applied to different permits. For example, a permit restriction may limit the parking in zone A from Monday to Wednesday for permit P1 holders, and from Thursday to Sunday for permit P2 holders.

Permit restrictions are used by AutoVu Patrollers configured for University Parking Enforcement.

The permit restriction entity is a type of hit rule. A hit rule is a method used by AutoVu to identify vehicles of interest. Other types of hit rules include *hotlist, overtime,* and *permit*. When a plate read matches a hit rule, it is called a hit. When a plate read matches a permit restriction, it generates a permit hit. Additionally, a shared permit hit occurs when two plates sharing the same permit ID are read in the same parking zone within a specific time period.

System: AutoVu IP license plate recognition

Task: LPR – Permit restrictions

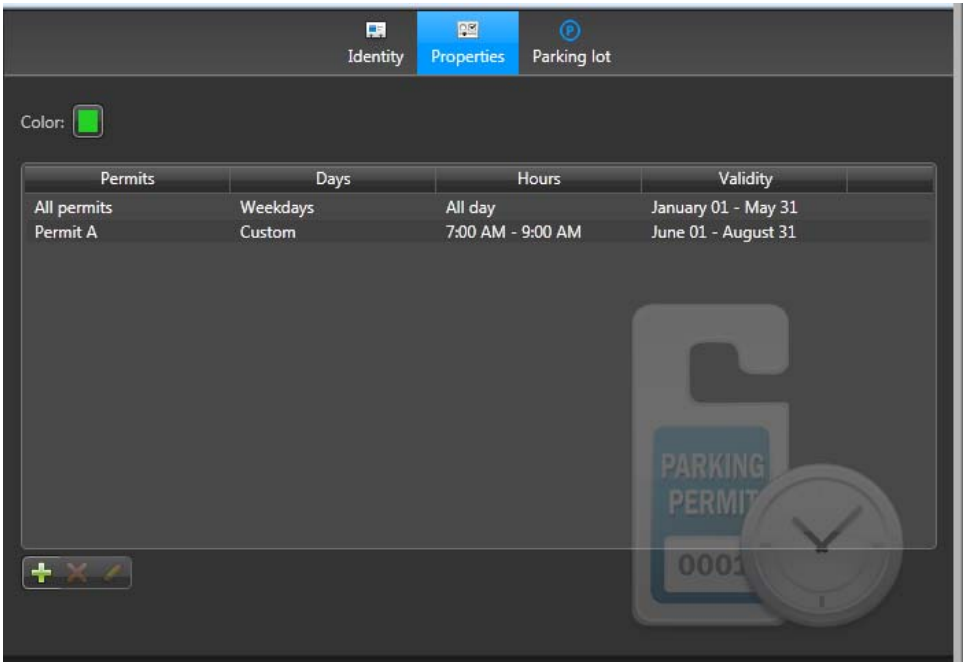
	Identity	Name, description, logical ID, and relationships of this entity with other entities in the system.
	Properties	The parking restrictions applied to this entity.
	Parking lot	The parking zone where this entity is enforced.
	Custom fields	Custom field values for this permit restriction.

- "Overtime rule" on page 319
- "Patroller" on page 330
- "Permit" on page 311

Properties

The *Properties* tab is used to configure the restrictions for the individual permits that apply to the parking zone represented by the rule.

For more information on how to configure permit restrictions, see "Configuring permits and permit restrictions in Security Center" on page 215.



- **Color.** Color used to represent the permit restriction in Security Desk. In Patroller, permit restrictions are always green for regular permit hits, or blue for shared permit hits. A read is displayed as a triangular-shaped icon in the selected color on the map, when an permit restriction is in effect. When a read violates one of the restrictions, the icon is encircled with a red ring. It indicates a permit hit.
- **List of restrictions.** Define the time restrictions for the different permits associated to a parking zone. Each time restriction is described by the following attributes:
  - *Permits.* Select the permits the time restriction applies to:
    - *Everyone*. Parking is available to everyone, regardless of whether they have a permit or not. No restriction is enforced during the specified time period.
    - *No permit*. Only vehicles without permits can park. For example, you can use this type of restriction to reserve a zone for visitors parking. A plate read that matches any of the permits downloaded to the Patroller raises a hit.

- *All permits*. Only vehicles with a permit can park. A plate read that does not match any of the permits downloaded to the Patroller raises a hit.
- *Specific permits*. Only vehicles having one or more of the specified permits can park. A plate read that does not match any of the specified permits raises a hit.

When multiple time restrictions apply at a given time, conflicts are resolved by evaluating the restrictions in the following order: 1. *Everyone*, 2. *No permit*, 3. *All permits*, 4. *Specific permits*. Moreover, a hit is raised when a matched permit is not valid (either not yet effective or already expired).

- *Days.* Days of the week when parking is allowed.
- *Hours.* Time during the day when parking is allowed.
- *Validity.* Dates when parking is allowed. Choose **All year** or select a specific time span using the date picker.

NOTE The date span must be longer than one day.

Parking lot

The *Parking lot* tab defines the parking zone where this parking rule must be enforced. The Parking lot tab displays a Bing map, on which you can add a parking lot, define the number of spaces in the lot, and then draw a polygon on top of the map to represent the physical parking lot. The number of spaces in the lot is used to calculate the percentage of parking occupancy in that area. For more information on how this information is being used, see "Zone occupancy report" in *Genetec Security Desk User Guide.*

NOTE This applies only to AutoVu Patroller University Parking applications.

You can add multiple lots to a map.

Overtime rule

The *overtime rule* entity specifies time limits of parking within a restricted area (a single parking space, a city district, or both sides of a city block). It also specifies the maximum number of overtime violations enforceable within a single day.

The overtime entity is downloaded to Patroller. In Patroller, an overtime hit occurs when the time between two plate reads of the same plate is beyond the time limit specified in the overtime rule. For example, your overtime rule specifies a four hour parking limit within a city district. The Patroller operator does a first pass through the district at 9:00 A.M. collecting license plate reads. The operator then does a second pass through the district at 1:05 P.M. If a plate was read during the first and second pass, Patroller will generate an overtime hit.

The overtime rule is a type of hit rule. A hit rule is a method used by AutoVu to identify vehicles of interest. Other types of hit rules include *hotlist*, *permit*, and *permit restriction*. When a plate read matches a hit rule, it is called a hit. When a pair of plate reads (same plate read at two different times) violates an overtime rule, it is called an overtime hit.

System: AutoVu IP license plate recognition

Task: LPR – Overtime rules

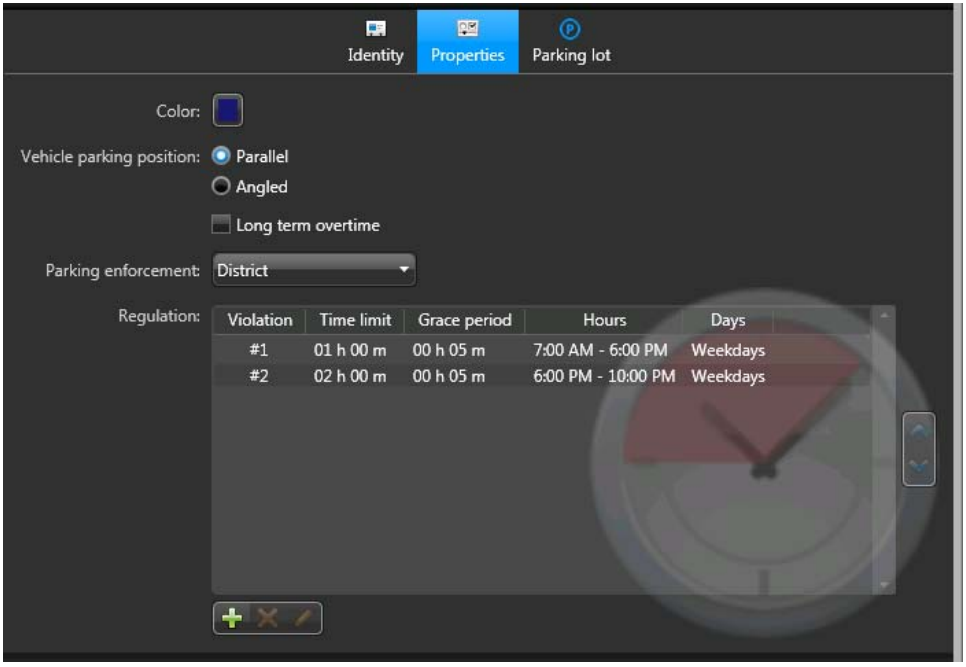
	Identity	Name, description, logical ID, and relationships of this entity with other entities in the system.
	Properties	The parking regulations enforced by this entity.
	Parking lot	The parking zone where this entity is enforced.
	Custom fields	Custom field values for this overtime rule.

- "Hotlist" on page 304
- "Patroller" on page 330
- "Permit" on page 311
- "Permit restriction" on page 315

Properties

The *Properties* tab is used to configure the parking regulations enforced by this overtime rule.

For more information on how to configure overtime rules, see "Configuring overtime rules in Security Center" on page 212.



- **Color.** Assign a color to the overtime rule. When you select the overtime rule in Patroller, the plate reads on the map, and the hit screen, are displayed in this color.
- **Vehicle parking position.** Each Patroller has two sets of calibrated parameters for the optimal reading of wheel images, based on the parking position of the vehicles: Parallel or Angled (45-degree). This setting tells the Patroller which set of parameters to use.

  NOTE This setting applies to AutoVu Patroller City Parking Enforcement with wheel imaging applications.

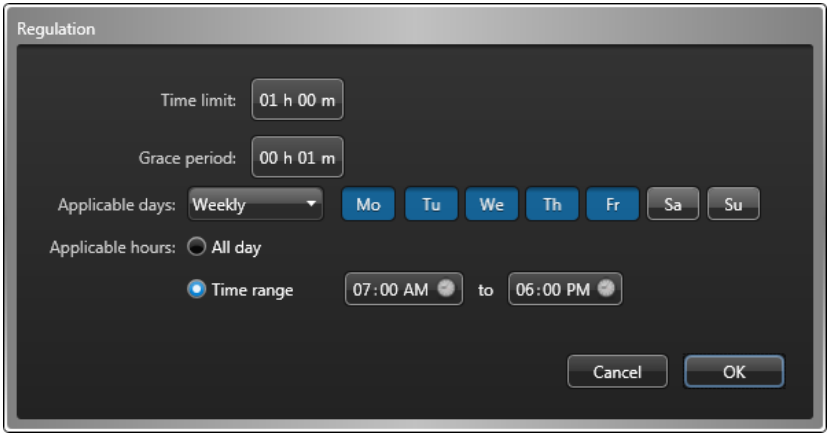
- **Long term overtime.** Use this option for long term parking; that is, where vehicles can park in the same spot for over 24 hours. When Long term overtime is selected, the parking time limit is specified in days (2 to 5 days).

  This option automatically sets the parking regulation to same position, meaning the vehicle has parked overtime when it stays in the same parking space beyond the parking time limit set for such parking space.

NOTE This setting applies to AutoVu Patroller City Parking Enforcement with or without wheel imaging. Wheel imaging is recommended if you plan to use this rule to detect vehicles parked long term so that you can distinguish between someone who parks in the same position and a vehicle which has been abandoned.

- **Parking enforcement.** Select the type of restricted parking area that applies to the time limit: a single parking spot, a district within a city, or both sides of a city block.
  - *Same position.* A vehicle is parked overtime if it parks in the same spot beyond the time limit specified. For example, your overtime rule specifies a one hour parking limit for a single parking space. The Patroller operator does a first pass through the district at 9:00 A.M. collecting license plate reads. The operator does a second pass at 10:05 A.M. If Patroller reads the same plate in the same spot both times, it results in an overtime hit.

    IMPORTANT For this feature to work, Patroller needs GPS capability.
  - *District.* A vehicle is parked overtime if it is parked anywhere within a city district (a geographical area) beyond the specified time limit. For example, your overtime rule specifies a four hour parking limit within a city district. The Patroller user does a first pass through the district at 9:00 A.M. collecting license plate reads. The operator does a second pass through the district at 1:05 P.M. If Patroller reads the same plate in the same district both times, it results in an overtime hit.
  - *Block face (2 sides).* A vehicle is parked overtime if it is parked on both sides of a road between two intersections beyond the specified time limit. For example, your overtime rule specifies a 1hour parking limit within a city block face.The Patroller operator does a first pass through the block face at 9:00 A.M. collecting license plate reads. The operator does a second pass down the block at 10:05 A.M. If Patroller reads the same plate in the same block face both times, it results in an overtime hit.
- **Regulation.** Defines the parking time limit, when it is to be enforced, the grace period to be granted, and how many times it can be enforced within a single day. You can add, delete, and modify a parking regulation. To add a regulation, click , and do the following.



- *Time limit.* The parking time limit in hours and minutes.
- *Grace period.* Time beyond the parking time limit during which overtime violation is waived. For example, Patroller will generate an overtime hit on a plate when time between the capture of the same plate exceeds the Time limit plus the Grace period.
- *Applicable days.* Days of the week when the time limit is enforced. You can select a weekly time frame from the drop-down list: Always (7 days), Weekdays (Monday to Friday), Weekends (Saturday and Sunday), and Custom. To create a custom time frame, click on the days.
- *Applicable hours.* Select when the time limit is enforced. You can choose All day or Time range. To define a time range, click in the date picker field, and use the text field or the graphical clock to specify the time.

About multiple overtime violations

You can add multiple parking regulations to an Overtime rule to specify the maximum number of citations that can be issued to the same vehicle for the same offence. For example, let's say your overtime rule has two separate parking regulations defined (of differing time limits if required). If a vehicle exceeds the first parking time limit an overtime hit occurs. If the same vehicle remains parked and subsequently exceeds the second parking time limit, a second overtime hit occurs. If the same vehicle still remains parked a third overtime hit will not occur.

By default, Patroller keeps reads associated to an overtime rule for 12 hours. Therefore, if the next day the vehicle is still in the same spot, and exceeds the parking time limit, an overtime hit will occur. To change the reset time of overtime rules, see the Patroller Config Tool setting *LinkReadPersistenceDuration* (see "Overtime" on page 352).

Parking lot

The *Parking lot* tab defines the parking zone where this parking rule must be enforced. The Parking lot tab displays a Bing map, on which you can add a parking lot, define the number of spaces in the lot, and then draw a polygon on top of the map to represent the physical parking lot. The number of spaces in the lot is used to calculate the percentage of parking occupancy in that area. For more information on how this information is being used, see "Zone occupancy report" in *Genetec Security Desk User Guide.*

NOTE This applies only to AutoVu Patroller University Parking applications.

You can add multiple lots to a map.

Parking facility

The *Parking facility* entity defines a large open parking area or a parking garage as a number of sectors and rows for the purpose of tracking the location of vehicles inside that parking facility. It is used in the AutoVu Mobile License Plate Inventory (MLPI) application.

The license plate inventory is the list of vehicles present in a parking facility within a given time period.

Before AutoVu MLPI units (mobile Patrollers and handheld devices) can collect license plates for the inventory, you must define their collection route as a sequence of sectors and rows configured in the parking facility. The sector and row where a license plate is read represents the location of the vehicle inside the parking facility.

Security Center collects license plate reads from the MLPI units and creates an inventory for the current date. Using Security Desk, you can find where a vehicle is parked (sector and row) and how long it has been parked there in the current inventory. You can also compare two inventories on different dates to view the vehicle movements (vehicles that were arrived, moved, or left).

System: AutoVu IP license plate recognition

Task: LPR – Parking facilities

	Identity	Name, description, logical ID, and relationships of this entity with other entities in the system.
	Properties	Assigns an LPR Manager to this entity and configures its sectors and rows.
	Custom fields	Custom field values for this parking facility.

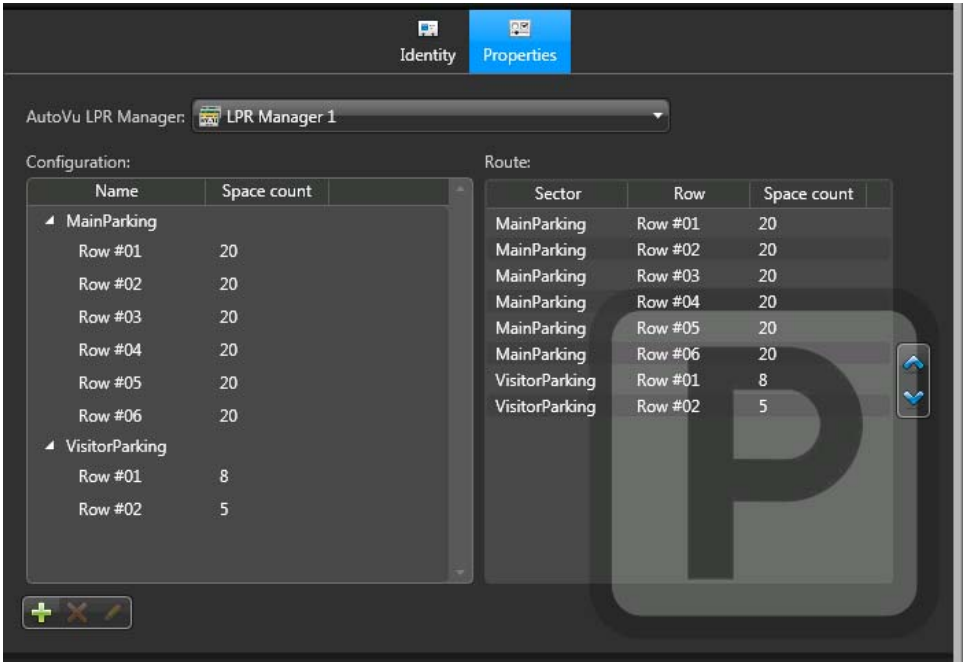
Related topics:

- "Patroller" on page 330

Properties

The *Properties* tab is used to assign an LPR Manager to the parking facility and configure its sectors and rows for the license plate collection route.

For more information on how to configure parking facilities, see "Configuring parking facilities in Security Center" on page 257.



- **AutoVu LPR Manager.** Select the LPR Manager responsible for creating and managing the license plate inventory for this parking facility.

  Only offloads from MLPI Patrollers managed by the same LPR Manager are used to build the inventory for this parking facility. An MLPI Patroller offload can include the vehicle inventory for multiple parking facilities, but only the reads tagged for this parking facility are used to build the inventory.

  IMPORTANT Make sure to set a *Read retention period* for the LPR Manager (see "General settings" on page 286) that is long enough for the period of time you want to keep your inventories.

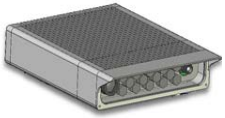
- **Configuration.** List of sectors, rows, and space count of the parking facility. The parking space of a parking facility is divided into sectors (or levels in the case of a parking garage) for ease of reference. Each sector contains *x* number of rows, and each row contains *x* number of spaces. You can configure Patroller to trigger an alarm (sound or warning message) if the reads collected during your sweep of a row exceed the space count for that row.

- **Route.** License plate collection route to be followed by the MLPI units responsible for collecting the license plates for the inventory. The route is downloaded by the Patrollers and handheld devices assigned to this parking facility.

  Only one route may be defined per parking facility, but each MLPI device can start its sweeping round at a different point in the route. The route forms a closed circuit.

  New sectors and rows are added to the end of the route by default. You can change the order of sector-rows in the route using the  and  buttons.

LPR unit



An *LPR unit* is an IP-based license plate recognition (LPR) device. An LPR device converts license plate numbers cropped from camera images into a database searchable format. Typically, an LPR unit includes two cameras: an LPR camera that produces high resolution close-up images of license plates; and a context camera that produces a wide-angle color image of the license plate and the vehicle.

AutoVu Sharp is the LPR unit used in Security Center AutoVu solutions. The Sharp includes license plate capturing and processing components, as well as digital video processing functions, enclosed in a ruggedized casing. Sharps can be deployed in mobile and fixed installations. A mobile installation is where the Sharp is mounted on a vehicle and is integrated into AutoVu Patroller (the in-vehicle software of the AutoVu LPR system), which in turn is integrated into Security Center. A fixed installation is where the Sharp is mounted in a fixed location, such as on a pole, and integrated directly into Security Center.

The LPR Manager automatically detects Sharps on the network and adds them to the Security Center system. It detects mobile Sharps through the AutoVu Patroller system they are connected to. It detects fixed Sharps directly through the Security Center discovery port.

System: AutoVu IP license plate recognition

Task: Role view (under the LPR Manager roles and Patrollers)

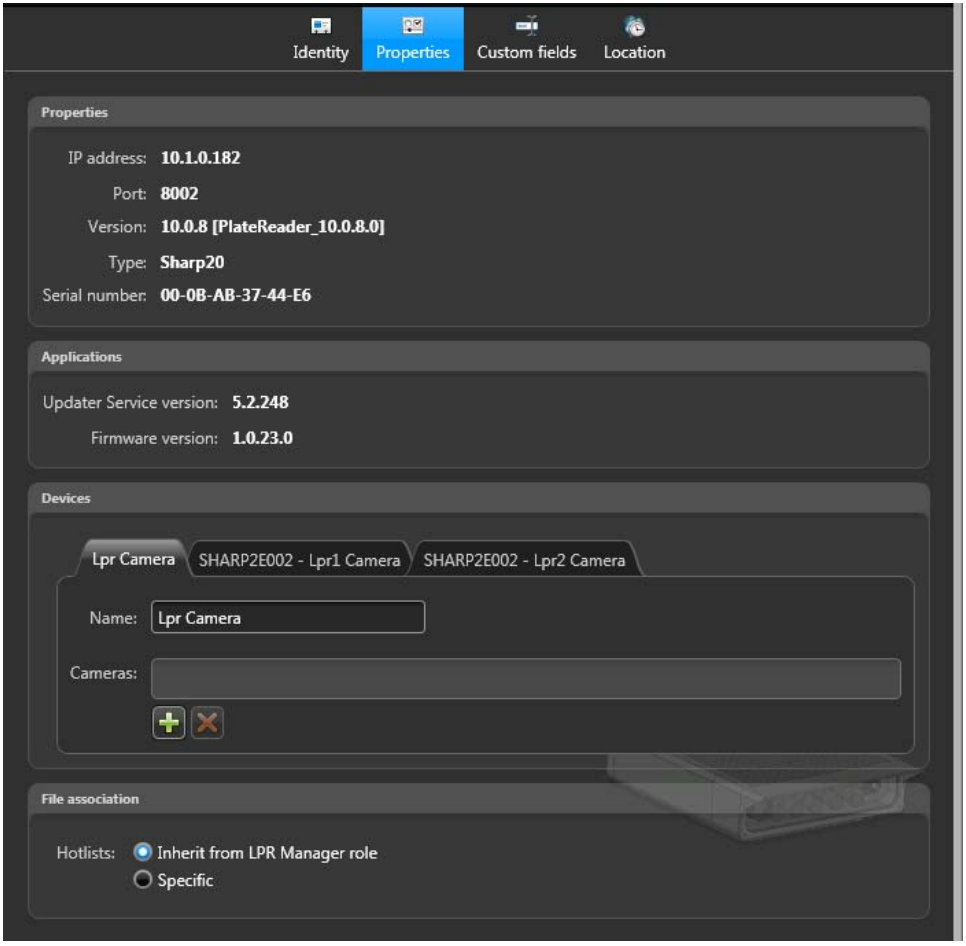
	Identity	Name, description, logical ID, and relationships of this entity with other entities in the system.
	Properties	Unit properties such as manufacturer, model, firmware version, network settings, and authentication password.
	Custom fields	Custom field values for this LPR unit.
	Location	Time zone and geographical location of this unit.

Related topics:

- "LPR Manager" on page 284
- "Patroller" on page 330

Properties

The *Properties* tab displays hardware and software information about the Sharp unit, such as the IP address and port being using. You can also associate a specific hotlist to the Sharp, or link the LPR camera in the Sharp to an Omnicast camera, or the Sharp's own context camera.



- **Properties.** Displays hardware and software information about the Sharp unit:
  - *IP address.* IP address of the Sharp unit.
  - *Port.* Port used by the LPR Manager to communicate with the Sharp unit.
  - *Version.* AutoVu PlateReaderServer software version running on the unit.
  - *Type.* Unit hardware version.
  - *Serial number.* Unit factory installed serial number.

- **Applications.** Displays which Updater service and Firmware versions are running on the Sharp.
- **Devices.** Link the LPR camera to an Omnicast camera.
- **File association.** Select how the Sharp behaves with hotlists:
  - *Inherit from LPR Manager role.* The Sharp uses the hotlists associated with its parent LPR Manager. This is the default setting.
  - *Specific.* Associate specific hotlists with the Sharp unit. This allows you to create Event-to-actions in Security Desk that trigger on that specific hotlist. For example, if you're using the Sharp to allow access to a parking lot, you would put the vehicle plates on a hotlist, and then associate that hotlist to the Sharp.

NOTE To reboot a fixed Sharp, click the **Reboot** button found on the *Contextual command toolbar* at the bottom of the Config Tool window. If the Reboot button is not visible, log on to the Sharp Portal's Configuration page, and then select *Accept remote reboot requests* (see "Extension" on page 379).

Patroller

A *Patroller* entity represents the in-vehicle software that runs on board a mobile data computer (MDC). It verifies license plates captured by LPR units mounted on the vehicle against lists of vehicles of interest and vehicles with permits. It also collects data for time-limited parking enforcement. The *Patroller* interface alerts users of license plates matching the above rules so that immediate action can be taken.

System: AutoVu IP license plate recognition

Task: Logical view, or LPR – Units (under LPR Manager)

Identity	Name, description, logical ID, and relationships of this entity with other entities in the system.
Properties	Assigns an LPR Manager to this entity and configures its sectors and rows.
Custom fields	Custom field values for this Patroller.
Location	Time zone and geographical location of this unit.

Related topics:

- "LPR unit" on page 327

Properties

The Properties tab displays information about the computer hosting the Patroller entity (you cannot edit the Patroller properties). You can also configure sound management, acknowledgment buffer settings, and a hit delay for the Patroller unit.

TIP Use the **Copy configuration tool** to copy these settings to another Patroller entity. For more information on the Copy configuration tool, see the Security Center Administrator Guide.

- **Properties.** Lists the properties of the Patroller in-vehicle computer.
  - *IP address.* IP address of the Patroller computer.
  - *Version.* Version number of the Patroller application.
  - *Type.* Patroller installation type(s).
  - *Serial number.* Serial number of the Patroller.
  - *Machine name.* Name of the Patroller computer.
- **File association.** Select how the Patroller behaves with hotlists and/or permit lists:
  - *Inherit from LPR Manager role.* Patroller uses the hotlists and permit lists associated with its parent LPR Manager. This is the default setting.
  - *Specific.* Associate specific hotlists or permit lists with the Patroller unit rather than the LPR Manager. If you later want to move the Patroller entity to another LPR Manager on your system, the hotlist or permit list will follow.
- **Sound management.** Configure Patroller to play a sound when reading a plate and/or generating a hit, and choose whether sounds should be played even when Patroller is minimized.
  - *Play sound on hit.* Plays a sound when Patroller generates a hit.
  - *Play sound on read.* Plays a sound when Patroller reads a plate.
  - *Play sounds even when minimized.* Play sounds even if the Patroller window is minimized.
- **Acknowledgment buffer.** Specify a buffer restriction that limits how many hits can remain unacknowledged (not accepted or rejected) before Patroller starts automatically rejecting *all* subsequent hits. You can also choose (by priority) which hotlists should comply with this restriction.
  - *Reject count.* How many unacknowledged hits are allowed.
  - *Reject priority.* When you create a hotlist entity, you can specify a priority for that hotlist. This setting tells Patroller which hotlist(s) should comply with the buffer restriction.
- **Hotlist.** Specify the *Duplicate hit delay* that tells Patroller to disregard multiple hits on the same plate for the duration of the delay. For example, if you set a delay of 10 minutes, no matter how many times Patroller reads the same plate during those 10 minutes, it will generate only one hit.

  NOTE If you are using Patroller 6.0 or later, this setting is applicable for permits as well.

User

The *user* entity identifies a person who can use Security Center applications and defines the rights and privileges that person has on the system. Each user is assigned a username and a password, which are that person's credentials to log on to the system.

While the *user privileges* limit the range of activities a user can perform on the system, the partitions limit the range of entities the user can exercise his/her privileges on.

A user can be a member of one or more *user groups*. Users can inherit the privileges and the access rights from their parent user groups.

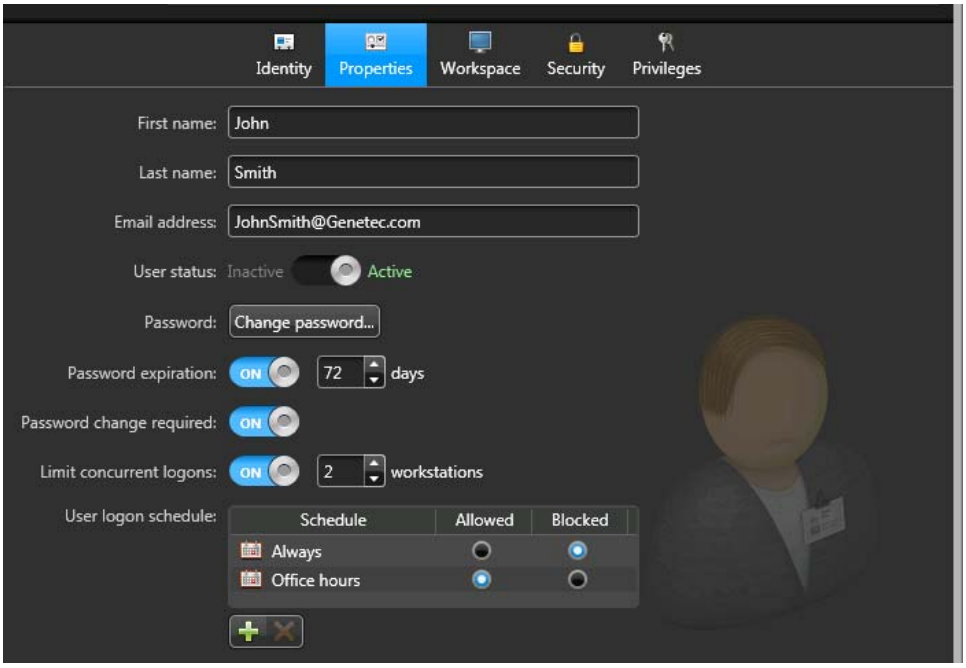
System: General

Task: Security – Users

	Identity	Name, description, logical ID, and relationships of this entity with other entities in the system.
	Properties	User's general profile.
	Workspace	User's default Security Desk workspace configuration.
	Security	User's security profile.
	Privileges	User's privileges.
	Custom fields	Custom field values for this user.

Properties

The *Properties* tab lets you configure the user's general profile.



First name, last name, email address

The personal information of the user can be imported from your company's directory service.

TIP The email address can be used to send emails or to email reports to the user via *Send an email* and *Email a report* actions.

User status

Use this switch to activate or deactivate the user profile. A user cannot log on when their profile is deactivated. Deactivating a user's profile while the user is logged on will immediately log off the user.

Password

Administrators and users that have the *Change own password* user privilege can change their password.

Password expiration

You can configure a user's password to expire after a certain number of days. The system automatically warns users whose password is expiring soon, and gives them a chance to set a new password immediately. You can set the password expiry notification period to between 0 and 30 days.

If you see that your password is going to expire soon, but do not have the *Change own password* user privilege, contact your administrator so they can change your password.

Password change required

You can configure Patroller and/or Security Desk to require a password change the next time the user tries to log on. Users must have the proper privilege to change their own passwords.

Limit concurrent logons

You can limit the number of different workstations a user can log on at the same time. This limit only applies to Security Desk. Config Tool is not restricted by this setting.

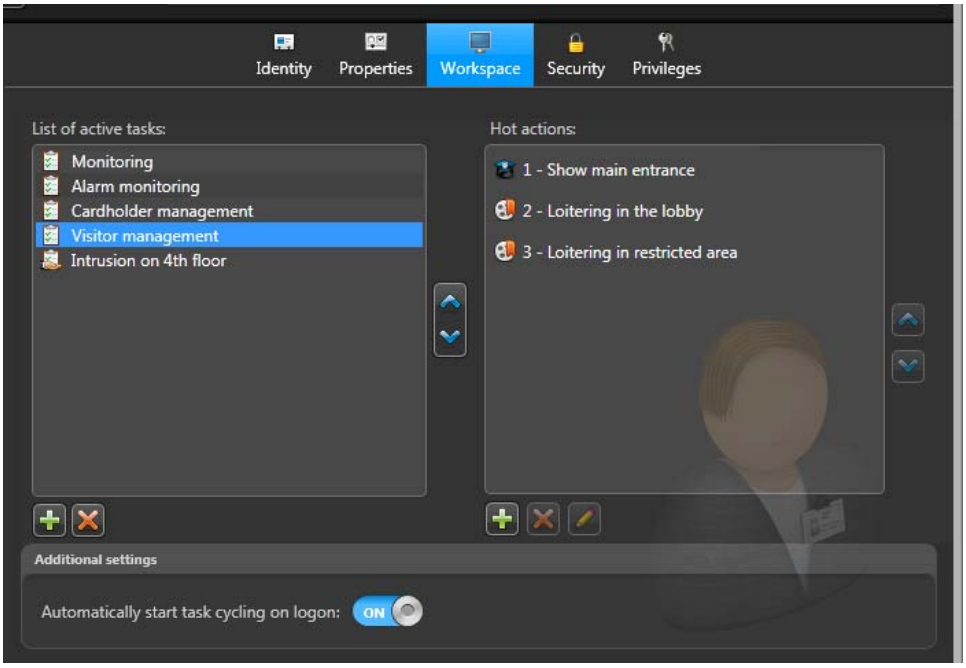
User logon schedule

You can restrict the user logon according to schedules. A schedule can either be used to allow user logon or to block user logon.

When multiple schedules are being used, the schedule conflict rules apply. When two schedules with the same priority level overlap, the blocking schedule has priority over the allowing schedule.

Workspace

The *Workspace* tab lets you configure the user's Security Desk workspace.



List of active tasks

This list shows the tasks found in the user's active task list. Users can save their task list using the *Save workspace* (Ctrl+Shift+S) command found in the Security Desk command menu.

Hot actions

This list shows the hot actions mapped to the PC keyboard function keys (Ctrl+F1 through Ctrl+F12) when this user is logged on to Security Center via Security Desk.

The user configures his hot actions via the Monitoring task. For more information, see "Working with hot actions and alarms" in the *Security Desk User Guide*.

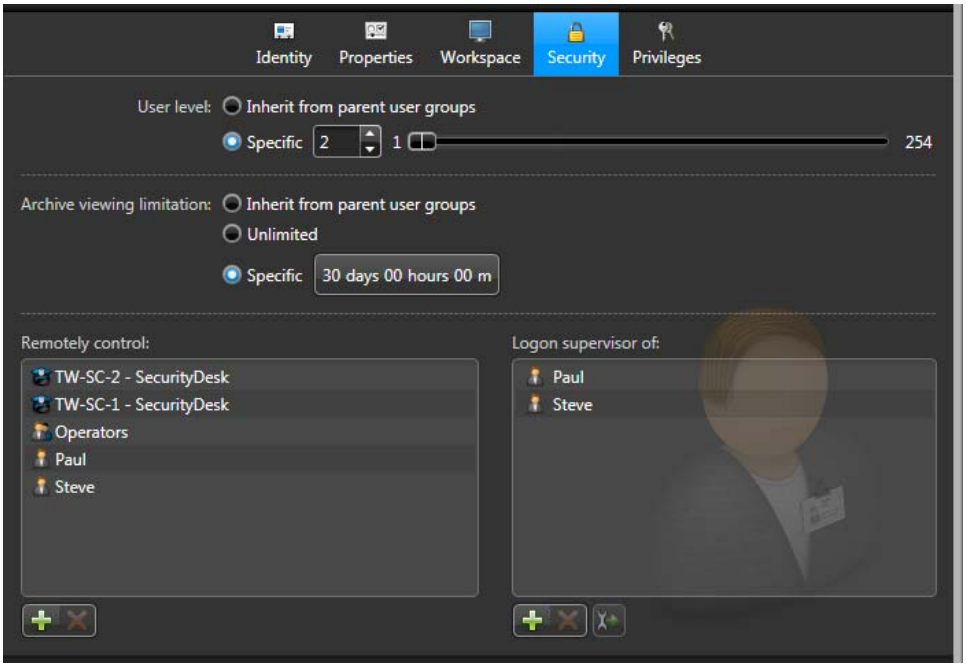
Additional settings

Turn on the switch *Automatically start task cycling on logon* so the next time the user logs on via Security Desk, task cycling will start automatically.

TIP To prevent users from stopping the task cycling once the Security Desk is open, deny them the *Start/stop task cycling* privilege. There are many more privileges that are designed to help the users focus on their tasks.

Security

The *Security* tab lets you configure the user's security profile.



User level

User levels affect three things in Security Center:

- They determine which user has priority over the PTZ controls of a camera when two or more users are trying to take control of the same camera at the same time.

  Priority is always given to the highest level user (1=highest). If two competing users have the same user level, it is decided on a first come first served basis.

  Once a user gains control over a PTZ camera, it is locked by that user. This means no other users can take control of that camera unless they have a higher user level. The control over the PTZ camera is automatically relinquished after 5 seconds of inactivity.
- They determine which users are logged out of the system when a threat level is set. For example, if you configure a threat level to trigger the *Set minimum user level* action, when the threat level is set, users with a lower user level than the one you specified are logged out.
- They determine which users can continue viewing a video stream when a camera is blocked in Security Desk. When you block a camera, users that have a lower user level than the one you specified can no longer view the video stream.

  For more information about blocking cameras, see "Blocking/unblocking cameras" in the *Security Desk User Guide*.

Level 1 is the highest user level, with the most privileges. The user level can be inherited from a parent user group. If the user has multiple parents, the highest user level will be inherited. If the user has no parent, the lowest user level (254) will be inherited.

Archive viewing limitation

This parameter serves to restrict the user's ability to view archived video to the last *n* days.

This limitation can be inherited from a parent user group. If the user has multiple parents, the most restrictive limitation will be inherited. If the user has no parent, no restriction will be imposed.

Remotely control

This section lists the Security Desk workstations that this user is allowed to control remotely in order to display entities. This list applies to both the Security Desk workstations you can connect to and control using the *Remote* task in Security Desk, and the Security Desk monitors that you can control using a CCTV keyboard.

NOTE Every monitor controlled by the Security Desk is assigned a unique monitor ID (displayed in the notification tray). Using a CCTV keyboard, you can display an entity on a remote Security Desk workstation by specifying its monitor ID, tile ID, and the logical ID of the entity you want to display. The Security Desk workstation monitors available on your system are listed in the Logical ID tab of the System entity. Select *Monitors* from the drop-down list to see them all. For each Security Desk workstation, the first monitor is called A, the second monitor B, and so on.

You can specify which workstation can be controlled using one of following methods:

- **User.** Any Security Desk workstation where that user is logged on can be remotely controlled.
- **User group.** Any Security Desk workstation where a member of that user group is logged on can be remotely controlled.
- **Application.** The specified workstation (*COMPUTER - SecurityDesk*) can be remotely controlled, regardless of who is logged on.

For more information, see "Remote monitoring" and "Connecting to remote Security Desks" in the *Security Desk User Guide*.

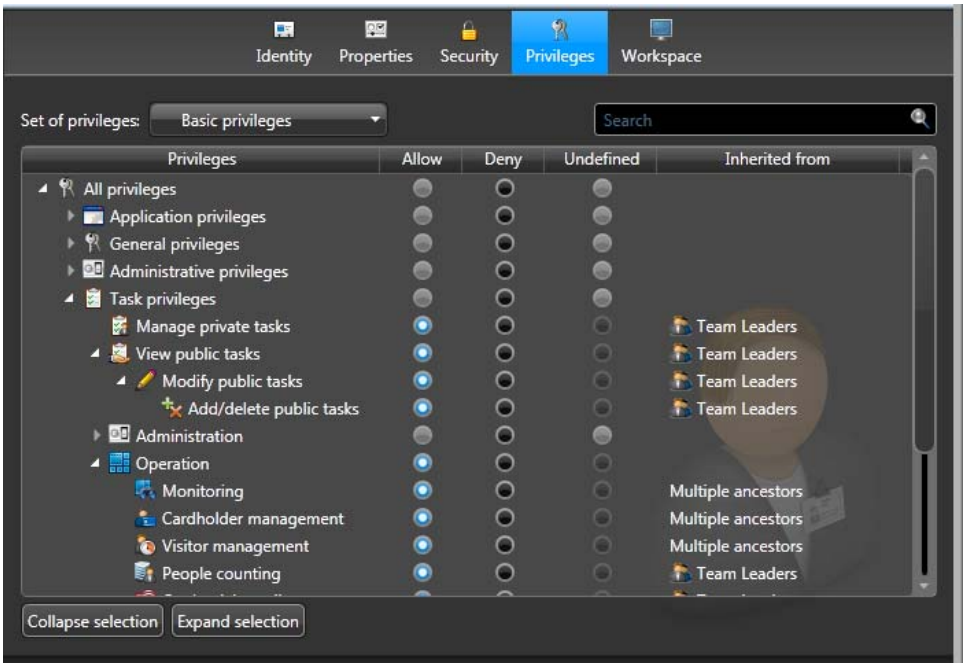
Logon supervisor of

This section lists the users whose logons are supervised by this current user. This means that when a user in this list needs to log on to the system, the current user must also provide his/her username and password in order to complete the logon.

A user can have more than one logon supervisor. For more information, see "Connecting to Security Center – Log on with supervision" in the *Genetec Security Desk User Guide*.

Privileges

The *Privileges* tab lets you view and configure the user's privileges.



Set of privileges

Use this drop-down list to select the set of privileges to view and edit. A user can have many sets of privileges. Each user has the *Basic privileges* set, plus one for every partition he/she is an accepted user of. Regarding access to entities contained in that partition, partition privileges supercede basic privileges.

User group

The *user group* entity describes a group of Security Center *users* who share common properties and privileges.

By becoming a member of a user group, a user automatically inherits all the properties of that group. This approach simplifies the configuration of users on large systems.

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

System: General

Task: Security – User groups

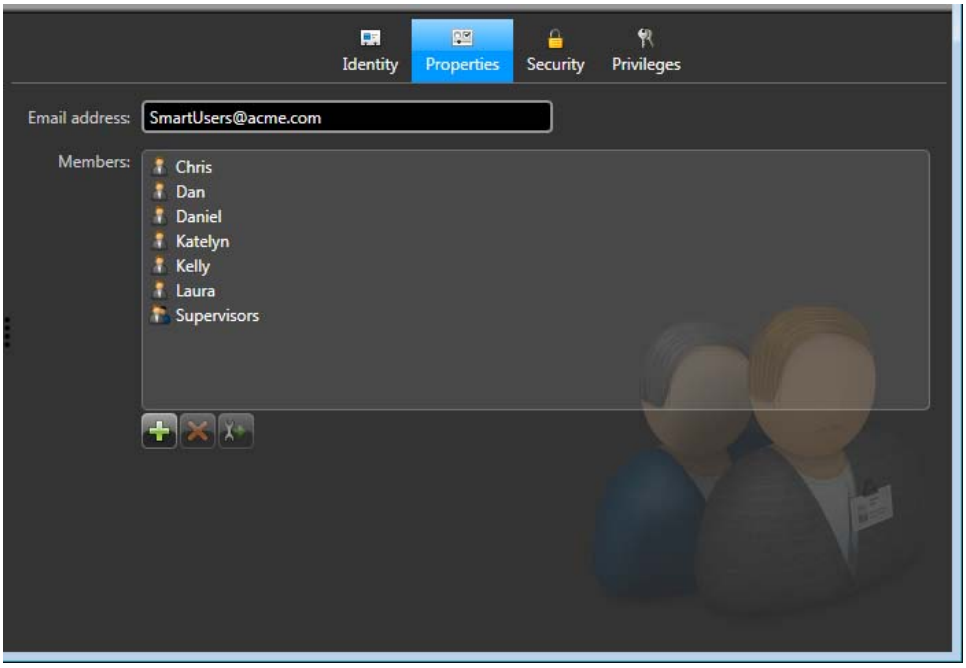
	Identity	Name, description, logical ID, and relationships of this entity with other entities in the system.
	Properties	User group's common email address and members.
	Security	User group's security attributes than can be inherited by its members.
	Privileges	Privileges that can be inherited by the group members.
	Custom fields	Custom field values for this user group.

Related topics:

- "User" on page 332

Properties

The *Properties* tab lets you view and configure the members of the user group.



Email address

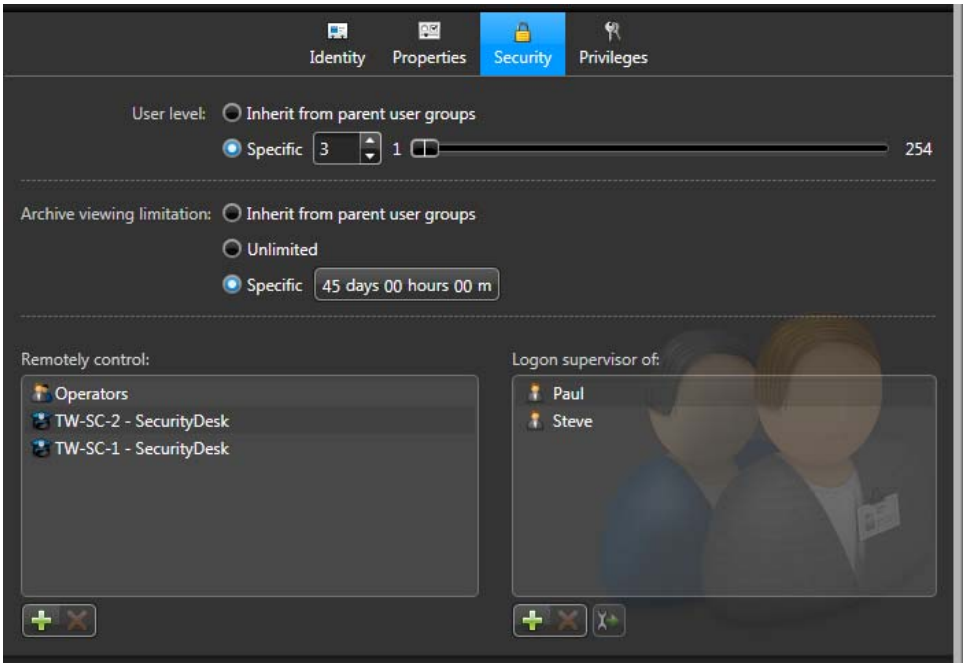
The email address you set for a user group should be a group address that is used by all members of the group. This information can be imported from your company's directory service.

Members

List of user group members. The members inherit by default the rights to partitions and the privileges of the user group. The email address can be used to send emails or to email reports to users via *Send an email* and *Email a report* actions.

Security

The *Security* tab lets you configure common security attributes for the group members.



Security attributes can be inherited by the members of the user group, and can themselves be inherited from other user groups.

User level

User levels affect three things in Security Center:

- They determine which user has priority over the PTZ controls of a camera when two or more users are trying to take control of the same camera at the same time.

  Priority is always given to the highest level user (1=highest). If two competing users have the same user level, it is decided on a first come first served basis.

  Once a user gains control over a PTZ camera, it is locked by that user. This means no other users can take control of that camera unless they have a higher user level. The control over the PTZ camera is automatically relinquished after 5 seconds of inactivity.
- They determine which users are logged out of the system when a threat level is set. For example, if you configure a threat level to trigger the *Set minimum user level* action, when the threat level is set, users with a lower user level than the one you specified are logged out.
- They determine which users can continue viewing a video stream when a camera is blocked in Security Desk. When you block a camera, users that have a lower user level than the one you specified can no longer view the video stream.

For more information about blocking cameras, see "Blocking/unblocking cameras" in the *Security Desk User Guide*.

Level 1 is the highest user level, with the most privileges. The user level can be inherited from a parent user group. If the user group has multiple parents, the highest user level will be inherited. If the user group has no parent, the lowest user level (254) will be inherited.

Archive viewing limitation

This parameter serves to restrict this user group members' ability to view archived video to the last *n* days.

Remotely control

This section lists the Security Desk workstations that the members of this user group are allowed to control remotely in order to display entities. This list applies to both the Security Desk workstations you can connect to and control using the *Remote* task in Security Desk, and the Security Desk monitors that you can control using a CCTV keyboard.

NOTE Every monitor controlled by the Security Desk is assigned a unique monitor ID (displayed in the notification tray). Using a CCTV keyboard, you can display an entity on a remote Security Desk workstation by specifying its monitor ID, tile ID, and the logical ID of the entity you want to display. The Security Desk workstation monitors available on your system are listed in the Logical ID tab of the System entity. Select *Monitors* from the drop-down list to see them all. For each Security Desk workstation, the first monitor is called A, the second monitor B, and so on.

You can specify which workstation can be controlled using one of following methods:

- **User.** Any Security Desk workstation where that user is logged on can be remotely controlled.
- **User group.** Any Security Desk workstation where a member of that user group is logged on can be remotely controlled.
- **Application.** The specified workstation (*COMPUTER - SecurityDesk*) can be remotely controlled, regardless of who is logged on.

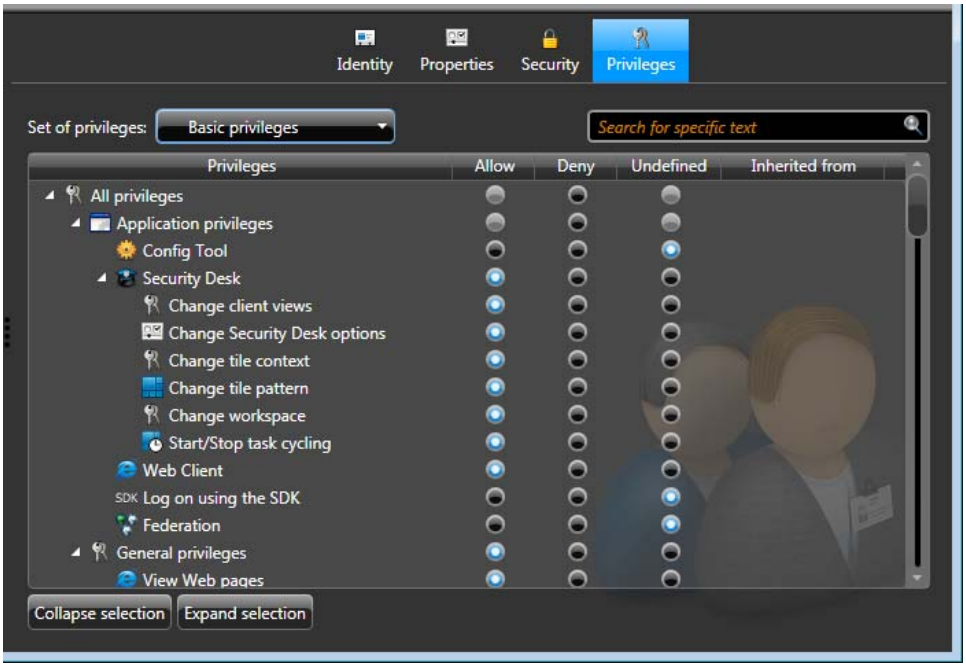
For more information, see "Remote monitoring" and "Connecting to remote Security Desks" in the *Security Desk User Guide*.

Logon supervisor of

This section lists the users whose logons are supervised by the members of this user group. This means that when users from this list need to log on to the system, any member of this user group can help them complete their logon.

Privileges

The *Privileges* tab lets you view and configure the user group's privileges.



The privileges of a user group are inherited by its members, and can themselves be inherited from other user groups.

Set of privileges

Use this drop-down list to select the set of privileges to view and edit. A user group might have many sets of privileges. Every one has the *Basic privileges* set, plus one for every partition the group is an accepted user of. Regarding access to entities contained in that partition, partition privileges supercede basic privileges.

19

Patroller Config Tool reference

This section describes all the Patroller Config Tool options you can use to customize Patroller for your particular AutoVu system.

Many of the options described are not required for a typical AutoVu deployment. For more information on a typical deployment process, see "Deploying fixed AutoVu systems" on page 43, "Deploying mobile AutoVu systems" on page 46, and "Deploying Patroller Standalone systems" on page 49.

NOTE For a description of Patroller 6 Config Tool options, see the Patroller 6 Help and the *Patroller 6.1 Administator Guide*.

This section includes the following topics:

General

The **General** settings page allows you to configure basic Patroller options such as the Patroller unit's name, how users should log on, etc.

NOTE Patroller Standalone is not connected to Security Center, therefore for some settings it's indicated that they are not applicable for Patroller Standalone and those settings do not appear in Patroller Config Tool.

Setting	Description
Patroller name	Enter the name of the Patroller unit as you want it to be seen in Patroller, Security Center, and Security Desk. NOTE The following notes apply only to the Patroller application that is connected with Security Center not Patroller Standalone • The Patroller name is **not** the same as your Security Center username. You log on to Patroller with your *Security Center* username. You create a Security Center username in Security Center Config Tool when you create a User entity. The Patroller name you create here is the name of the Patroller unit or vehicle as it will appear in Security Center Config Tool and Security Desk. For more information on creating users and user groups, see the Security Center Config Tool product help. • The Patroller name is detected automatically when you connect Patroller to Security Center (see "Security Center" on page 359). It will appear as a Patroller entity under the LPR Manager.
Logon type (not available for Patroller Standalone)	Select how to log on to Patroller: • **No logon.** No username or password required. • **Windows logon.** If the username logged on to Windows matches a username contained in the *Users* file downloaded to Patroller, you won't be asked for a username or password; Patroller will simply open. • **Secure name.** Only the Patroller user's Security Center username is required. • **Secure name and password.** The Patroller user's Security Center username and password are required. Note You create usernames and passwords in Security Center Config Tool when configuring users and user groups.
SQL Server	The address and name of the SQL Server.
Database name	You can leave the default database name, or change it to whatever you want. You can change this name at any time to create a new database.

Setting	Description
Use Windows authentication	• Turn this setting on to use your Windows credentials to connect to the database. • Turn this setting off to use the specific User ID and Password you specified during Patroller installation to connect to the database. NOTE Your username and password are part of the database Connection string.
User ID	The User ID to connect to the Patroller database. This User ID was entered during Patroller installation.
Password	The password to connect to the Patroller database. This password was entered during Patroller installation.
Advanced	• **Max logout.** Set the amount of time (in hours) that a user can be logged out and still resume their shift when logging back on. When this period has elapsed, or if a different user logs on, the system sees this as the start of a new shift and the data presented to the user reflects that. A value of 0 deactivates this feature, meaning that a new shift begins any time a user logs in. The default logout time is 4 hours. • **Store reads for.** Set the amount of time that reads are stored in the Patroller database. Reads older than this value are deleted from the database at the start of the next shift. The default storage time is 96 hours. • **Store hits for.** Set the amount of time that hits are stored in the database. Hits older than this value are deleted from the database at the start of the next shift. The default storage time is 120 hours. • **Record search.** Set the amount of time that records (reads or hits) are searchable by the Patroller user. Records older than this value will no longer be searchable at the start of the next shift. The default search time is 48 hours. • **Record display.** Set the amount of time that a record can be displayed. The default time is 12 hours. • **Folder path.** Type the folder path where the database files are created and replicated. • **Offload query timeout.** Define the timeout duration for the offload queries. The default timeout is 1800 seconds. • **Connection string.** The string to connect to the Patroller database. You shouldn't need to configure this option since SQL is installed automatically, or an existing SQL instance is used when you install Patroller. If you selected *SQL Server and Windows Authentication (mixed mode)* when you installed Patroller, you can see the *User ID* and *Password* you selected in this string.
Test connection	Test the connection to the Patroller database with the options selected.

Cameras

The **Cameras** page allows you to add Sharp camera units to your network, and configure basic settings related to Patroller's interaction with the Sharp cameras. You can also enable Sharp analytics, which provide information on vehicle speed, relative motion, and more.

This section includes the following topics:

Units

Setting	Description
Units	These are the Sharp units connected to your in-vehicle LAN. • **Add a Sharp** (). Manually add a Sharp camera unit to the network. Do the following: ▪ You'll need to enter the Sharp unit name. This is the IP address of the Sharp (for example, 192.168.10.1 for a SharpX). You also need to specify the camera's orientation, meaning where it's installed on the vehicle (front right, front left, and so on). ▪ If you're using a *SharpX - Multi* system, the "unit" corresponds to a single processor on the LPR Processing Unit, which controls two SharpX cameras. Add your second camera as "Lpr Camera 2" (case-sensitive). • **Remove a Sharp** (). Remove a Sharp camera from the network. • **Edit a Sharp** (). Edit the Sharp's connection settings to Patroller. • **Configure the Sharp** (). Opens the Sharp Portal in a web browser so you can configure the Sharp's properties. • **Start discovery.** Automatically detect installed Sharp cameras and add them to the network. You will still need to specify each camera's orientation (front right, front left, and so on). This is the preferred method of adding Sharps to the network. For more information on how to add Sharp units to Patroller, see "Connect Sharp units to Patroller" on page 182.
Camera exposure on startup	Use the slider to set the initial value for the camera exposure control when you first login to the application.
Pause reads on startup	Turn on to have plate reading paused when you log on to Patroller.

Setting	Description
Discovery port	When you use the **Start discovery** option to auto-detect Sharp units on the network, Patroller will search for Sharps connected on this port. Default value is 5000. Note This discovery port must match the discovery port you set in the Sharp Portal for each Sharp (see "Configuration" on page 373).

Analytics

Sharp cameras can provide analytical information based on the license plate and context images they capture.

Setting	Description
Confidence score	The Sharp assigns a numerical value (from 0 to 100) to each license plate read. This value tells you how confident the Sharp is in the accuracy of the read.
Relative Motion	The Sharp can detect if the vehicle is getting closer or moving away.
Speed Estimation	Sharp cameras are able to estimate a vehicle's approximate speed. Note For a mobile AutoVu installation, the Patroller vehicle must be stopped for this feature to work.
Vehicle Make	Sharp cameras can recognize the make of certain vehicles. Vehicle make recognition is performed on a best-effort basis and is continually being updated. Note The Sharp must see the vehicle's logo for this feature to work.
Vehicle Type	Certain license plates include character symbols that identify specific vehicle types (for example, taxi, transport, and so on). The Sharp can read these symbols, and display the vehicle type along with the other read/hit information.

Operation

The **Operation** page allows you to configure options related to Patroller operation and enforcement.

This section includes the following topics:

General

Configure the general options that apply to all types of hits.

Setting	Description
Pause reads while enforcing	Turn on to pause Patroller plate reading while you're in the process of accepting or enforcing a hit.
Allow popup hit	Turn on for Patroller to display hits on screen as they occur. Turn off for hits to accumulate in the background.
First hit on top	Choose the order that hits are displayed. Turn on to display the oldest hit first (right side of the Patroller scrollbar). Turn off to display the latest hit first.
Enable plate editing	Turn on to allow editing of license plate characters when you receive a hit. From the hit screen, click or tap the plate text string to open the editor.
Text-to-speech voice (not available in Patroller Standalone)	Select the voice you want to use for notifications, such as when the Patroller vehicle is entering and exiting a zone and the name of the zone. Select **None** to disable the option. NOTE The voices that are available depend on your Windows operating system.

Hotlists

Configure hotlist-related options.

NOTE You set New wanted attributes and categories in Security Center Config Tool.

Setting	Description
Allow consecutive hits	Turn on to allow sequential hits for the same plate. For example, if you capture a plate that raises a hit, and then capture the same plate again, it will raise another hit. If you turn this setting off, Patroller would need to capture a new plate before allowing a hit for the same plate.
Enable new wanted	Turn on to allow Patroller users to add New wanted hotlist entries.
Enable new wanted management	Turn on to allow Patroller users to edit and delete New wanted entries from the database.
Enable comments for new wanted	Turn on to activate a text box in Patroller where you can enter a comment when entering a New wanted hotlist item.
New wanted expiry options (days)	Create the expiry option(s) available to the Patroller user when adding a New wanted entry. For example, let's say you create the options 1, 5, and 10. When you add a New wanted entry, you'll be able to choose for that entry to expire in 1, 5, or 10 days. If you don't provide an expiration option, New wanted entries will remain in the Patroller database indefinitely. • **Add expiration option** ( ). Enter an expiration option (in days). Maximum value is 100. • **Delete expiration option** ( ). Delete an existing expiration option.
Bypass hit enforcement	Turn on to bypass the additional step of enforcing a hit after accepting it. When turned on, Patroller assumes you enforced the hit, and will not display the Enforced/Not enforced prompt.
Auto-enforce hotlist hits	Turn on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction. Note If you're connected to Security center and you've configured "Hit accept" or "Hit reject reasons", they are ignored when this setting is on.
Display hits by priority	Turn on to display hits in Patroller by the priority you specified in Security Center Config Tool. If you are using Patroller Standalone, the hotlist priority is specified at the time you import the list in Patroller. For example, if you've set "Hotlist A" to a higher priority than "Hotlist B", hits generated from Hotlist A will be displayed first (on the right of the Patroller scrollbar).

Setting	Description
Use simple matcher	Turn on Simplematcher when using very large hotlists with millions of entries. You'll also need to turn off OCR equivalence. For more information, see "Manage large hotlists using Simplematcher" on page 127.

Permits

Enable and configure permits, shared permits (if applicable), and related options.

Setting	Description
Use permit	Turn on to enable the use of permits.
Bypass permit hit enforcement	Turn on to bypass the additional step of enforcing a hit after accepting it. When turned on, Patroller assumes you enforced the hit, and will not display the Enforced/Not enforced prompt.
Auto enforce permit hits	Turn on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction. NOTE If you're connected to Security Center and you've configured Hit reject reasons, they are ignored when you turn this setting on.
Use shared permit	(University Parking Enforcement only). Turn on to enable the use of shared permits.
Bypass shared permit hit enforcement	(University Parking Enforcement only). Turn on to bypass the additional step of enforcing a hit after accepting it. When turned on, Patroller assumes you enforced the hit, and will not display the Enforced/Not enforced prompt.
Auto enforce shared permit hits	(University Parking Enforcement only). Turn on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction. NOTE If you've configured Hit reject reasons, they are ignored when you turn this setting on.

Overtime

Enable and configure overtime enforcement, wheel imaging (if applicable), and related settings.

NOTE This tab is not available in Patroller Standalone.

Setting	Description
Use overtime	Turn on to enable the use of overtime rules.
Advanced	Click to configure the **Advanced overtime settings**: • **Link read persistence duration.** Enter the amount of time that a plate read stored in the Patroller database is considered to be a "time 1" read for a particular overtime rule. EXAMPLE Let's say you enter 8 hours, which is a typical Patroller's shift. You start your shift and select *OT_Rule1*. You do your first pass and read plate *ABC123* at 9:00 a.m. This is now "time 1" for the rest of the day (until 5:01 P.M.). Even if you close and restart Patroller, the "time 1" for plate *ABC123* for *OT_Rule1* will be 9:00 a.m. If you start Patroller after the duration (8 hours in this example), the 9:00 a.m. read is no longer considered to be a "time 1" read. • **Minutes to due vehicles.** Enter the amount of time before the vehicles are due for enforcement. This value determines the *Show Due* functionality in Patroller. The default is 5 minutes. • **Preferred Long Term Overtime zone.** If you have more than one Long Term Overtime zone configured in Security Center, you must type the name of the zone you want Patroller to display, since you can only enforce one zone at a time. This value is not case-sensitive. • **Enable logs.** Turn on to enable logs related to overtime enforcement. This option should only be used for troubleshooting and technical support, if required. • **Same position tolerance.** This is a buffer used for "Same position" overtime rules. It is the distance that Patroller considers to be a single position or parking space.
Bypass hit enforcement	Turn on to bypass the additional step of enforcing a hit after accepting it. When turned on, Patroller assumes you enforced the hit, and will not display the Enforced/Not enforced prompt.
Auto enforce overtime hits	Turn on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction. NOTE If you've configured Hit reject reasons, they are ignored when you turn this setting on.
Use tire images	Turn on to use wheel imaging. Wheel images are saved to the in-vehicle computer.

Setting	Description
Wheel imaging enforced	Select whether wheel imaging is enforced or not from the drop-down list: • **Mandatory.** The user is required to verify wheel images for both passes in order to enforce a hit. • **Optional.** The user can enforce a hit without verifying wheel images.
Tire cam-to-plate distance	Specify the distance (in meters) from the tire camera to the vehicle license plate when the car is parked. The default parallel distance is 4 meters, and the default 45 degree angle distance is 3 meters. For more information, see "Configure Patroller overtime settings" on page 245.
Maximum vehicle length	Specify the length of the longest vehicle that can be processed when the car is parallel parked. The default parallel distance is 11 meters, and the default 45 degree angle distance is 5 meters. For more information, see "Configure Patroller overtime settings" on page 245.
Distance travelled before saving	Specify the distance that must be travelled before saving a tire image when the car is parallel parked. The default parallel and 45 degree angle distance is 0.3 meters. For more information, see "Configure Patroller overtime settings" on page 245.

MLPI

Enable and configure options related to Mobile License Plate Inventory.

NOTE This tab is only available in MLPI mode.

Setting	Description
Enable read deletion	Allows you to delete the plate read from the information panel of the Patroller main window. This is useful to correct any mistakes before the plate data is offloaded. For example, if you have misreads, or did a sweep but specified the wrong location before you started, you can delete those reads before they are offloaded to Security Center. NOTE This only applies to plates that are read when an MLPI zone is selected.
Enable read modification	Allows you to modify plate numbers from the information panel of the Patroller main window. This is useful if a plate is misread and you want to correct it before offloading the data.

Setting	Description
Enable too many reads popup	Patroller will trigger an alarm (sound or warning message) if the reads collected during your sweep of a row exceed the number of spaces specified in the “Space count” for that row. NOTE You specify the “Space count” in the Parking facility rule in Security Center Config Tool.

Navigation

The **Navigation** page allows you to configure options related to Patroller location and movement, such as GPS functionality, map usage, etc.

This section includes the following topics:

GPS

Enable and configure GPS options.

Setting	Description
Use GPS	Turn on to activate communication with the GPS device. This setting applies to both the USB GPS antenna that connects to the in-vehicle computer, and to the GPS antenna that connects to the Navigator box and is used with odometry.
Device	Click in the field to open the **Select device** dialog box. Choose the appropriate USB device and click **OK** > **Apply**.
Baud rate	The speed of the GPS communications channel (serial port). The default value is 9600, but some USB GPS devices require a reduced speed of 4800. For example, if you're using Genetec's USB GPS antenna that connects to the in-vehicle computer (model number BU-353), you need to change this value to 4800.

Setting	Description
Advanced	• **Port.** Specify the COM port number of the GPS device as seen in Windows Device Manager. ▪ If you're using the USB GPS that connects directly to the in-vehicle computer, the name of the device in Device Manager is **Prolific USB-to-Serial Comm Port**. ▪ If you're using the GPS antenna that connects to the Navigator box, the name of the device in Device Manager is **u-blox 5 GPS and GALILEO Receiver**. • **GPS initialization string.** Displays the initialization commands to be sent to the GPS device when you login to the application. IMPORTANT This is a default firmware setting. Do not modify. • **Consecutive invalid strings before restart.** Specify the number of consecutive invalid GPS strings (can't detect GPS signal) allowed before the device is restarted. The default number is 10. IMPORTANT You should not need to change this setting. • **Noise.** Specify the noise value. If the distance from 0,0 to the GPS position is less than the value you define, no GPS event is generated. The default noise value is 5. IMPORTANT You should not need to change this setting.

Odometry

Configure the settings for the AutoVu Navigator box, which provides vehicle odometry data for more precise GPS readings. This is required if you are using Patroller for City Parking Enforcement with Wheel Imaging.

NOTE Patroller Standalone is not connected to Security Center, therefore for some settings it's indicated that they are not applicable for Patroller Standalone and those settings do not appear in Patroller Config Tool.

Setting	Description
Read when car is stopped	Specify whether or not to continue reading plates when the Patroller vehicle is stopped. When doing parking enforcement, Patroller vehicles may stop and reverse frequently.
Read when moving backwards	Specify whether or not to continue reading plates when the Patroller vehicle is in reverse. When doing parking enforcement, Patroller vehicles may stop and reverse frequently.
NavBox (not applicable for Patroller Standalone)	Turn this setting on to enable the Navigator box. NOTE If you're using the Navigator box for odometry as well as GPS, you also need to turn on the **Use odometry** option.

Setting	Description
Port (not applicable for Patroller Standalone)	Click **Detect port** to display the COM port number of the Navigator box device as seen in Windows Device Manager. Type the port number in the **Port** field. Note The name of the device in Windows Device Manager is *Silicon Labs CP210x USB to UART Bridge*.
Shutdown delay (not applicable for Patroller Standalone)	Specify the number of seconds to wait after the vehicle's ignition is turned off before shutting down the in-vehicle computer. To disable this feature, enter "0".
Use odometry (not applicable for Patroller Standalone)	Turn this setting on to enable the odometry capability of the Navigator box (you can use the Navigator box for GPS positioning only). Using odometry data increases GPS positioning precision (required for wheel imaging).
Use reverse (not applicable for Patroller Standalone)	Turn this setting on to reverse the odometry polarity to negative. When calibrating the Navigator box, you may encounter negative signal ticks from the vehicle's engine. This depends entirely on the make and model of the vehicle. If you see negative ticks while calibrating the Navigator box, use this option to reverse the polarity, which will display the ticks as positive.
Scale (not applicable for Patroller Standalone)	This value is provided by the IO Services software during Navigator box calibration. It is the number of wheel ticks (ticks) your Patroller vehicle generates per meter travelled.
Sensitivity (not applicable for Patroller Standalone)	This value is provided by the Navigator oscilloscope software during Navigator box calibration. This number adjusts the sensitivity of the Navigator box so it doesn't mistake random engine noise for real vehicle movement.

Maps

Enable and configure maps and related GPS options.

Setting	Description
Mapping type	Select the map type from the drop-down list: • **None.** Do not use maps. • **BeNomad.** The default map type for AutoVu. For more information, see "Install BeNomad files on the in-vehicle computer" on page 97.
Show vehicle route	Displays a trail behind the Patroller icon that allows you to see the route Patroller has taken. Turn this setting off to show only the Patroller's current position.

Setting	Description
GPS distance tolerance	Specify the distance (in meters) where a GPS match is almost 100% certain. For example, a value of 50 means that a location result from the GPS matcher is almost 100% accurate within 50 meters. The smaller the value, the more aggressive are the GPS matching location corrections. The default distance is 20 meters.
GPS odometry calibration tolerance	Specify the error in which the odometry calibration factor is correct with near 100% certainty. For example, a value of 0.4 means that it's almost certain that a calibration result from the GPS matcher is accurate within 40%. The smaller the value, the more aggressive the GPS odometry calibration corrections. The default tolerance is 0.4.
Max distance error	Specify the maximum distance error (in meters). If the distance between the vehicle and the closest map item is greater than this value, no snapping will occur.

Security Center

The **Security Center** page is where you configure how Patroller connects to Security Center.

NOTE This tab is not available in Patroller Standalone.

Setting	Description
Connect to Security Center	Turn on to connect Patroller to Security Center. This is required for all communication with the LPR Manager role. For example, you need to be connected to Security Center to do any of the following: • Send live updates to Patroller and connected Sharp cameras. • Send hotlist modifications using periodic transfer. • Send Patroller a new or modified hit accept survey. You also need to be connected to Security Center in order to offload LPR data wirelessly. For more information, see "Offload" on page 361. Note After you properly configure this setting, leave it on indefinitely. Patroller will connect to Security Center whenever a wireless connection is available (e.g. you are in range of the company WiFi network), and download any modifications or updates required.
IP address	Enter the IP address of the Security Center machine hosting the LPR Manager role.
Port	Enter the port number Patroller should use to connect to the LPR Manager role. Note You must *also* enter the same port number for the listening port in Security Center Config Tool. Go to the LPR Manager **Properties** page, and then under **Live**, enter the **Listening port** (see "Live" on page 288).
Encrypt communication channel	Turn this setting on if you want to encrypt communication between Patroller and Security Center. Note To use this feature, you must *also* encrypt communication in Security Center Config Tool. Go to the LPR Manager **Properties** page, and then under **Live**, select **Encrypt communication channel** (see "Live" on page 288).
Update provider port	Enter the port that Security Center uses to send hotfixes and other updates to Patroller and connected Sharp units. Note To use this feature, you must *also* enter the same port number for the listening port in Security Center Config Tool. Go to the LPR Manager **Properties** page, turn on **Update provider**, and then enter the **Listening port** (see "Update provider" on page 301).

Setting	Description
Live events	• **Hits.** Send hits live to Security Center. • **Reads.** Send reads live to Security Center. • **Unit position.** Send the position of the Patroller unit live to Security Center.
Periodic transfer	Specify how often hotlist and permit list changes are downloaded to Patroller (if you have a live connection). The default transfer period is every 240 minutes. Note You can disable Periodic transfer on specific hotlists (not permit lists) in Security Center Config Tool on the hotlist's **Advanced** page (see "Advanced" on page 308).

Offload

Offloading is how you transfer reads, hits, and other Patroller data to Security Center. Please note that if you're running Patroller Standalone (no connection to Security Center) your data is offloaded to a local *.Standalone* file on the in-vehicle computer.

NOTE Patroller Standalone is not connected to Security Center, therefore for some settings it's indicated that they are not applicable for Patroller Standalone and those settings do not appear in Patroller Config Tool.

Setting	Description
Offload method	Select your offload method: • **None.** Does not offload data. • **Local file.** You can configure Patroller to offload data to a file on the in-vehicle computer. ▪ If you are connected to Security Center: After you have offloaded the data, you can then copy the data to a USB key, and transfer it to the Security Center computer. ▪ If you are using Patroller Standalone: After you have offloaded the data, you can open the *Offload.Standalone* file in Internet Explorer to view the information or import the *.Standalone* into your own reporting tool. • **Live transfer (not applicable to Patroller Standalone).** This offload method transfers all data from the Patroller vehicle to Security Center using a wireless connection. For example, you can offload your data at the end of a shift, when you're in range of the company's wireless network. You also use this option to offload data to a network drive rather than your local drive on the in-vehicle computer. NOTE Please note the following about **Live transfer**: ▪ This option automatically transfers the offload data into the *Offload* folder under the LPR Manager root folder. For more information on the root folder, see "General settings" on page 286 ▪ If you try to offload without being connected to Security Center, the offload is done on your local in-vehicle computer. You can then transfer the offload data to Security Center with a USB key.
Local offload drive	If using **Local file** as your offload method, specify where on your machine the data should be saved (e.g. C:\ if you want to offload to your C drive). IMPORTANT Do **not** specify the folder. Patroller creates the offload folder on the drive you specify.
Use encryption (not applicable to Patroller Standalone)	Turn on to encrypt the offloaded data. You'll also need the Public key (not applicable to Patroller Standalone).

Setting	Description
Public key (not applicable to Patroller Standalone)	To encrypt offload data, Patroller needs the public key from the Security Center computer. Do the following: 1 On the Security Center computer, go to *C:\Program Files\Genetec Security Center 5.2*, and copy the *OffloadPublicKey.xml* file to your clipboard. 2 On the Patroller computer, go to *C:\Program Files\Genetec AutoVu X.Y\MobileClient*, and paste the *OffloadPublicKey.xml* in the folder. 3 In the **Public key** field, enter the path to the public key you just pasted to the Patroller computer (*C:\Program Files\Genetec AutoVu X.Y\MobileClient\OffloadPublicKey.xml).*
Offload events	This option allows you to choose which data you want to include in an offload. For example, you may only want to offload **Hits** to use less bandwidth when performing an offload.
Include all images	Turn on to offload all images. If this option is turned off, only images associated with a hit will be included in the offloaded data.
Incremental offload	By default, Patroller offloads data in increments, or segments. Turn this setting off if you want to offload the full data file each time.
Data segment size	Specify the maximum file size of each data segment (MB) when using Incremental offload. Once the offload file reaches the size limit, a new offload file is created and the offload process continues. The default maximum file size is 1 MB.
Force offload before exit	Turn on to make Patroller exit commands unavailable. The only way to close the application is to perform an offload. Note This option won't work if you set Offload method and Action after offload to **None**.
Action after offload	Select the exit procedure that occurs after you have performed an offload: • **None.** Return to the application. • **Exit.** MobileServer, MobileClient, and IO.Services are exited. • **Shutdown.** If the *PowerManagement.UsePowerManagement* option is selected, the OffloadExit setting is automatically set to **Shutdown**. This option does not work with laptops; choose **Exit** instead.
Delete after offload	Turn on to delete all records of user logins, images, hotlist hits, vehicles, unit states, street blocks, tire images, cameras, and attributes after a successful offload.

Plugin

The **Plugin** page is where you enable and configure AutoVu custom solutions. If you select **None**, no plugin settings are displayed.

NOTE Custom plugins are not included with a standard AutoVu system. They add functionality specifically designed for certain deployments. For more information on custom solutions, contact your Genetec representative.

Setting	Description
Street sweeper	• **AddTimeStampOverlay.** Turn Time Stamp overlay ON or OFF. • **CameraLogin.** Enter the camera login name. • **CameraPassword.** Enter the camera password. • **CameraServerName.** Enter the IP address of the camera. • **ImageParameterString.** Enter the desired resolution and rotation of the time stamp. • **OverviewImageDelay.** Enter the time delay between the plate read and the overview image up to a maximum of ten. • **TimeStampOverlayColor.** Select a color for the overlay. • **TimeStampOverlayFormat.** Format for the time stamp. • **TimeStampOverlayPosition.** Select the position of the overlay in the image. • **TimeStampOverlaySize.** Use the slider to increase or decrease the size of the overlay.
Scofflaw mdt	• **Plate type.** Displays the plate type with one letter. This is only for Philadelphia specifications. • **Queries path.** Displays the path on the local machine for storing text files with accepted hits.
Survey	• **Division.** Set this option to use a specific hit accept survey.

User interface

The **User interface** page allows you to configure options related to how the Patroller user interface looks and behaves, such as whether to highlight license plates in context images, and whether to enable printing of data, etc.

General

Configure the settings related to how Patroller is displayed.

Setting	Description
System unit	Displays speed and distance in metric or U.S. system (for example, km/h or mph).
Default plate state	Displays the default state or province when you enter a plate manually. NOTE You should enter the state's abbreviation (for example, NY, QC, and so on), not the full name.
Enable virtual keyboard	Turn on for Patroller to display an onscreen keyboard when you need to enter text. The onscreen keyboard appears when you tap or click in a text field.
Circle plate	Turn on for Patroller to circle license plates in the context images. To use this feature with a *SharpX - Mutli* system, you need to have a SharpX camera connected to the first interface of a camera interface pair. EXAMPLE Here are some possible scenarios for using plate circling with a *SharpX - Multi* system: • **One camera with a two-port system.** Use interface 1. • **One camera with a four-port system.** Use interface 1 or 3. • **Two cameras with a four-port system.** Use one of the following: ▪ Interfaces 1 and 2. ▪ Interfaces 1 and 3. ▪ Interfaces 3 and 4. • **Three cameras with a four-port system.** Use one of the following: ▪ Interfaces 1, 2, and 3. ▪ Interfaces 1, 3, and 4.
Show overview label	Turn on to display the overview label if the overview image exists.
Enable reviews	Turn on to allow users to review reads or hits in the Patroller user interface.

Setting	Description
Show plate lists indicator	Turn on to display the download status indicator in the Patroller notification bar. The indicator shows if there are: • Downloaded hotlist and permit lists • Downloads in progress • Download errors
Show plate lists on startup	Turn on to automatically display the list of downloaded files (hotlists and permit lists) when Patroller starts up.
Enable manual capture	Turn on to enable Manual capture in Patroller. This allows users to manually enter a license plate, and select the camera that captured it.

System

Configure the settings related to how Patroller behaves.

Setting	Description
Enable minimize button	Turn on to allow the Patroller window to be minimized.
Enable system tray menu	Turn on to enable the Patroller menu located in the Windows system tray (right-click the Patroller icon in the system tray for more options).
Start application minimized	Turn on to start Patroller with the window minimized. This option is not recommended if you log with a username and/or password.
Silent mode	Turn on to enable silent mode. In this mode, the Patroller window starts and stays minimized until a hit is generated. After acknowledging the hit, Patroller returns to a minimized state.
Enable main buttons	Turn on to enable the *Disabled, Hit, Zone, ShowDue, Manual Capture*, and *Cameras* buttons. NOTE For the Street Sweeper plugin, you need to disable this setting.
Show taskbar when fullscreen	Turn on to show the Windows taskbar when Patroller is full screen.
Enable printing	Turn on to enable printing of read/hit information from the Patroller window.
Show username in tray	Turn on to show the Patroller user's Security Center username in the notification bar. NOTE If you're using Patroller for parking enforcement, you can turn this option off to make room for long enforcement rule names.
Show Patroller name in tray	Turn on to show the Patroller's unit name in the notification bar. NOTE If you're using Patroller for parking enforcement, you can turn this option off to make room for long enforcement rule names.

Advanced

The **Advanced** page allows you to configure advanced Patroller options. Most AutoVu deployments do not require advanced options to be modified.

IMPORTANT Advanced settings in Patroller Config Tool are used mostly by Genetec for diagnostic, debugging, and testing purposes. There are only a few settings that you should attempt to modify yourself, and they are documented in this section. For all the other advanced settings, contact your Genetec representative before you attempt to modify them.

Hit

Setting	Description
Confirm real time	Turn on to require a confirmation of a hit status (*enforced*, *not enforced*) in the real-time mode.

User interface

Setting	Description
Log user actions	Turn on to monitor Patroller user activity such as selecting a camera, turning plate reading on and off, selecting a permit, and so on. Information is written to the *Patroller.exe.log* file located in the MobileClient folder.

20

Sharp Portal reference

This section describes all the Sharp Portal options you can use to customize a Sharp unit for your particular AutoVu system.

NOTE The settings shown in the Sharp Portal are different depending on what type of Sharp unit you are connecting to. For example, if you are connecting to a SharpX, you will see the number of available inputs on the LPR Processing Unit. That information is not displayed if you are connecting to a Sharp XGA.

NOTE For a description of Sharp 11 Portal options, see the Sharp 11 Help and the *Sharp 11 Administrator Guide*.

This section includes the following topics:

Status

The **Status** page displays information on the status of the Sharp unit you are connected to. You will find information such as the Sharp name, serial number, GPS coordinates (fixed Sharp), and license. The Status page is also where you can reboot the Sharp unit, and import or export diagnostic data.

This section includes the following topics:

Properties

Displays Sharp hardware information. This information is also on the printed adhesive label located under the Sharp visor or on the rear of the LPR Processing Unit (for SharpX).

Setting	Description
Name	Displays the Sharp unit name.
Serial number	Displays the Sharp hardware serial number.
Type	Displays the type of Sharp unit (Sharp XGA, SharpX, and so on).
Inputs	Displays the number of physical inputs on the SharpX LPR Processing Unit.
Relays	Displays the number of physical relay inputs on the SharpX LPR Processing Unit.
Version	Displays the date of the SharpOS update package.
GPS	Displays whether or not GPS is supported on a Sharp XGA (with attached GPS antenna).
Lens	Displays the unit lens depth available for context images and LPR images.
Illuminator	Displays the illuminator on the Sharp (for example, 850 nm)

Actions

Displays several actions you can perform.

Setting	Description
Reboot Sharp	Click to reboot the Sharp unit. You will be asked to confirm reboot. If you reboot the Sharp, you will lose connection to the Sharp Portal. Wait a few minutes for the Sharp to reboot, and then refresh the Web page to log on again.
File versions	Displays the file versions of the services running on the Sharp. You can use this information to confirm your Sharp is up to date.
Update	Click to update the SharpOS. You will be asked to provide a file that contains updates for the following: • Sharp firmware • Plate Reader • Updater Service • Web Updater For more information, see "Updating a Sharp unit using the Web Updater" on page 114.
Change password	Click to change the password you use to log on to the Sharp Portal. **Best practice:** You should always change the default password after you log on for the first time, *especially* if you configure the Sharp for HTTPS encryption. For more information on using HTTPS encryption, see "Portal Security" on page 374
Show Extension details	When you have an extension configured (see "Extension" on page 379), this will display information about that extension's status.
Free space on the disk	Click to free up space on the disk. IMPORTANT All reads and log files will be deleted.
Configure the other unit	If you are connected to a SharpX - Multi, this opens a new Sharp Portal window so you can configure the SBC (single board computer) that controls the other SharpX camera unit. For more information, see "AutoVu SharpX components" on page 4.

License

Displays whether or not the Sharp has a valid AutoVu license.

Setting	Description
Status	Displays if unit license is valid, invalid, or missing.

Diagnostics

You can import or export Sharp settings for use as diagnostic information by technical support (if required), or import settings from another Sharp.

Setting	Description
Export settings	Exports 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. Note You can only import settings from a similar Sharp (same model and SharpOS version). If you import settings from a SharpX you may have to restart the trunk unit for the cameras to be detected.

GPS coordinates

Displays the GPS coordinates for a fixed Sharp unit. The coordinates displayed are from the Sharp's GPS antenna (if applicable). If the Sharp is not equipped with a GPS antenna, the coordinates displayed are those you set in Config Tool (see "Location" on page 272).

If the coordinates are properly set, either in Config Tool, or by the Sharp's own GPS antenna (if applicable), you will have the option to view the Sharp's location on a map. You must have internet capability to view the map.

Setting	Description
Longitude	Displays the current GPS longitude coordinates if GPS functionality is supported.
Latitude	Displays the current GPS latitude coordinates if GPS functionality is supported.

Clock

The Sharp unit's internal clock.

Setting	Description
Status	Shows if there is a drift between the Sharp unit's clock, and the clock on the computer you are currently using to connect to the Sharp Portal. • **Local clock.** The clock on the computer you are using to connect to the Sharp Portal. • **Remote clock.** The Sharp unit's clock. • **Synchronize now.** Synchronizes the Sharp's clock with your computer's clock. IMPORTANT Do **not** click **Synchronize now** unless you are connecting to the Sharp Portal from the server (computer hosting the LPR Manager role). If you synchronize clocks with a computer other than the server, the Sharp's reads and hits will not have accurate timestamps. NOTE Note the following: • The Sharp unit automatically synchronizes clocks with its server every 12 hours, or whenever the connection between the Plate Reader and LPR Manager role is established. • For mobile AutoVu deployments, the Sharp must be in sync with the Patroller computer to ensure reads, hits, and overtime wheel images have the correct timestamps. If the sync is not successful, make sure that the time sync port is not blocked by the Patroller computer's firewall.

Firmware

Displays the current version of the components and indicates if an upgrade is required.

Setting	Description
Component	Lists the components of the Sharp.
Version	Displays the version of the component. Each component is marked by a colored indicator: • Green: No update required. • Red: Component firmware version must be updated. • Yellow: The component cannot be identified.

Services (Advanced mode only)

This field is only visible if you are logged on the Sharp Portal in Advanced mode. For more information on how to log on in Advanced mode, see "Log on to the Sharp Portal" on page 36.

Setting	Description
Genetec Sharp - Plate Reader	You can stop or start the Plate Reader service from here without having to go to the Windows Services menu.

System resources

Displays the status of the Sharp hardware.

Setting	Description
CPU	Displays the Sharp CPU usage. Note If you see two CPU bars in this section, it means you are connected to a Sharp unit that has a dual-core SBC (single board computer).
Usage (%)	The current CPU usage.
Memory	Displays the memory drives.
Free space (MB)	Displays the amount of free space left on the memory drives.
Total space	Displays the total space (in MB) available on the memory drives.
Used (%)	Displays how much percentage of memory is currently being used on each drive.

Configuration

The **Configuration** page is where you configure the Sharp unit. This is where you set the Sharp to use a static IP or DHCP, configure the Sharp Portal to use HTTPS encryption, select the Context (Oregon, Quebec, and so on), specify the read strategy (for example, slow or fast moving vehicles), and more.

This section includes the following topics:

Network settings

Configure the Sharp network settings.

Setting	Description
Mode	Click **Edit**, select a network setting mode from the drop-down list, and then click **Save**. You can select one of the following modes: • **DHCP.** Select this option if a DHCP server is available on the same network and you want it to assign an IP adress to the Sharp. When you are on a DHCP server with DNS capability, you will be able to connect to the Sharp using the Sharp name (for example, Sharp1234) rather than the IP address (for example, 198.162.10.100). EXAMPLE Select DHCP if you are configuring a SharpX system with a router in the vehicle. In this case, the router assigns the IP address. • **Static.** This is the default state of the Sharp, and is used in most situations. The default static IP addresses for the Sharps are: ▪ 198.162.10.100 (Sharp) ▪ 198.162.10.1 (SharpX SBC1) ▪ 198.162.10.2 (SharpX SBC2)
IP address	Enter the new IP address you want to assign to the Sharp unit.

Setting	Description
Subnet mask	If you changed the subnet when selecting a new static IP address, enter the new subnet mask.
Gateway	Enter the gateway.
Reserved range	(SharpX systems only) This setting changes dynamically depending on the static IP address you enter in the Mode section. It will automatically reserve up to nine IP addresses in sequence depending on the type of system you have. EXAMPLE If you have a SharpX - Multi with four camera units installed, you will need nine IP addresses to account for all the components. If you enter a static IP of *192.168.12.34*, you will get the following range: • **SBC1.** 192.168.12.34 • **SBC2.** 192.168.12.35 • **GVP1.** 0.0.0.0 • **GVP2.** 0.0.0.0 • **CAMU1 for SBC1.** 192.168.12.38 • **CAMU2 for SBC1.** 192.168.12.39 • **MPU.** 192.168.12.40 • **CAMU1 for SBC2.** 192.168.12.41 • **CAMU2 for SBC2.** 192.168.12.42 Note For SharpX - Multi systems, the offset (SBC1 or SBC2) is taken into account by the range. This means you only need to set the static IP address once (for SBC1 **or** SBC2). The system will know if you are configuring SBC2 instead of SBC1, and will reserve one address below to be assigned to SBC1 (192.168.12.34) so the IP range remains consistent.

Portal Security

Configure the Sharp Portal to accept HTTPS encrypted connections (HTTP is the default).

NOTE Changes will take effect after a unit reboot.

Setting	Description
Select Sharp Portal security methods	Select one of the following networking protocol options: • HTTP (Hypertext Transfer Protocol) • HTTPS (Hypertext Transfer Protocol Secure) Note If you select HTTPS you will need to provide a trusted certificate.
Show settings	Click to configure the SSL certificates required to enable a secure connection. For more information, see "Configuring Sharp Portal security" on page 148.

Camera status LED

Turn the camera LED on or off.

Setting	Description
Run in covert mode	Select this option to turn off the LED on the front of the Sharp unit, making it less conspicuous.

Image feed port (Advanced mode only)

This field is only visible if you are logged on the Sharp Portal in Advanced mode. For more information on how to log on in Advanced mode, see "Log on to the Sharp Portal" on page 36.

Setting	Description
Image feed port	If your AutoVu configuration includes two or more fixed Sharp units connected to the network through a router, you can use port forwarding to see each Sharp's live video feed. **EXAMPLE** For example, if you connect five Sharps to a router, and then connect the router to your network, you need to specify a different image feed port for each Sharp. A maximum of 32 ports are available for port forwarding (ports 4502 to 4534).

Support wheel imaging

Use these settings to configure the tire cameras for an AutoVu City Parking Enforcement with Wheel Imaging system.

Turning off the **Support wheel imaging** feature may result in the loss of the tire camera video feed in Patroller and in the Sharp Portal. As a workaround, turn the vehicle ignition OFF/ON to reboot the system and resolve the issue.

Setting	Description
Capture high definition wheel images	Capture images from the tire cameras in high definition (640 x 480).
Video format	Select the video format type from the drop-down list: • NTSC • PAL

Camera settings

Configure the Sharp camera settings. These settings are different depending on whether you are connected to a Sharp, or SharpX.

This section includes the following topics:

Sharp

If you are connected to a Sharp XGA or VGA, you will see the following settings:

Setting	Description
Capture high definition context images	Standard definition context images are 320 x 240 (pixels). Select this setting to capture images in 640 x 480.

SharpX

SharpX cameras are automatically detected when connected to the LPR Processing Unit. The Interfaces you see in the portal depend on how many cameras you have connected to the LPR Processing Unit and how many single board computers (SBCs) are on the LPR Processing Unit. For example, if you have four cameras connected to an LPR Processing unit with one SBC you will see all four interfaces: **Interface 1**, **Interface 2**, **Interface 3**, and **Interface 4**. On a SharpX-Multi system where you can connect two cameras to each SBC, you will only see two interfaces at a time in the portal (either **Interface 1** and **Interface 2**, or **Interface 3** and **Interface 4**) since the camera settings are configured on a separate portal page for each SBC.

The interfaces represent the following:

- **Interface 1 and Interface 2.** These correspond to the camera interfaces 1 and 2 on the faceplate of the LPR Processing Unit.
- **Interface 3 and Interface 4.** These correspond to the camera interfaces 3 and 4 on the faceplate of the LPR Processing Unit.

Setting	Description
Model	Displays the SharpX camera model and the serial number. • **VGA.** You have a SharpX VGA connected on this interface. • **XGA.** You have a SharpX XGA connected on this interface.

Setting	Description
LPR resolution	Select the resolution for the LPR camera. The resolution you select depends on several factors, such as the type of Sharp used, the type of lens, etc. Your initial site survey should provide you with the information you need to select the proper resolution. • **Standard (1024 x 768).** Used in specific situations as determined by the site survey. • **Tall (1024 x 946).** Used for most law enforcement installations to read up to three lanes of traffic. This setting generally provides the best results in the majority of cases. • **Wide (1280 x 808).** Used for most parking enforcement installations, especially for parallel parking.
Capture high definition context images	Standard definition context images are 320 x 240 (pixels). Select this setting to capture images in 640 x 480.

If there is a warning associated with a camera, there will be a yellow warning icon next to the interface number. Hover your mouse over the warning icon to see the details.

NOTES

- Tire cameras used for wheel imaging are not detected by default. If a tire camera is connected it must be configured manually by selecting **A tire camera is connected to this interface** and selecting the model. Tire cameras can be configured on **Interface 2** and **Interface 4** providing no LPR camera is connected to those interfaces already.
- If you are using an LPR Processor that has two SBCs you will need to configure the other SBC. To do this, click **Configure the other unit** located on the **Status** page, under **Actions**. For more information, see "Actions" on page 369.

Analytics

Configure which plates the Sharp will be reading (Quebec, Oregon, and so on), how fast the vehicles will be moving, and whether the Sharp should attempt to read the plate's origin in addition to the plate number (some license plates include the issuing state, province, or country).

Setting	Description
Context	Select which plates the Sharp will be reading.

Setting	Description
Read strategy	Select a read strategy from the drop-down list: • **Fast moving vehicle.** Use this when vehicles are travelling at moderate to high speeds. For example, use this for fixed Sharps overlooking a highway, or for mobile Law Enforcement installations when vehicles may be travelling at different speeds. • **Slow moving vehicle.** Use this when vehicles are travelling slowly (or stopped) when their plates are captured. For example, use this for parking lot gates or toll stations, or for mobile parking enforcement where vehicles are parked and the Patroller vehicle is moving slowly. • **Gate control.** Use this when you want to reduce reduce the number of duplicate plate reads when vehicles are stopped in the camera's field of view. This read strategy is ideal for fixed Sharp installations where vehicles come to a complete stop when their plates are read, forexample, at parking lot entrances or toll booths
Read plate state	Select this option if you want the Sharp unit to attempt to read the license plate origin (issuing state, province, or country). NOTE Plate state recognition may not be possible for all plates.
Read 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).
Estimate vehicle speed	(For fixed Sharps only) Select this option if you want the Sharp unit to attempt to estimate a vehicle's speed based on multiple captures of the license plate. The longer a vehicle is in the Sharp's field of view, the more accurate the estimate will be. NOTE Note the following: • Enabling this option automatically calibrates the Sharp for speed estimation, so you must enable it only *after* the Sharp has been properly installed and aligned. • If you move or re-position the Sharp after the initial installation, you must click **Calibrate** to re-calibrate the Sharp. • You can add the vehicle speed as an annotation field in Security Center in order to query for it in Security Desk reports. • Vehicle speed estimation may not be possible in all situations.
Give a confidence score for reads	Assigns a numerical value (from 0 to 100) to each license plate read. This value tells you how confident the Sharp is in the accuracy of the read. You can configure Patroller to display the score with all reads and hits, and you can add the score as an annotation field in Security Center in order to query for it in Security Desk reports.
Optimize for fixed installation	(Fixed Sharp units only) Use this option to create a smart region of interest that will decrease false positives.

Extension

Configure where the Sharp sends LPR data (Patroller, Security Center, or to an FTP server).

Setting	Description
None	The default state. You must choose one of the available options.
FTP	Send LPR data to an FTP server. For more information, see "Configuring the Sharp for an FTP connection" on page 144. The following options appear: • **Server.** Enter the FTP server name and location for the LPR data. You will 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. • **Time server.** Enter the DNS name of a known time server. The Sharp clock will be in sync with this server. • **Template.** LPR data is sent in xml format, using the template shown. You can change certain elements if you choose. For more information, see "Configuring the Sharp for an FTP connection" on page 144. • **Upload context image.** Send the context image to the FTP server. • **Upload LPR image.** Send the LPR image to the FTP server.
Patroller - Auto or vX.Y	Select **Auto** if you are using the current version of Patroller, or select an older version of Patroller from the list (the Sharp is backward compatible). The following option appears: • **Discovery port.** Port on which the Sharp listens for discovery requests. This port number must match the discovery port entered in Patroller Config Tool. For more information, see "Cameras" on page 347.

Setting	Description
Security Center - Auto or vX.Y	Select **Auto** if you are using the current version of Security Center, or select an older version of Security Center from the list (the Sharp is backward compatible). The following options appear: • **Connect to Security Center.** Use this **only** if the auto-discovery of connected Sharps does not work. You will need to enter the *IP address* and *port* of the Security Center computer. For example, if a Sharp is connected to a WiFi router, and the Sharp's IP address is then changed, the LPR Manager cannot detect the change automatically, so you can use this to re-connect to the Security Center computer. • **Discovery port.** Port on which the Sharp listens for discovery requests. This port number must match the discovery port entered on the LPR Manager **Properties** page. For more information, see "Properties" on page 285. • **Control port.** Used in Security Center Config Tool when creating a new LPR unit (Sharp) manually. For more information, see "LPR unit" on page 327. • **Video port.** The port used for streaming live video from the Sharp's context camera. For more information, see "LPR unit" on page 327. • **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. For more information, see "Update provider" on page 301. • **Accept remote reboot requests.** Select this so that you can reboot the Sharp from the LPR Unit **Properties** page. For more information, see "Properties" on page 285.

Inputs

Displays the status of the SharpX LPR Processing Unit inputs. You use these inputs to turn plate reading on/off depending on whether an input is receiving power.

Setting	Description
Name	Letter of the input.
Current status	Shows whether the input on the LPR Processing Unit is currently in an "on" or "off" state. • When the input is in an "on" state, it is detecting a voltage between 6V and 32V. • When the input is in an "off" state, it is detecting a voltage that is 1V or less.

Triggers

Enables the auxiliary inputs (*Aux inputs A, B, C and D*) on the SharpX LPR Processing Unit.

EXAMPLE In a street sweeper deployment with a SharpX camera on the left and right of the sweeper vehicle, you can configure the right SharpX to start reading when the LPR Processing Unit detects a power signal from the input, which would indicate that the sweeper's right brush (which is connected to the input) has been lowered.

Setting	Description
Generates reads only when input (A, B, C, or D) is (Off or On).	Enables conditional plate reading that depends on the auxiliary inputs on the LPR Processing Unit. If you select this option, you must also choose an Input and State from the drop-down list. EXAMPLE If you enable this setting, and then set Input to **A** and State to **On** it means that the SharpX will read plates only if the LPR Processing Unit detects power coming from the *Aux Input A* (for example, a street sweeper's brush being lowered).
Input	From the drop-down list, select which *Aux Input* turns on plate reading (for example, which input has the street sweeper's brush connected to it).
State	From the drop-down list, select which state turns on plate reading: • **On.** Starts reading when detecting voltage on the selected input that is between 6V and 32V. • **Off.** Starts reading when detecting voltage on the selected input that is 1V or less. Note Due to the nature of electrical systems, there is a grey area between 1V and 6V where the LPR Processing Unit may interpret the signal as **On** or **Off** depending on what is connected to the input, and if it generates leakage current. EXAMPLE If you have a dry contact switch opening and closing a battery circuit (such as when raising or lowering a street sweeper's brushes), you will not have a problem because the LPR Processing Unit will detect 0V (GND) when the circuit is open (clearly an **Off** state).

Live feed

The **Live feed** page is where you can display the live video feeds from the Sharp camera units. Use this page to test the Sharp cameras, and to enable a region of interest for fixed Sharp units.

This section includes the following topics:

Camera selection

Displays the different cameras available.

Setting	Description
Camera	Select the camera type from the drop-down list: • **None.** Default state. After you have finished viewing the live feeds, you should set this back to **None** in order to conserve CPU power. • **Context camera.** Displays the camera's normal video images. • **Tire camera.** Displays the tire camera images (if applicable). • **LPR camera.** Displays the LPR camera that captures license plates. Selecting the LPR camera allows you to define a region of interest by clicking on the screen. Each click creates a corner of the region of interest. You can click **Clear region of interest** to delete the region you created and start over. Defining a region of interest is only applicable to fixed installations and allows for more images to be processed. NOTE On a SharpX you can have more than one camera set, therefore you will see **LPR camera 2**, **Tire camera 2**, an so on.
	Click this button to refresh the live feed.

Image capture

You can capture a series of context and LPR images directly from the live feed window and save them to your computer as a zip file for later use.

Setting	Description
	Opens the **Image capture** window where you can choose where to save your zip file, the duration of the capture session, and more. NOTE Note the following: • You can save all images, or the best reads only (see "Best read" on page 383). • When the capture session begins, you cannot click another tab in the portal or select a different camera unless you stop the capture session. • The capture session will automatically stop based on the set **Duration**.
	Pause the capture session.
	Continue the capture session after pausing.
	Stop the capture session.

Information

Provides information about the live feed.

NOTE You can select the text in any of the text boxes and pres **Ctrl+C** on your keyboard to copy the information to your clipboard.

Setting	Description
Read	Displays the current read. This value can change rapidly depending on where the Sharp is installed. For example, a SharpX can read up to 30 frames per second. If a vehicle travels through the Sharp's field of view, the plate may be read 30 times. Only the Best read is saved.
Best read	Some Sharp cameras can read up to 30 frames (reads) per second. This is the best of those reads, as determined by the Sharp's internal analytics.
Plate 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 "Analytics" on page 377.
FPS	• Displays the FPS of the LPR engine when an LPR camera is selected. • Displays the FPS of the context camera when a context camera is selected.
Exposure	Displays the exposure value of the lens.
Total number of best reads	Displays the number of best reads that have been taken with the Sharp since the Plate Reader service was started. You can reset this value to zero by clicking the "Reset" button beside the field.

Setting	Description
Analytics	Displays the analytic information enabled in "Analytics" on page 377.

Diagnostics

The **Diagnostics** page is where you run reports and generate logs about the status of the Sharp unit. You can export this data to an XML file from the **Export settings** on the **Status** page. For more information, see "License" on page 370.

This section includes the following topics:

Search fields

These are the fields in the search area.

Setting	Description
Time	Time the event occurred.
Severity	Displays the severity of the event. You can choose which severity types to display in your "Search criteria" on page 386.
Source	The service that generated the error or message.
Message	Detailed message about the error and/or event.
Exception	Displays the software exception that generated the log entry. The exception gives extra information on where in the code the error occurred.

Sources to log

Select the sources from which to generate a log. For example, if you only want to see events related to Patroller, select **Patroller Extension** from the list

Click the **Refresh** button to refresh your results.

Search criteria

Select how you want to filter your search. You can search for events related to information, warnings, errors, and performance, or for all these events.

Setting	Description
Severity	Select which severity settings to include in the search: • Information • Warning • Error • Performance • Debug
Source	Filters query on the source of the log. Only logs containing this string will be shown.
Message	Filter query on the message. Only logs containing this string will be shown.
From/To	Select a date-and-time range for events.
Distinct entries only	Logs with identical messages will be displayed only once.

Part VII

Appendices

This part provides additional information which is not directly related to AutoVu installation or configuration, but that can be useful in AutoVu system maintenance.

This part includes the following chapters:

A

SharpX LED status reference

This section describes what the different states of the LED indicators mean on the SharpX LPR Processing Unit, and the SharpX camera unit.

This section includes the following topics:

LED status on the LPR Processing Unit

This section includes the following topics:

System status

The following table describes how the LEDs behave in response to the SharpX system's status. The headings **PWR, STAT 1, STAT 2, AND FAULT** correspond to the LEDs on the LPR Processing Unit.

State	Description	PWR	STAT 1	STAT 2	FAULT
Off	Unit powered off	Off	Off	Off	Off
Reflash	The unit has failed an integrity test on the contents of the control board flash memory. It is waiting for a reflash to be performed over the network.	On	On	Off	Off
POST	Power-on self-test. All LEDs flash in sequence and then together for approximately three seconds at power-up, if the control board flash memory has passed validation.	See description	See description	See description	See description
Get DHCP	The unit is waiting for a DHCP lease over the network (it is configured in "external DHCP mode").	On	5 quick flashes then pause, every 3 seconds	Off	Off
Thermal Shutdown	The internal temperature is outside the operational limits. Power is no longer supplied to most components. No Ethernet network connectivity is possible.	Toggles once per second	Off	Off	Toggles once per second
Power Fault	A fault was detected on the main power source.	Toggles once per second	Off	Off	On

State	Description	PWR	STAT 1	STAT 2	FAULT
Ethernet Fault	Could not configure an internal Ethernet switch.	On	Off	Off	Blinks **on** every three seconds
Firmware Fault	A critical fault was detected in the control board microcontroller.	On	Off	Off	On
SBC 1 On-line	First SBC is operational.	On	Blinks **off** every three seconds	N/A	Off
SBC 1 Off-Line	First SBC is not operational.	On	Blinks **on** every three seconds	N/A	Off
SBC 2 On-Line	Second SBC is operational.	On	N/A	Blinks **off** every three seconds	Off
SBC 2 Off-Line	Second SBC is not operational.	On	N/A	Blinks **on** every three seconds	Off
Ignition Cut	The ignition was cut. Unit is in a pre-shutdown grace period (default 10 seconds). If ignition is restored within this period, the shutdown is cancelled.	Blinks **off** every three seconds	Off	Off	Off

Camera data-link status

The following table describes how the Data-Link LEDs behave in response to the SharpX system's status.

State	Description	Data (amber)	Link (green)
Data idle	No Ethernet data is being received/transmitted between the camera and the trunk unit.	Off	N/A
Data transmit	Ethernet data is being received/ transmitted between the camera and the trunk unit.	Blink	N/A

State	Description	Data (amber)	Link (green)
Not registered	The camera is not registered with the trunk unit yet. It may take up to 30 seconds for a camera to be registered.	N/A	Off
Registered	The camera is registered with the trunk unit, and can exchange control messages with the LPR engine.	N/A	On

LED status on the SharpX camera unit

The following table describes how the SharpX camera unit's LED behaves in response to the SharpX system's status.

State	Description	LED (red/green)
Off	Unit is powered off	Off
Reflash	The unit has failed an integrity test on the contents of the control board flash memory. It waits for a reflash to be performed over the network.	Green (steady)
Get DHCP	The unit is waiting for a DHCP lease over the network (either from the LPR Processing Unit or an external server, depending on configuration).	Blinks green rapidly (e.g. twice per second).
Normal	The camera is running normally.	Flashes green briefly every second.
Covert	The camera is configured in covert mode. It will still blink green a couple of times at power-up.	Off
Thermal Shutdown	The internal temperature is outside the operational limits. Power is no longer supplied to most components. No Ethernet network connectivity is possible.	Toggles slowly every second.
Illuminator Fault	An abnormal condition was detected with the illumination. Depending on the fault, the unit may run in degraded mode (some LEDs shut off), or the illuminator may be completely disabled.	Blinks red rapidly (e.g. twice per second).
Firmware Fault	A critical fault was detected in the control board microcontroller.	Red (steady)

B

AutoVu Sharp and SharpX parts lists

This section lists the parts that are included with the Sharp and SharpX, and explains the components of a Sharp part number.

This section includes the following topics:

AutoVu Sharp parts

This section includes the following topics:

Fixed AutoVu Sharp parts list

These are the parts included with a fixed AutoVu system.

Part number	Part name
AU-S-XXX-XXXXXX[a]	Sharp camera
AU-H-PWRACINT	Power supply (optional)[b]
AU-H-FIXCBLXXPE[c]	Sharp fixed cable

a. For more information on your Sharp part number, see "Understanding the Sharp part number" on page 396.
b. You can order your AutoVu system with a power supply, or you can use your own. If you use your own power supply, make sure it conforms to the Sharp specifications.
c. The "XX" in this part number corresponds to the desired length of the cable. For example, "03" is a 3 metre cable.

Mobile AutoVu Sharp parts list

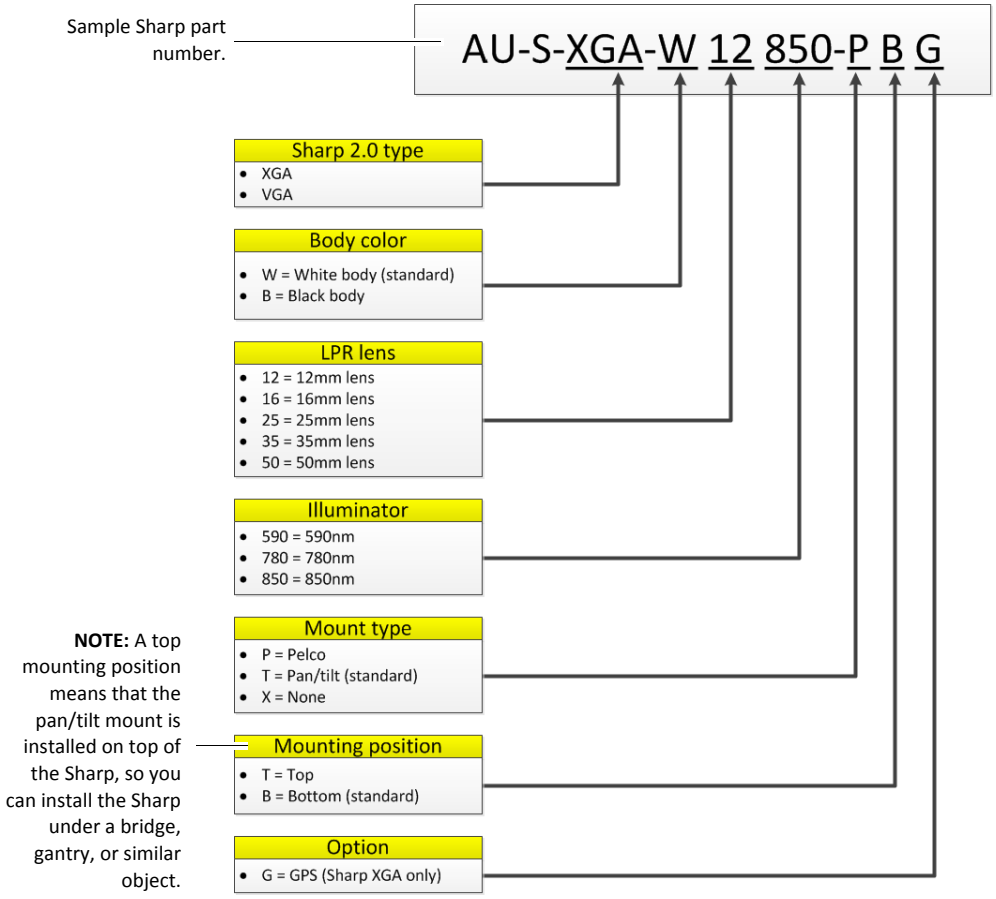
These are the parts included with a mobile AutoVu system using a Sharp camera.

Part number	Part name
AU-S-XGA-XXXXXX	Sharp camera
AU-H-MAGMNT	Sharp magnetic mount (optional)
AU-H-SBCBL05	Sharp cable to breakout box
AU-H-BOBUNIT	Breakout box
AU-H-BATCBL	Breakout box power cable to battery
AU-H-ILFUSE15A	Power cable in-line fuse
AU-H-CIGCBL	Cigarette lighter power cable (optional)
AU-H-ETHCBL14	Ethernet cable

Part number	Part name
AU-H-SHPHMBOT	Hardmount bottom component (optional)
AU-H-SHPHMTOP	Hardmount top component (optional)
AU-H-NAVBOX	Navigator unit (optional)
AU-H-USBCBL15	Type A to type B USB cable (optional)
AU-H-PCASE1510	Pelican case (optional)
AU-H-GPSANT	GPS antenna (optional)
AU-H-UWDSEAL	Universal window seal (optional)
AU-H-VID4T9L6	Tire camera (optional)
AU-H-VIDTICBL	Tire camera cable to breakout box (optional)
N/A	Ruggedized touchscreen PC

Understanding the Sharp part number

The Sharp part number is composed of information that will help you determine what kind of Sharp camera you have.



AutoVu SharpX parts

This section includes the following topics:

AutoVu SharpX parts list

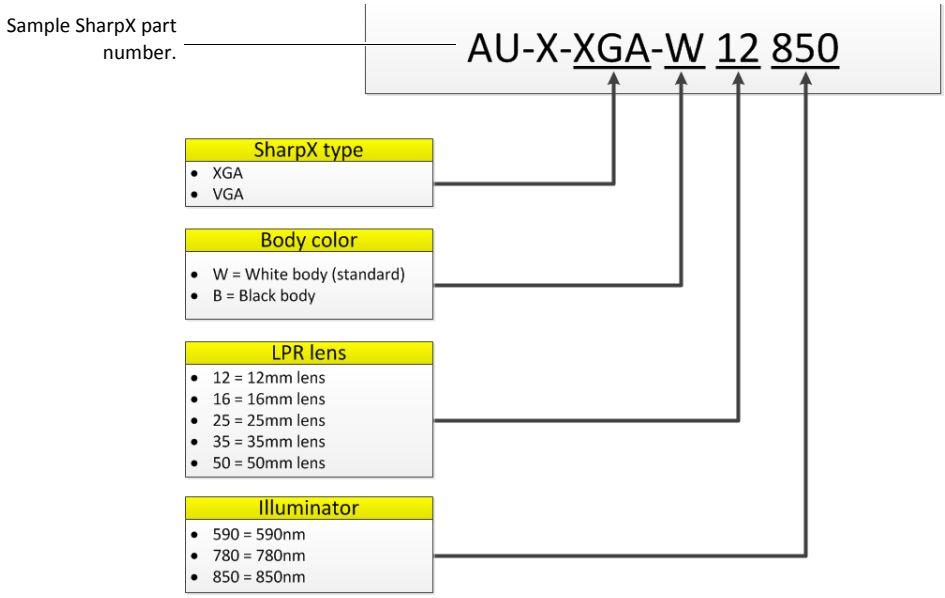
These are the parts included with a mobile AutoVu system using a SharpX system.

Part number	Part name
AU-X-XXX-XXXXXX[a]	SharpX camera unit
AU-H-XTU-X1	SharpX system LPR Processing Unit. One processor supporting one camera.
AU-H-XTU-X2	SharpX system LPR Processing Unit. Two processors supporting two cameras.
AU-H-XTU-X2M	SharpX - Multi system LPR Processing Unit. One multi-thread processor supporting two cameras.
AU-H-XTU-X4M	SharpX - Multi system LPR Processing Unit. Two multi-thread processors supporting four cameras.
AU-H-XCBL05	SharpX to Processing Unit Cable (5 m)
AU-H-XTU-MNT1V **or** **AU-H-XTU-MNT1H**[b]	SharpX LPR Processing Unit standard mounting bracket.
N/A	Ruggedized touchscreen PC
(Optional) AU-H-XMNT-CAMU	SharpX camera portable mounting bracket - Pan Tilt Universal
(Optional) AU-H-XMNT-CAMH	SharpX camera hardmount mounting bracket - Pan Tilt
(Optional) AU-H-XMNT-CAMLB	SharpX light bar bracket (light bar make and model required)
(Optional) AU-H-XVISOR	SharpX Camera Visor

a. For more information on your SharpX part number, see "Understanding the SharpX part number" on page 398.
b. The “V” and “H” in these part numbers correspond to a vertical or horizontal trunk unit.

Understanding the SharpX part number

The SharpX part number is composed of information that will help you determine what kind of SharpX camera you have.



C

Hardware compliance information

AutoVu Sharp and SharpX products are certified based on the power supplies provided by Genetec. If you use a different power supply, you do so at your own risk, and you are responsible for the EMC compliance of the new system formed by the Sharp/SharpX and the new power supply.

AutoVu Sharp

This device complies with Part 15 of the FCC rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modification to the product not expressly approved by Genetec could void the user's authority to operate this device.

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

This equipment has been tested and found to comply with the limits of a Class B digital device, pursuant to Part 15 of the FCC rules and CISPR 22/EN 55022. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase separation between the equipment and receiver.

- Connect the equipment into an output on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To maintain electromagnetic compliance in an end user installation, follow these conditions:

- Ensure that the drain wire (shield) of the approved camera cable is connected to earth ground, either via the chassis/frame of the installation site, or via a dedicated conductor following recognized good grounding practice. Do not use any cable other than the one approved by and supplied by Genetec for connecting the device.
- Any changes or modifications to the product or installation practice not expressly approved by Genetec, may result in interference to radio or television reception, and could void the user's right to operate the equipment.

AutoVu SharpX system

This device complies with Part 15 of the FCC rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This equipment has been tested and found to comply with the limits of a Class A digital device, pursuant to Part 15 of the FCC rules and CISPR 22/EN 55022. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area might cause harmful interference in which case the user will be required to correct the interference at his own expense.

To maintain electromagnetic compliance in an end user installation, follow these conditions:

- Ensure that the LPR Processing Unit (also referred to as the “trunk unit”) has its enclosure grounded/earthed to the chassis/frame using its mechanical mounting.
- Do not use any cable other than the one supplied by Genetec to connect the camera units. The drain wire of this cable must be connected to the terminal intended for this purpose on the LPR Processing Unit’s camera port.
- Any changes or modifications to the product, or to the installation practice not expressly approved by Genetec, may result in interference to radio or television reception, and could void the user’s right to operate the equipment.

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

Security Center is the unified platform for all Genetec's IP security solutions, which include AutoVu™, Omnicast™, and Synergis™ modules. The definitions in this glossary pertain to all three modules.

A

accepted user

A user who has read access over all entities contained in a partition. This allows the user to view them in all entity browsers. Additional access rights may be granted through user privileges.

access right

access right.

(1) Type of rights a user has over entities in the system (view, add, modify, delete), which are defined by a combination of partitions and user privileges.

action

User-programmable function that can be triggered as an automatic response to an event (door held open for too long, object left unattended) or executed according to a specific time table.

See also event and event-to-action.

active alarm

An alarm that has not yet been acknowledged.

See also alarm.

Active Directory

Active Directory (AD).

(1) A directory service created by Microsoft.

(2) Type of role that imports users and cardholders from an Active Directory and keeps them synchronized.

Activity trails

Type of maintenance task that reports on the user activity related to video 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.

agent

Subprocess created by a Security Center role to run simultaneously on multiple servers for the purpose of sharing its load.

See also redirector agent.

alarm Type of entity that describes a particular trouble situation that requires immediate attention and how it should be handled in Security Center. Namely, its priority, what entities (usually cameras and doors) best describe it, who should be notified, how it should be displayed to the user, and so on.

alarm acknowledgement User response to an alarm. There are two variants of alarm acknowledgement in Security Center:

- Default acknowledgement
- Alternate acknowledgement

Each variant is associated to a different event so that specific actions can be programmed based on the alarm response selected by the user.

See also action and event.

Alarm monitoring Type of operation task that allows you to monitor and respond to alarms (acknowledge, forward, snooze, among other things) in real time, as well as review past alarms.

See also monitor group.

alarm panel Another name for intrusion panel.

See also intrusion panel.

Alarm report Type of investigation task that allows you to search and view current and past alarms.

area Type of entity that represents a concept or a physical location (room, floor, building, and so on) used for the logical grouping of entities in the system.

See also Logical view.Synergis

asset Type of entity that represents any valuable object with an RFID tag attached, allowing it to be tracked by an asset management software.

See also RFID tag.

Audit trails Type of maintenance task that reports on the configuration changes who made them, on selected entities in the system.

automatic discovery The process by which IP units on a network are automatically discovered by Security Center. This is done by broadcasting a discovery request on the discovery port and waiting for all listening units to respond with a packet that contains connection information about itself. Security Center uses the information to automatically configure the connection to the unit, thus enabling communication. Not all units support this feature.

See also unit.

AutoVu

AutoVu™ is the IP license plate recognition (LPR) system of Security Center that automates the reading and verification of vehicle license plates. AutoVu Sharp cameras capture license plate images, and send the data to 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 (e.g. on a pole in a parking lot), or in a mobile configuration (e.g. 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.

AutoVu LPR Processing Unit

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 "trunk unit" because it is typically installed in a vehicle's trunk.

See also LPR camera and SharpX.

B

block face (2sides)

Type of parking regulation characterizing an overtime rule. A block face is the length of a street between two intersections. A vehicle is in violation if it is seen parked within the same block over a specified period of time. Moving the vehicle from one side of the street to the other does not make a difference.

Breakout box

Genetec's proprietary connector box for AutoVu mobile solutions that use Sharp version 2.0 cameras. The breakout box provides power and network connectivity to the Sharp units and the in-vehicle computer. Currently, the AutoVu SharpX system is the preferred solution for a mobile AutoVu installation.

broadcast

Communication between a single sender and all receivers on a network

C

canvas

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.

See also tile.

cash register

Type of entity that represents a single cash register (or terminal) in a point of sale system.

See also point of sale system.

certificate Additional license information that is required to run plugins or SDK-based applications.

City Parking Enforcement Patroller software installation that is configured for city parking enforcement: the enforcement of parking permit and/or overtime restrictions.

See also overtime rule and permit.

City Parking Enforcement with Wheel Imaging A "City Parking Enforcement" installation of a Patroller application that also includes wheel imaging. The use of maps and of the Navigator is mandatory.

See also City Parking Enforcement.

compatibility pack See Omnicast compatibility pack.

Config Tool 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.

Conflict resolution utility Tool that helps you resolve conflicts caused by importing users and cardholders from an Active Directory.

context camera 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.

See also LPR camera and LPR unit.

Copy configuration tool Tool that copies the configuration of one entity to many other entities.

covert hit 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 the Security Desk by a user with proper privileges.

covert hotlist Hotlist hidden from the AutoVu Patroller users. Reads matching a covert hotlist generate covert hits.

custom event 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 may be renamed and deleted.

custom field User defined property associated to an entity type to store additional information that is useful to your particular organization.

D

Daily usage per patroller 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

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.

See also widget.

Data Server

Plan Manager Server module that manages the Plan Manager database where the map configuration is stored.

See also Plan Manager Server.

database

Collection of data that is organized so that its contents can easily be accessed, managed, and updated.

database server

An application that manages databases and handles data requests made by client applications. Security Center uses Microsoft SQL Server as its database server.

DHCP server

A DHCP (Dynamic Host Configuration Protocol) server provides configuration parameters necessary for a unit to automatically connect to an IP network. DHCP automatically supplies the unit with an IP address, the network mask, a gateway IP address, and a DNS server IP address.

Directory

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 *main server*. All other servers in Security Center must connect to the main server and are called *expansion servers*.

See also expansion server, main server, and server.

Directory Manager

The role that manages the Directory failover and load balancing in order to produce the high availability characteristics in Security Center.

See also Directory server and high availability.

Directory server

Any one of the multiple servers simultaneously running the Directory role in a high availability configuration.

See also Directory, high availability, and server.

discovery port

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.

See also automatic discovery.

district

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.

Driver Development kit Driver Development Kit (DDK). An SDK for creating device drivers.

E

enforce To take action following a confirmed hit. For example, a parking officer can enforce a scofflaw (unpaid parking tickets) violation 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 may represent a physical device, such as a camera or a door, or an abstract concept, such as an alarm, a schedule, a user, or a software module.

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

See also Logical view.

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, conferring intelligent behavior to the system. Every event mainly focuses on one entity, called the *event source*.

See also event-to-action.

event-to-action The coupling of an action to an event to confer automatic and intelligent behavior to the system.

expansion server 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.

See also main server and server.

F

failover 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 when the primary server becomes unavailable, either through failure or through scheduled downtime.

See also high availability and load balancing.

federated entity Any entity that is imported from an independent system via a federation role.

federated system

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 manipulate its entities as if they belong to the local system.

See also Omnicast Federation and Security Center Federation.

Federation

The Federation™ is a virtual system formed by joining multiple remote independent Genetec IP security systems together. The purpose of the Federation is to allow the users on your local system (the Federation host) to access the entities belonging to independent systems as if they were on your local system.

G

Genetec Server

Windows service at the core of Security Center architecture 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.

See also server.

geocoding

The process of finding associated geographic coordinates (latitude and longitude) from a street address.

See also reverse geocoding.

ghost Patroller

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.

See also Patroller.

GIS

Geographic information system (GIS) is a third party map provider that Plan Manager can connect to, to bring maps and all types of geographically referenced data to Security Center.

See also KML, OGC, and WMS.

Global Cardholder Synchronizer

Type of role that ensures the two-way synchronization of shared cardholders and their related entities between the local system (sharing participant) and the central system (sharing host).

See also sharing guest and sharing host.

global entity Entity that is shared across multiple independent Security Center systems by virtue of its membership to a global partition. Only cardholders, cardholder groups, credentials, and badge templates are eligible for sharing.

See also global partition.

global partition Partition that is shared across multiple independent Security Center systems by the partition owner, called the sharing host.

See also global entity, partition, and sharing guest.

GUID A globally unique identifier, or GUID, is a special type of identifier used in software applications to provide a unique reference number.

H

Hardware inventory 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.

Health history Type of maintenance task that reports on health issues.

See also Health statistics and Health Monitor.

Health Monitor The central role that monitors system entities such as servers, roles, units, and client applications for health issues.

See also Health history and Health statistics.

Health statistics Type of maintenance task that gives you an overall picture of the health of your system.

See also Health history and Health Monitor.

high availability Design approach used to enable a system to perform at a higher than normal operational level. This often involves failover and load balancing.

See also failover and load balancing.

HIP A hardware integration package, or HIP, is an update that can be applied to Security Center. It enables the management of new functionalities (for example, new video unit types), without requiring an upgrade to the next Security Center release.

hit License plate read that matches a hit rule (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.

See also enforce.

hit rule
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.

hit, hotlist, overtime rile, permit, and permit restriction.

Hits
Type of investigation task that reports on hits reported within a selected time range and geographic area.

See also hit and hotlist.

hot action
An action mapped to a PC keyboard function key (Ctrl+F1 through Ctrl+F12) in Security Desk for quick access.

hotlist
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).

See also hit rule.

Hotlist and permit editor
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.

See also hotlist and permit.

hotspot
Type of map object that represents an area on the map that requires special attention. Clicking on a hotspot displays associated fixed and PTZ cameras.

See also map object.

HTTPS
Secure Hypertext Transfer Protocol for the World Wide Web that provides safe data transmission by encrypting and decrypting information sent over the Internet.

I

illuminator
A light in the Sharp unit that illuminates the plate, thereby improving the accuracy of the images produced by the LPR camera.

See also LPR camera.

Immersive view
Plan Manager feature that lets you 'walk' inside a building or a city in a first person view.

inactive entity
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.

See also entity.

incident
Any incident reported by a Security Desk user. Incident reports can use formatted text and include events and entities as support material.

See also Incidents.

Incidents
Type of investigation task that allows you to search, review, and modify incident reports.

intrusion detection area
Type of entity that corresponds to a zone or a partition (group of sensors) on an intrusion panel.

See also intrusion detection unit.

Intrusion detection area activities
Type of investigation task that reports on activities (master arm, perimeter arm, duress, input trouble, and so on) in selected intrusion detection areas.

intrusion detection unit
Type of entity that represents an intrusion panel (or alarm panel) that is monitored and controlled by Security Center.

See also Intrusion Manager.

Intrusion detection unit events
Type of investigation task that reports on events (AC fail, battery fail, unit lost, input trouble, and so on) pertaining to selected intrusion detection units.

Intrusion Manager
Type of role that monitors and controls intrusion panels. It also logs the intrusion events in a database for intrusion activity reports.

See also intrusion detection unit.

intrusion panel
A wall-mounted unit where the alarm sensors (motion sensors, smoke detectors, door sensors, and so on) and wiring of the intrusion alarms are connected and managed.

See also intrusion detection unit.

Inventory management
Type of operation task that allows you to add and reconcile license plate reads to a parking facility inventory.

Inventory report
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).

IO linking

IO (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 would be to sound a buzzer (via 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).

See also zone.

IP

The protocol that routes data packets through a local area network (LAN) and the Internet.

IP address

An IP Address is a unique numeric address for a specific computer or computing device connected to the Internet, or to a LAN.

See also IPv4 and IPv6.

IPv4

First generation IP protocol using a 32-bit address space.

IPv6

New generation IP protocol extending the address space from 32 to 128 bits.

J

K

KML

Keyhole Markup Language (KML) is a file format used to display geographic data in an Earth browser such as Google Earth and Google Maps.

See also GIS.

L

Law Enforcement

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.

See also hotlist.

license key

Software key used to unlock the Security Center software. The license key is specifically generated for each computer where the Directory role is installed. You need the System ID (which identifies your system) and the Validation key (which identifies your computer) in order to obtain your license key.

license plate inventory

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).

See also Inventory report.

license plate read

License plate number captured from a video image using LPR technology.

See also hit and License Plate Recognition.

License Plate Recognition 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.

See also LPR camera and OCR equivalence.

live hit A hit matched by the Patroller and immediately sent to the Security Center over a wireless network.

live read A license plate captured by the Patroller and immediately sent to the Security Center over a wireless network.

load balancing Distribution of workload across multiple computers.

See also failover and high availability.

logical ID Unique IDs assigned to each entity in the system for ease of reference. Logical IDs are only unique within a particular entity type.

Logical view Browser view that organizes all viewable entities in Security Desk (such as areas, cameras, doors, elevators, maps, and so on) according to their logical relationships. Areas are used as logical groupings for other entities. Each area may represent a concept or a physical location.

See also Security Desk.

Logons per Patroller Type of investigation task that reports on the logon records of a selected Patroller.

long term Type of parking regulation characterizing an overtime rule. The "long term" regulation uses the same principle as the "same position" 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 *See* License Plate Recognition.

LPR camera A camera connected to an LPR unit that produces high resolution close-up images of license plates.

See also context camera and SharpX.

LPR Manager Type of role that manages and controls Patrollers and fixed Sharp units. The LPR Manager manages the data (reads and hits) collected by the LPR units it controls and updates the configuration of the mobile units (Patrollers) every time they begin a new shift.

LPR rule Method used by Security Center/AutoVu for processing a license plate read. An LPR rule can be a "hit rule" or a "parking facility".

See also hit rule and parking facility.

LPR unit

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.

See also AutoVu LPR Processing Unit, License Plate Recognition, LPR Manager, and Sharp unit.

M

macro

Type of entity that encapsulates a C# program that adds custom functionalities to Security Center.

main server

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.

See also Directory server, expansion server, and server.

manual capture

When license plate information is entered into the system by the user, and not by the LPR.

manufacturer extension

Manufacturer specific settings for access control units, video units, and intrusion detection units.

Map Generator

Map Server module that imports raster and vector maps to Plan Manager database.

See also Mlap Server.

map link

Type of map object that lets you jump to either another map or another area of the same map.

See also map object.

Map mode

Security Desk canvas operating mode where the main area of the canvas is used to display a geographical map.

map object

A graphical object displayed on a Plan Manager map, such as a camera, a door, or a hyperlink, that allows you to monitor and control your Security Center system, or to navigate through your maps.

See also hotspot, map link, and Plan Manager Client.

Map Server
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.

See also Map Generator, Tile Server, and Plan Manager Server.

map view
A defined display position and zoom level for a given map.

master arm
Arming an intrusion detection area in such a way that all sensors attributed to the area would set the alarm off if one of them is triggered. Some manufacturers call this arming mode "Away arming".

metadata
Metadata is data about data. Any data that describes or enriches the raw data.

MLPI
See Mobile License Plate Inventory.

Mobile Admin
Web-based administration tool used to configure the Mobile Server.

See also Mobile Server.

Mobile app
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.

See also mobile device, Mobile Server, and Web Client.

Mobile Data Computer
Mobile Data Computer (MDC). 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 device
Any handheld device that can connect to Wi-Fi or wireless carrier networks, such as a smartphone, tablet, and so on, on which the Mobile app is installed.

See also Mobile app.

Mobile License Plate Inventory
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.

See also license plate inventory and parking facility.

Mobile Server
The server component of Security Center Mobile that connects Mobile apps and Web Clients to Security Center. The Mobile Server connects to Security Center, and synchronizes the data and video between Security Center and supported Mobile client components.

See also Mobile Admin, Mobile app, and Web Client.

Monitoring
Type of operation task that allows you to monitor and respond to real time events pertaining to selected entities of interest.

Move unit — Tool 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.

multicast — Communication between a single sender and multiple receivers on a network.

N

NAT — *See* network address translation.

Navigator — Genetec's proprietary in-vehicle device that provides GPS coordinates and odometer readings to Patroller. The Patroller uses this information to provide precise reverse geocoding to vehicles and reads.

See also reverse geocoding.

network — Entity type used to capture the characteristics of a network for stream routing purposes.

network address translation — 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 — Browser view that illustrates your network environment by showing each server under the network they belong to.

new wanted — In Patroller, a manually entered hotlist item. 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.

O

OCR equivalence — The interpretation of OCR 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.

See also Optical Character Recognition.

OGC — Open Geospacial Consortium (OGC) is a standards organization for geographic information systems.

See also GIS and WMS.

Omnicast — Omnicast™ is the IP video surveillance system of Security Center that provides seamless management of digital video. Omnicast allows for multiple vendors and CODEC (coder/decoder) to be used within the same installation, providing the maximum flexibility when selecting the appropriate hardware for each application.

Omnicast compatibility pack — Software component that you need to install to make Security Center compatible with an Omnicast 4.x system.

Omnicast Federation — Type of role that imports entities from an independent Omnicast 4.x system so that its cameras and events can be used by your local Security Center users.

Optical Character Recognition — Optical Character Recognition (OCR) is the technology used to translate the characters found in images into machine editable text.

See also OCR equivalence.

output behavior — Type of entity that defines a custom output signal format such as a pulse with a delay and duration.

overtime rule — 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 zone where these restrictions apply.

See also hit rule and parking zone.

P

parking facility — Type of entity that defines a large parking area as a number of sectors and rows for the purpose of inventory tracking.

See also Mobile License Plate Inventory.

parking lot — 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.

See also parking zone.

parking zone — General concept used to designate the area where a given parking regulation (overtime rule, permit, or permit restriction) is enforced. When used in the context of university parking enforcement, the parking zone must be explicitly defined as a list of parking lots.

See also parking lot.

partition

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 doors, elevators, and cameras in one building.

See also accepted user and partition manager.

partition manager

An accepted user of a partition who has full administrative rights over the partition and its members. A partition manager can add, modify, and delete all entities within the partition, including users and user groups.

Patroller

Patroller.

(1) Type of entity that represents a patrol vehicle equipped with the Patroller software.

(2) 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.

See also LPR camera and LPR Manager.

Patroller Config Tool

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.

perimeter arm

Arming an intrusion detection area in such a way that only sensors attributed to the area perimeter would set the alarm off if triggered. Other sensors such as motion sensors inside the area will be ignored.

permit

Type of entity that defines a single parking permit holder list. Each permit holder is characterized by a permit ID, 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.

See also City Parking Enforcement and University Parking Enforcement.

permit hit

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

Type of entity that applies time restrictions to a series of parking permits for a given parking zone. Permit restrictions are only used in university parking enforcement. Different time restrictions can be associated to different permits. For example, a permit restriction may limit the parking in zone A from Monday to Wednesday for permit P1 holders, and from Thursday to Sunday for permit P2 holders.

A plate read generates a *permit hit* in the following instances:

- Does not match any entry in the list
- Matches one or more permit in the list that are not valid in the parking zone
- Matches an invalid permit
- Matches a valid permit, but the permit is not valid at that time
- Matches a valid permit number, but the permit is temporarily not allowed to park.

Additionally, a *shared permit hit* occurs when two plates sharing the same permit ID are read in the same parking zone within a specific time period.

See also parking zone, permit, and permit hit.

Plan Manager

Map-based interface built into Security Center that allows you to view, control, and monitor your access control, LPR, and video equipement directly from an interactive map within Security Desk.

See also Plan Manager Client and Plan Manager Server.

Plan Manager Client

Client component of Plan Manager that runs as a tile plugin within Security Desk. It enables operators to use maps to monitor and control cameras, doors, and other security devices, and administrators to create map objects.

See also map object, tile plugin, and Tile Server.

Plan Manager Server

Server component of Plan Manager that must be hosted by a Security Center Plugin role. Plan Manager Server includes two server modules, Data Server and Map Server, which can be hosted on the same Plugin role or two separate Plugin roles.

See also Data Server, Map Server, and Plugin.

Plate Reader

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.

See also LPR Manager, Patroller, and Sharp unit.

Plugin

Plugin. There are two definitions:

(1) Proper noun – Type of role that hosts a specific plugin.

(2) Common noun – A software module that adds a specific feature or service to a larger system.

Point of Sale

Type of role that imports transaction data from an external point of sale system so that transaction reports can be generated from Security Desk for investigation purposes.

See also point of sale system.

point of sale system

Point of sale (POS) typically refers to the hardware and software used for checkouts - the equivalent of an electronic cash register. Point of sale systems are used in supermarkets, restaurants, hotels, stadiums, and casinos, as well as almost any type of retail establishment.

Today's POS systems handle a vast array of features, including, but not limited to, detailed transaction capture, payment authorization, inventory tracking, loss prevention, sales audit and employee management.

primary server

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.

See also failover.

private IP address

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

Entity that represents a saved type of task that is visible only to the user who created it.

See also public task and task.

properties panel

One of the three panels found in the Security Desk canvas. It is used to show the metadata associated to the entity displayed in the current tile.

Public partition

A special partition created at system installation that has the unique characteristic that all its members are visible to all users on the system, regardless whether they are accepted users or not.

public task

Entity that represents a saved task that can be shared among multiple Security Center users.

See also private task and task.

Q

R

read — *See* license plate read.

Reads — Type of investigation task that reports on license plate reads performed within a selected time range and geographic area.

Reads/hits per day — Type of investigation task that reports on the number of reads and hits per day for a selected date range.

Reads/hits per zone — Type of investigation task that reports on the number of reads and hits per parking zone for a selected date range.

Report Manager — Type of role that automates report emailing and printing based on schedules.

report pane — A section in the Security Desk's task workspace used to display information in a tabular form. The rows may correspond to query results or real-time events.

See also task workspace.

reverse geocoding — AutoVu feature that translates a pair of latitude and longitude into a readable street address.

See also geocoding and Navigator.

RFID tag — Radio Frequency Identification tag. A device that communicates location data, and other data related to the location, of an object to which it is attached.

role — A software module that performs a specific function (or job) within Security Center. Roles must be assigned to one or more servers for their execution.

See also server.

Role view — Browser view that lists all roles on your system with the devices they control as child entities.

Route playback — Type of investigation task that replays the route followed by a Patroller on a given date on a map.

S

same position — 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. The Patroller must be equipped with GPS capability in order to enforce this type of regulation.

schedule 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).

See also standard schedule and twilight schedule.

scheduled task Type of entity that defines an action that executes automatically on a specific date and time, or according to a recurring schedule.

secondary server Any alternate server on standby intended to replace the primary server in the case the latter becomes unavailable.

See also failover and primary server.

Security Center Security Center is the unified security platform that seamlessly blends Genetec's IP security and safety systems within a single innovative solution. The systems unified under Security Center include Genetec's Omnicast IP video surveillance system, Synergis IP access control system, and AutoVu IP license plate recognition (LPR) system.

See also Security Desk.

Security Center Federation Type of role that imports entities from an independent Security Center system so that its entities can be used by your local Security Center users.

Security Center Mobile Security Center Mobile is a feature of Genetec's unified platform that lets you remotely connect to your Security Center system over a wireless IP network. Supported Mobile client components include a platform-independent, unified Web Client, as well as various Mobile apps for smartphones and tablets.

See also Mobile Admin, Mobile app, Mobile Server, and Web Client.

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.

See also Security Center.

selector One of the panes found in the Security Desk's task workspace. The selector contains different sets of tools, grouped in tabs, to help you find and select the information you need to work on.

See also task workspace.

server

Type of entity that represents a server machine on which Genetec Server is installed.

See also expansion server, Genetec Server, and main server.

Server Admin

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.

sharing guest

Security Center system that is given the rights to view and modify entities shared by another system, called the sharing host.

See also Global Cardholder Synchronizer and global partition.

sharing host

Security Center system that owns partitions that are shared with other Security Center systems, called sharing guests.

See also global partition.

Sharp EX

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

See also context camera, LPR camera, and Sharp unit.

Sharp Portal

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.

See also Sharp unit.

Sharp unit

Genetec's proprietary LPR unit that integrates license plate capturing and processing components, as well as digital video processing functions, inside a ruggedized casing.

See also context camera, PlateReaderServer, LPR camera, Sharp EX, Sharp VGA, Sharp XGA, SharpX, and.

Sharp VGA

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.

See also context camera, LPR camera, and Sharp unit.

Sharp XGA

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.

See also context camera, LPR camera, and Sharp unit.

SharpX

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.

See also AutoVu LPR Processing Unit.

SharpX VGA

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.

See also AutoVu LPR Processing Unit.

Software Development Kit

Software Development Kit (SDK). Allows end-users to develop custom applications or custom application extensions for Security Center.

SSL

Secure Sockets Layer is a protocol used to secure applications that need to communicate over a network.

standard schedule

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

See also twilight schedule.

standby server

See secondary server.

Synergis

Synergis™ is the IP access control system of the Security Center designed to offer end-to-end IP connectivity, from access control reader to client workstation. Synergis™ seamlessly integrates a variety of access control capabilities including, but not limited to, badge design, visitor management, elevator control, zone monitoring and more.

system event

A system event is a standard Security Center event defined at system installation. Unlike custom events, system events cannot be renamed or deleted.

See also custom event.

System status 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 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.

See also private task and public task.

task cycling Security Desk feature that automatically cycles through all tasks in the active task list following a fixed dwell time.

task workspace Area in the Security Center client application window reserved for the current task. The workspace is typically divided into three panes:

- canvas
- selector
- report pane

See also canvas, report pane, and selector.

taskbar User interface element of the Security Center client application window, composed of the Home button and the task list. The taskbar can be configured to appear on either edge of the application window.

threat level Emergency handling procedure that a Security Desk operator can enact on one area or the entire system to deal promptly with a potentially dangerous situation, such as a fire or a shooting.

tile An individual window within the tile panel, 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.

See also tile panel.

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

See also tile and tile panel.

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

tile panel Panel within the canvas used to display multimedia information, such as videos, maps and pictures. The tile panel is composed of individual display windows called tiles.

See also canvas and tile.

tile pattern Predefined tile arrangements within the tile panel.

See also tile panel.

Tile Server Map Server module that answers the map requests issued from Plan Manager Client.

See also Map Server and Plan Manager Client.

tile plugin Type of entity that represents an application that runs inside a Security Desk tile. Examples of tile plugins include a web browser (available as standard Security Center feature) and Plan Manager Client.

See also Plan Manager and plugin.

timeline 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.

Transmission Control Protocol The Transmission Control Protocol (TCP) is a connection-oriented protocol used to send data over an IP network. The TCP/IP protocol defines how data can be transmitted in a secure manner between networks. TCP/IP is the most widely used communications standard and is the basis for the Internet.

trickling The process of transferring data in small amounts.

twilight schedule A subtype of schedule entity that supports both daytime and nighttime coverages. A twilight schedule may not be used in all situations. Its primary function is to control video related behaviors.

See also standard schedule.

U

unicast Communication between a single sender and a single receiver over a network.

Uniform Resource Locator A URL (Uniform Resource Locator, previously Universal Resource Locator) is the unique address for a file that is accessible on the Internet. The URL contains the name of the protocol (*http:*, *ftp:*, *file:*) to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a path name, a hierarchical description that specifies the location of a file in that computer.

unit

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:

-  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.

See also access control unit, Access Manager, Archiver, Intrusion Manager, LPR Manager, LPR unit, and video unit.

Unit discovery tool

Tool that allows you to discover IP units connected to your network, based on their type (access control or video), manufacturer, and network properties (discovery port, IP address range, password, and so on). Once discovered, the units can be added to your system.

Unit replacement

Tool 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

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.

See also overtime rule, permit, and permit restriction.

unreconciled read

MLPI license plate read that has not been committed to an inventory.

See also Mobile License Plate Inventory.

user

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.

See also Active Directory and user group.

User Datagram Protocol

The User Datagram Protocol (UDP) is a connectionless protocol used to exchange data over an IP network. UDP is more efficient than TCP for video transmission because of lower overhead.

user group 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 member of multiple user groups. User groups can also be nested.

See also user.

user level 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 to stay logged on when a threat level is set. The smaller the value, the higher the priority.

See also threat level, user, and user group.

user privilege Privileges that control what operations a user is allowed to perform in Security Center, independent of what entities they can access, and within the constraints set by the software license. User privileges can be inherited from user groups.

See also access right, partition, user, and user group.

V

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

See also license key.

vehicle identification number All vehicles have a manufacturer assigned vehicle identification number (VIN). 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.

virtual zone A subtype of zone entity where the IO linking is done by software. The input and output devices may belong to different units of different types. A virtual zone is controlled by the Zone Manager and only works online. It can be armed and disarmed from Security Desk.

See also hardware zone and zone.

W

watchdog Security Center service installed alongside the Genetec Server service on every server computer, whose sole purpose is to monitor the operation of Genetec Server, and to restart it if abnormal conditions are detected.

Web-based SDK Type of role that exposes the Security Center SDK methods and objects as Web services to support cross-platform development.

Web Client
The client component of Security Center Mobile that provides access to Security Center features from a Web browser. Web Client users connect to Mobile Server to configure and monitor various aspects of your Security Center system.

See also Mobile Server.

wheel imaging
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 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.

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

See also GIS and OGC.

X

Y

Z

zone
Type of entity that monitors a set of inputs and triggers events based on their combined states. These events can be used to control output relays.

See also hardware zone, IO linking, and virtual zone.

Zone activities
Type of investigation task that reports on zone related activities (zone armed, zone disarmed, lock released, lock secured, and so on).

Zone Manager
Type of role that manages virtual zones and triggers events or output relays based on the inputs configured for each zone. It also logs the zone events in a database for zone activity reports.

Zone occupancy
Type of investigation task that reports on the number of vehicles parked in a selected parking zone, and the percentage of occupancy (for university parking only).

See also University Parking Enforcement.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X

Z

Where to find product documentation

You can find our product documentation in the following locations:

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

Technical support

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

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

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

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

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

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

Additional resources

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

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