Product documentation

Security Center includes the following documentation:

- **Security Center Release Notes.** Describes the release in detail, including new features, resolved issues, known issues, and limitations.

- **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.

- **Security Center Administrator Guide.** Provides all the instructions and conceptual information you’ll need to set up, configure, and administer your Security Center system.

- **Getting Started with Security Desk.** A task-oriented introduction to Security Desk that uses real-world scenarios (viewing a camera, searching/exporting video, and managing alarms) to show new users how to use the basic product features.

- **Genetec Security Desk User Guide.** Provides the instructions and conceptual information you need to get started with Security Desk, to monitor and generate reports for AutoVu LPR, Omnicast video surveillance, and Synergis access control systems.

- **Security Center Video Unit Configuration Guide.** Provides the pre-configuration instructions for integrating video units into Security Center, and any configuration steps required for some video unit features to work.

- **Security Center Portable Archive Player User Guide.** Explains how to use the Portable Archive Player to view exported video files.

- **AutoVu Patroller Release Notes.** Describes the AutoVu Patroller release in detail, including new features, resolved issues, known issues, and limitations.

- **AutoVu Hardware Release Notes.** Describes the AutoVu Hardware for this release in detail, including new features, resolved issues, known issues, and limitations.

- **AutoVu Handbook.** Provides AutoVu installers and administrators with a single source of information about installing and configuring AutoVu hardware and software.

- **AutoVu Patroller User Guides.** Quick reference guides to using Patroller, AutoVu’s mobile LPR solution. There is a separate user guide for each Patroller installation type (Law Enforcement, City Parking Enforcement, City Parking Enforcement with Wheel Imaging, University Parking Enforcement, and Mobile License Plate Inventory).

- **AutoVu Connecting the Sharp Camera.** Explains how to power up and connect your Sharp. A printed version is provided in the Sharp box.

- **AutoVu Connecting the SharpX Camera.** Explains how to power up and connect your SharpX. A printed version is provided in the SharpX box.

- **Plugin User Guides.** Introduces you to the plugin features and describes what’s new in the current release. It also explains how to install and configure the plugin in Security Center, and how to use it in Security Desk.

Where can I find the product documentation?

- **Product DVD.** The documentation is available on the product DVD in the Documentation folder. Release notes and installation guides include a direct link to the latest version of the document.

- **Genetec Technical Assistance Portal (GTAP).** The latest version of the documentation is available from GTAP. Note, you’ll need a username and password to log on to GTAP.

- **Online help.** Security Center client applications include online 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 online 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.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product documentation</td>
<td>iii</td>
</tr>
<tr>
<td>Technical support</td>
<td>iv</td>
</tr>
<tr>
<td>About this guide</td>
<td>xvii</td>
</tr>
<tr>
<td><strong>Chapter 1: Introducing AutoVu</strong></td>
<td></td>
</tr>
<tr>
<td>What is AutoVu?</td>
<td>2</td>
</tr>
<tr>
<td>AutoVu hardware components</td>
<td>4</td>
</tr>
<tr>
<td>AutoVu Sharp components</td>
<td>4</td>
</tr>
<tr>
<td>AutoVu SharpX components</td>
<td>4</td>
</tr>
<tr>
<td>Ruggedized touchscreen PC</td>
<td>5</td>
</tr>
<tr>
<td>AutoVu software components</td>
<td>6</td>
</tr>
<tr>
<td>What is Security Center?</td>
<td>6</td>
</tr>
<tr>
<td>What is Patroller?</td>
<td>7</td>
</tr>
<tr>
<td>What is Patroller Config Tool?</td>
<td>7</td>
</tr>
<tr>
<td>What is the Sharp Admin?</td>
<td>7</td>
</tr>
<tr>
<td>How do AutoVu hardware and software components work together?</td>
<td>8</td>
</tr>
<tr>
<td>How AutoVu fixed installations work</td>
<td>8</td>
</tr>
<tr>
<td>How AutoVu mobile installations work</td>
<td>8</td>
</tr>
<tr>
<td><strong>Chapter 2: AutoVu software interface tours</strong></td>
<td></td>
</tr>
<tr>
<td>Security Center Config Tool interface tour</td>
<td>10</td>
</tr>
<tr>
<td>Log on to Config Tool</td>
<td>10</td>
</tr>
<tr>
<td>Log off Config Tool</td>
<td>11</td>
</tr>
<tr>
<td>Close the Config Tool application</td>
<td>11</td>
</tr>
<tr>
<td>Config Tool Home page</td>
<td>12</td>
</tr>
<tr>
<td>Patroller Config Tool interface tour</td>
<td>13</td>
</tr>
<tr>
<td>Open Patroller Config Tool</td>
<td>13</td>
</tr>
<tr>
<td>Close Patroller Config Tool</td>
<td>13</td>
</tr>
<tr>
<td>Patroller Config Tool interface overview</td>
<td>14</td>
</tr>
</tbody>
</table>
Using Patroller Config Tool on a touchscreen ................................................. 15
How to restore a default setting ........................................................................... 15

Sharp Admin interface tour .................................................................................. 16
Log on to the Sharp Admin .................................................................................... 16
Log off the Sharp Admin ......................................................................................... 17
Restart the Sharp unit ............................................................................................. 17
Using the Sharp Admin with SharpX ....................................................................... 17
Sharp Admin interface overview ............................................................................. 18

Benefits of a web-based configuration tool ............................................................. 19

Where to find the most common tasks .................................................................... 20

Chapter 3: AutoVu fixed deployment overview

About the fixed deployment process overview ......................................................... 23
AutoVu deployment prerequisites ............................................................................. 23
Understanding how LPR unit entities are created .................................................. 23
Phase 1: AutoVu hardware installation .................................................................. 24
Phase 2: AutoVu software installation and Sharp upgrade ..................................... 25
Phase 3: Configure Sharp units for a fixed AutoVu system ..................................... 26
Phase 4: Configure LPR Manager for a fixed AutoVu system ................................. 27

Create an LPR Manager ......................................................................................... 27
Configure LPR Manager server, database, and database retention periods .......... 28
Configure LPR Manager Root folder ...................................................................... 29
Connect Security Center to fixed Sharp units ......................................................... 29
Turn on email notification for hotlist hits ............................................................... 30
Activate hotlists on the LPR Manager .................................................................... 30
Activate hotlist filtering ........................................................................................... 31
Set discovery port for fixed Sharp units ................................................................. 31
Set which LPR images the Sharp sends to Security Center .................................... 32
Turn on hotlist matching for fixed Sharp ............................................................... 32
Set fixed Sharp time zone and location ................................................................. 33
Configure updates for Sharps .................................................................................. 33

Phase 5: Configure LPR unit .................................................................................. 34

Create an LPR unit .................................................................................................. 34
Chapter 4: AutoVu mobile deployment overview

About the mobile deployment process overview ......................................... 41
AutoVu deployment prerequisites ................................................................. 41
Understanding how Patroller unit entities are created .............................. 41
Phase 1: AutoVu hardware installation ....................................................... 42
Phase 2: AutoVu software installation and Sharp upgrade ......................... 43
Phase 3: Configure Sharp units for a mobile AutoVu system ...................... 44
Phase 4: Configure LPR Manager for a mobile AutoVu system ................. 45
  Create an LPR Manager ........................................................................... 45
  Configure LPR Manager server, database, and database retention periods .... 46
  Configure LPR Manager Root folder ....................................................... 47
  Set Patroller user group managed by LPR Manager ................................ 47
  Connect Patroller to Security Center ..................................................... 48
  Configure updates for Patrollers and Sharps .......................................... 48
  Turn on email notification for hotlist hits .............................................. 48
  Activate hotlists on the LPR Manager .................................................... 49
  Activate hotlist filtering ....................................................................... 49
  Configure hotlist privacy settings ......................................................... 50
Phase 5: Configure hotlists ...................................................................... 51
  Add a hotlist .......................................................................................... 51
  Configure hotlist properties .................................................................. 52
  Configure advanced hotlist properties .................................................. 52
Fixed installation procedure

What you need
Install your Sharp XGA
Step 1: Mount the Sharp
Step 2: Connect the Sharp
Step 3: Mount the electrical enclosure
Step 4: Finishing up
Install your Sharp EX

Chapter 7: Installing mobile AutoVu hardware

Mobile installation examples for Sharp
Basic mobile installation example
Advanced mobile installation example
Sharp wiring diagram

Mobile installation guidelines for Sharp

Mobile installation procedure for Sharp
What you need
Hardmount installation
Prepare your vehicle
Install your Sharp camera
Install your breakout box
(Optional) Install your Navigator unit
(Optional) Install USB GPS antenna
(Optional) Install tire cameras
Connect cables and wires
Finishing up
Magnetic mount installation
Install your Sharp camera
Connect cables and wires

Mobile installation guidelines

Mobile installation procedure
What you need
About third-party connectors
AutoVu SharpX connections
Chapter 8: Installing Security Center

Chapter 9: Installing Patroller

System requirements .......................... 106
  Patroller system requirements ............... 106
  SQL Express database requirements ......... 107
    Increase SQL server memory ............... 107
Before you install ............................ 109
  Read the Release Notes ...................... 109
  Disable User Account Control (Windows 7 only) .... 109
  Disable Aero Themes (Windows 7 only) ....... 109
About the AutoVu Patroller installation package .......... 110
  Where can I find the installation package .... 110
  Installer languages ....................... 110
  What’s not included ....................... 110
    In-vehicle mapping ...................... 110
    Customized hotlists, permit lists, and overtime configurations .... 110
Installation overview .......................... 111
Installing AutoVu Patroller ...................... 112
  Install AutoVu Patroller ................... 112
  Download latest hotfixes ................. 113
  Install MapInfo files ..................... 113
Chapter 10: Upgrading AutoVu

Upgrading Patroller and Sharp units from Security Center

Before you begin
About AutoVu update files
About zipping sound files
About adding sound files to the Genetec zip file
Enable updates and create update folder
Update AutoVu components

Upgrading Patroller

Before you upgrade.
Read the Release Notes
Backup Patroller database
Close Patroller
Upgrade overview
Upgrading Patroller
Upgrade Patroller database

Upgrade FAQ for Patroller users

Creating a Zones file in Patroller versions 4.4 and later
Where can I find the configuration file from the earlier version?
Are my settings transferred to the latest version?

Chapter 11: Advanced configuration tasks

About advanced configuration

Configure the Sharp for an FTP connection
Configure the Sharp for FTP
Modify the FTP XML

Using a SharpX – Multi system
What is the SharpX – Multi?
Connect and configure cameras for a SharpX – Multi 4-port system

Configuring Sharp Admin security
Why use encryption?
Configure encryption with a Genetec certificate
Install the Genetec certificate on the client machine
Configure encryption with a signed certificate 135

Connecting Sharp units to Patroller 137

Setting up USB support 140
  Set up USB support on the Security Center computer 140
  Install USB batch files on the Security Center computer 140
  Set Root folder and the USB drive letter on the Security Center computer 141
  Set up USB support on the Patroller computer 141
  Install USB batch files on Patroller 141
  (Optional) Install USB autorun 142
  Set Offload folder and the USB drive letter on Patroller 142

Using a SharpX system with multiple LPR Processing Units 144
  About the LPR Processing Unit’s default IP addresses 144
  Change the LPR Processing Unit’s default IP addresses 145

Install the GPS driver 146

Switching images on the Sharp 148

Enabling privacy on individual hotlists 149
  Why enable privacy on a specific hotlist? 149
  How to enable privacy 149

Moving Patroller or LPR units between LPR Managers 151

Chapter 12: Config Tool reference

Common configuration tabs 154
  Identity 154
    Standard information 155
    Specific information 155
  Cameras 156
  Custom fields 157
  Location 158
    Time zone 158
    Location 158
  Hotlist entity 160
    Properties 161
    Advanced 164
LPR Unit entity .................................................. 167
Properties ..................................................... 168
Patroller entity .................................................. 169
Properties ..................................................... 169
User entity ...................................................... 172
Properties ..................................................... 173
  First name, last name, email address ....................... 173
  User status ................................................ 173
  Password .................................................. 173
  Password expiration ....................................... 173
  Limit concurrent logons ................................... 174
  User logon schedule ....................................... 174
Security ....................................................... 174
  User level ................................................ 175
  Archive viewing limitation ............................... 175
  Remote user control ...................................... 175
  Logon supervisor of ...................................... 175
Privileges ..................................................... 176
  Set of privileges ......................................... 176
Workspace ..................................................... 177
  List of active tasks ...................................... 177
  Hot actions .............................................. 177
  Additional settings ....................................... 177
  Force a user to start in full screen mode .............. 178
User group entity ............................................ 179
Properties ..................................................... 180
  Email address ............................................ 180
  Members .................................................. 180
Security ....................................................... 181
  User level ................................................ 181
  Archive viewing limitation ............................... 181
  Logon supervisor of ...................................... 182
Privileges ..................................................... 182
  Set of privileges ......................................... 182
## LPR Manager role
- Properties ........................................ 184
- Resources ........................................ 185
- Servers ........................................... 185
- Database ......................................... 185
- Options .......................................... 185
  - General ........................................ 186
  - Live ........................................... 188
  - Data import .................................... 189
  - Email notification .............................. 190
  - Geocoding ...................................... 192
  - Matching ....................................... 192
  - XML export ..................................... 193
  - XML import ..................................... 195
  - Update provider ................................ 195
  - Hotlist filtering ................................ 195

## LPR administration task
- Units ............................................. 198
- General settings ................................ 198
  - Applications ................................... 199
  - Hotlist ........................................ 201
  - Annotation fields ............................. 202
  - Updates ....................................... 202

## Chapter 13: Patroller Config Tool reference

### General

### Security Center
- Live connection ................................ 207
- Offload ......................................... 209

### Plugin

### Cameras

### Hits
- General ........................................ 213
Chapter 14: Sharp Admin reference

Status
Properties
License
GPS coordinates
Clock
Actions
System resources
Configuration
Network settings
Portal Security
Camera status LED
Support wheel imaging
Camera settings
Sharp
Sharp EX
SharpX
Appendix A: SharpX LED status reference

LED status on the LPR Processing Unit ................................................. 242
  System status ................................................................................. 242
  Camera data-link status .......................................................... 243
LED status on the SharpX camera unit ........................................ 245

Appendix B: AutoVu Sharp and SharpX parts lists

AutoVu Sharp parts ............................................................................ 247
  Fixed AutoVu Sharp parts list .................................................. 247
  Mobile AutoVu Sharp parts list .............................................. 247
  Understanding the Sharp part number .................................... 249
AutoVu SharpX parts ...................................................................... 250
  AutoVu SharpX parts list ......................................................... 250
  Understanding the SharpX part number .................................. 251

Glossary .......................................................................................... 252

Index .................................................................................................. 290
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 5.1 systems.

IMPORTANT  This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

This guide is organized into the following sections:

- **Chapter 1, “Introducing AutoVu”**. This section describes the main features and components of AutoVu, the IP license plate recognition (LPR) solution of Security Center.
- **Chapter 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.
- **Chapter 3, “AutoVu fixed deployment overview”**. This section provides an overview of how to install and configure a fixed AutoVu system.
- **Chapter 4, “AutoVu mobile deployment overview”**. This section provides an overview of how to install and configure a mobile AutoVu system for Law Enforcement.
- **Chapter 5, “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.
- **Chapter 6, “Installing fixed AutoVu hardware”**. This section explains how to install AutoVu in a fixed configuration, such as on a pole.
- **Chapter 7, “Installing mobile AutoVu hardware”**. This section explains how to install AutoVu in a mobile configuration, such as in a vehicle.
- **Chapter 8, “Installing Security Center”**. This section provides a link to the Security Center Installation and Upgrade guide.
- **Chapter 9, “Installing Patroller”**. This section explains how to install AutoVu Patroller on the in-vehicle computer.
- **Chapter 10, “Upgrading AutoVu”**. This section explains how to upgrade the various AutoVu components (e.g. Patroller, Sharp cameras, and other services).
• **Chapter 11, “Advanced configuration tasks”**. This chapter describes the advanced procedures required to configure an AutoVu system. It also describes some extra tasks and features you can use to further customize an AutoVu system for your specific installation.

• **Chapter 12, “Config Tool reference”**. This section describes the main 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.

• **Chapter 13, “Patroller Config Tool reference”**. This section describes all the Patroller Config Tool options you can use to customize Patroller for your particular AutoVu system.

• **Chapter 14, “Sharp Admin reference”**. This section describes all the Sharp Admin options you can use to customize a Sharp unit for your particular AutoVu system.

• **Appendix A, “SharpX LED status reference” on page 241**. This section describes what the different states of the LED indicators mean on the SharpX LPR Processing Unit, and the SharpX camera unit.

• **Appendix B, “AutoVu Sharp and SharpX parts lists” on page 246**. This section lists the parts that are included with the Sharp and SharpX, and explains the components of a Sharp part number.
Introducing AutoVu

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

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click [here](#) for the most recent version of this document.

This section includes the following topics:

- "What is AutoVu?" on page 2
- "AutoVu hardware components" on page 4
- "AutoVu software components" on page 6
- "How do AutoVu hardware and software components work together?" on page 8
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). You can use AutoVu for scofflaw and wanted vehicle identification, city-wide surveillance, parking enforcement, parking permit control, vehicle inventory, security, and access control.
The following diagram shows how a typical AutoVu system works.
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" on page 4
- "AutoVu SharpX components" on page 4
- "Ruggedized touchscreen PC" on page 5

AutoVu Sharp components

The AutoVu Sharp is typically used for fixed installations, and comes in the following models:

- Sharp XGA. Sharp unit that integrates 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.
- Sharp VGA. Same as the Sharp XGA, except with a standard definition (640 x 480) LPR camera for plate capture.
- Sharp EX. Sharp unit that includes an integrated image processor and supports two standard definition NTSC or PAL inputs for external cameras (to be used for the LPR and context cameras).

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

AutoVu SharpX components

The AutoVu SharpX is used for mobile 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. 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, 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.

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 7.

- **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 Admin.** The web-based administrative application used to configure Sharp units.
  
  For more information, see "What is the Sharp Admin?" 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?

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.

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 Admin?

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 Admin, 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" on page 8
- "How AutoVu mobile installations work" on page 8

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 CCTV cameras. The Sharp cameras send each read to Security Desk in real-time. Reads are 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 police 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). Security Desk can also display these reads and hits from patrolling units.
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:

- "Security Center Config Tool interface tour" on page 10
- "Patroller Config Tool interface tour" on page 13
- "Sharp Admin interface tour" on page 16
- "Where to find the most common tasks" on page 20
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 Config Tool" on page 10
• "Log off Config Tool" on page 11
• "Config Tool Home page" on page 12

Log on to Config Tool

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

1  Click Start, then select All Programs > Genetec Security Center 5.1 > 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 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 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.
Config Tool Home page

The Home page resides in the background of Config Tool. You can bring it to the foreground by clicking the Home button or when the task list is empty.

A Home button. Click to show or hide the Home page.
B Search. Search for tasks, tools, and entities in the Config Tool. As you start to type in this field, search results start to appear in the pane below the search field.
C Favorites. Right-click any item (task or tool) to add or remove it from your Favorites.
D Task list. Displays your active tasks as tabs. Click a tab to switch the task workspace.
E Home menu. Click a menu item to switch to a different view.
F Notification tray. Displays important information about your system. It always appears at the upper right corner of the application window. Hold the pointer over an icon to view system information, or click the icon to perform an action.
G Recently used. Lists your recently used items (tasks and tools) in reverse chronological order.
H Click a task icon to open a new task or make that task the active window.
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" on page 13
- "Close Patroller Config Tool" on page 13
- "Patroller Config Tool interface overview" on page 14
- "Using Patroller Config Tool on a touchscreen" on page 15
- "How to restore a default setting" on page 15

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 Patrol- ler 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 13, “Patroller Config Tool reference” on page 204.

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 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 "How to restore a default setting" on page 15.

E Reset to default settings
- Reset all settings to the default state.

F 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.

How to restore 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.

   ![Patroller Config Tool interface](image)

2. To reset a default value, tap or click the orange button next to the setting.
3. Tap or click Apply.
4. Tap Show default value to return to normal view.
Sharp Admin interface tour

The Sharp Admin 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 Admin" on page 16
- "Log off the Sharp Admin" on page 17
- "Restart the Sharp unit" on page 17
- "Using the Sharp Admin with SharpX" on page 17
- "Sharp Admin interface overview" on page 18

Log on to the Sharp Admin

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

- **Sharp name.** The Sharp name is on the label under the Sharp camera's visor. It is typically in the format “Sharp1234”.
- **SharpX name.** The SharpX name is on the back of the LPR Processing Unit. For more information, see "Using the Sharp Admin with SharpX" on page 17.
- **Sharp IP address.** The default IP address is 192.168.10.100.
- **SharpX IP address.** 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 Admin with SharpX" on page 17.

To log on to the Sharp Admin:

1. Open your Web browser, and go to http://<Sharp name or IP address>/portal/.
   
   **EXAMPLE** if your Sharp camera name is Sharp1234, enter http://Sharp1234/portal/.
   
   The Sharp Admin appears.

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

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

3. Select your language, then click OK.

   The Sharp Admin opens to the Status page.
Log off the Sharp Admin

- To log off the Sharp Admin, 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 Admin.

1. Log on to the Sharp Admin.
2. Go to the Status page.
3. Click Reboot unit, then click OK to confirm.
   The connection to the Sharp Admin is momentarily lost.
4. Wait a few minutes to allow the Sharp to restart, then refresh the browser window.

Using the Sharp Admin with SharpX

There is an important difference between connecting to a Sharp and connecting to a SharpX. For SharpX units, the Sharp Admin 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 Admin 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 Admin, see "Sharp Admin reference" on page 224.
Sharp Admin interface tour

This section takes you on a tour of the main areas of the Sharp Admin user interface. For more information on Sharp Admin settings, see "Sharp Admin reference" on page 224.

Sharp Admin 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.

Help
Opens the contextual help for the Sharp Admin.

Note Please note the following:
• Pressing F1 on your keyboard accesses the browser's help (e.g. Internet Explorer), not the Sharp Admin help.
• Contextual help is designed for use with Adobe Reader. If you use another PDF viewer, the contextual help may not jump to the correct page in the documentation. You can install Adobe Reader from the Security Center installation package.
• If your browser has a pop-up blocker enabled, it may prevent the contextual help from opening.

Main menu
Shows the different pages of the Sharp Admin. Each page contains the related settings for that category. For example, the Configuration page includes settings for configuring your Sharp camera.
Benefits of a web-based configuration tool

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

- **Open Sharp Admins 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 Admins open within the same Web browser.

- **Secure connection.** You can log on to the Sharp Admin securely using an HTTPS protocol with SSL encryption. For more information, see "Configuring Sharp Admin security" on page 131.

- **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.

This table only lists a few of the common settings you can configure. For a complete list of all the settings in Config Tool, Patroller Config Tool, and the Sharp Admin, see the following chapters:

- Chapter 12, “Config Tool reference” on page 153.
- Chapter 13, “Patroller Config Tool reference” on page 204.
- Chapter 14, “Sharp Admin reference” on page 224.

<table>
<thead>
<tr>
<th>Common tasks</th>
<th>Security Center Config Tool</th>
<th>Patroller Config Tool</th>
<th>Sharp Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring users and user groups</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuring LPR root folder</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connecting Patroller to Security Center</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Configuring/activating hotlists</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enabling New Wanted</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Configuring Patroller sound management</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuring New Wanted attributes</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuring New Wanted categories</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enabling Manual Capture</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Configuring database and database retention</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adding cameras to Patroller</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
## Common tasks

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

This section provides an overview of how to install and configure a fixed AutoVu system.

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

**NOTE** The AutoVu product allows you to customize a deployment in a variety of ways. For this reason, only the tasks for a typical deployment are provided.

This section includes the following topics:

- "About the fixed deployment process overview" on page 23
- "AutoVu deployment prerequisites" on page 23
- "Understanding how LPR unit entities are created" on page 23
- "Phase 1: AutoVu hardware installation" on page 24
- "Phase 2: AutoVu software installation and Sharp upgrade" on page 25
- "Phase 3: Configure Sharp units for a fixed AutoVu system" on page 26
- "Phase 4: Configure LPR Manager for a fixed AutoVu system" on page 27
- "Phase 5: Configure LPR unit" on page 34
- "Phase 6: Configure hotlists" on page 37
About the fixed deployment process overview

The deployment process is divided into phases. Each phase explains at a high level what you need to do, and provides the basic steps for you to complete the task. For the more complex configuration tasks, you’ll find links to other sections in this guide (e.g. the Config Tool reference section) that provide the more detailed information you’ll need to complete the task.

AutoVu deployment prerequisites

This section provides an overview of the prerequisites for deploying an AutoVu system.

NOTE The AutoVu product allows you to customize a deployment in a wide variety of ways. For that reason, only the tasks for a typical deployment are provided.

Before you deploy AutoVu, do the following:

- Read the various release notes:
  - Security Center Release Notes
  - AutoVu Hardware Release Notes
  - AutoVu Patroller Release Notes
  For more information, see "Product documentation" on page iii.

- Have the information from your initial site survey on hand when you install the AutoVu hardware. For example, before installing the hardware you should know how high to install the Sharp camera, how many lanes you need to capture, and what pan/tilt angles are required to capture plates.

Understanding how LPR unit entities are created

The Security Center LPR Manager role manages and controls fixed Sharp units. It automatically detects fixed Sharps connected to the network through the LPR Manager discovery port, and then creates an LPR unit entity for each fixed Sharp detected.
Phase 1: AutoVu hardware installation

This is what you need to do to install fixed AutoVu hardware. You’ll see what a typical fixed installation looks like, read the various safety precautions and guidelines, and learn how to connect the related hardware components.

1 Read the hardware-related prerequisites.
   For more information, see:
   - "Hardware specifications and system requirements" on page 63
   - "About the hardware installation procedures in this guide" on page 63
   - "Safety precautions" on page 63

2 See an example of a fixed installation, and read the wiring instructions.
   For more information, see:
   - "Fixed installation example" on page 67
   - "Sharp wiring diagram" on page 68

3 Install the fixed AutoVu hardware.
   For more information, see:
   - "Fixed installation guidelines" on page 69
   - "Fixed installation procedure" on page 73

Related topics:
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 1: AutoVu hardware installation.
Phase 2: AutoVu software installation and Sharp upgrade

This is what you need to do to install and upgrade Security Center, and upgrade the Sharp units you already have deployed in the field so you can use them with 5.1 SR2.

1. Install and upgrade Security Center.
   For more information, see "Installing Security Center" on page 104

2. Upgrade Sharp services for use with 5.1 SR2.
   For more information on how to upgrade Sharp units for use with 5.1 SR2, contact your Genetec representative.

3. Upgrade firmware for Sharp 2.0 units with 1 GB of RAM.
   For more information, see "Upgrading Patroller and Sharp units from Security Center" on page 115.

4. Upgrade firmware for Sharp 1.5 units, and Sharp 2.0 units with 512 MB of RAM.
   For more information on how to upgrade Sharp units for use with 5.1 SR2, contact your Genetec representative.

Related topics:
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 2: AutoVu software installation and Sharp upgrade.
Phase 3: Configure Sharp units for a fixed AutoVu system

This is what you need to do to log on to the Sharp Admin 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.

Before you begin: Read about the Sharp Admin and take a tour of the user interface. This section also shows you how to log on and off the Sharp Admin. For more information, see "Sharp Admin interface tour" on page 16.

1. Log on to the Sharp Admin.
2. Go to the Live feed page to verify that the Sharp unit is working.
   For more information, see "Live feed" on page 237.
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 230.
   b. Under Camera settings, configure the settings for the type of Sharp you’re using.
      For more information, see "Camera settings" on page 231.
   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 "Analytics" on page 233.
   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 234.
   e. Configure the other settings as desired for your specific installation (e.g. set Sharp Admin encryption, turn off the Sharp LED, etc).
      For more information, see "Configuration" on page 229.

Related topics:
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 3: Configure Sharp units for a fixed AutoVu system.
Phase 4: Configure LPR Manager for a fixed AutoVu system

This is what you need to do in Config Tool to configure the LPR Manager role for a fixed AutoVu system. The LPR Manager is the main software component of Security Center that controls LPR-related entities and tasks. You’ll learn how to set the root folder, configure database retention periods, configure the hotlist settings that apply to all hotlists controlled by the LPR Manager, and more.

Before you begin: Read about Config Tool and take a tour of the user interface. This section also shows you how to log on and off Config Tool. For more information, see "Security Center Config Tool interface tour" on page 10.

This section includes the following topics:

- "Create an LPR Manager" on page 27
- "Configure LPR Manager server, database, and database retention periods" on page 28
- "Configure LPR Manager Root folder" on page 29
- "Connect Security Center to fixed Sharp units" on page 29
- "Turn on email notification for hotlist hits" on page 30
- "Activate hotlists on the LPR Manager" on page 30
- "Activate hotlist filtering" on page 31
- "Set discovery port for fixed Sharp units" on page 31
- "Set which LPR images the Sharp sends to Security Center" on page 32
- "Turn on hotlist matching for fixed Sharp" on page 32
- "Set fixed Sharp time zone and location" on page 33
- "Configure updates for Sharps" on page 33

Create an LPR Manager

The LPR Manager controls AutoVu-related entities and options. For more information, see "LPR Manager role" on page 183.

1 Log on to Config Tool.

2 From the Config Tool Home page, go to System > Roles, and then click the Add button (➕).

   The role creation wizard appears.

3 Select 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.
Phase 4: Configure LPR Manager for a fixed AutoVu system

- **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.

**Related topics:**
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a fixed AutoVu system.

**Configure LPR Manager server, database, and database retention periods**

1 Log on to Config Tool.

2 From the 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.

  For more information on databases, see the Config Tool help.

4 Select the Options tab, click General settings, and then specify the database retention periods.

  For more information, see "General" on page 186.

5 Click Apply.

**Related topics:**
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a fixed AutoVu system.
Configure LPR Manager Root folder

The root folder is the main folder on the computer hosting the LPR Manager.

1. Log on to Config Tool.
2. From the Config Tool Home page, go to System > Roles, and then click the LPR Manager you want to configure.
3. Select the Options tab, click General settings, and then enter the path to the root folder.
   Once you have set the root folder, the LPR Manager creates the required subfolders. For more information, see "General" on page 186.
4. Click Apply.

Related topics:
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a fixed AutoVu system.

Connect Security Center to fixed Sharp units

The listening port is used by the LPR Manager to connect to fixed Sharp units. The default value is 8731. You set this port from the LPR Manager Options tab, under Live.

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

1. Log on to Config Tool.
2. From the Config Tool Home page, go to System > Roles, and then click the LPR Manager you want to configure.
3. Click the Options tab and 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 188.
5. Click Apply.

After you are done: If you haven't already done so, perform the procedure described in "Phase 3: Configure Sharp units for a fixed AutoVu system" on page 26.

Related topics:
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a fixed AutoVu system.
**Turn on email notification for hotlist hits**

Before you begin: To use this feature, you need to do the following:

- On the computer hosting the LPR Manager, you’ll need to configure the mail server in Server Admin. For more information, see the Config Tool help.
- Set the email address in each hotlist’s Properties tab. For more information, see "Hotlist entity" on page 160.

To turn on hotlist email notification

1. Log on to Config Tool.
2. From the Config Tool Home page, go to System > Roles, then click the LPR Manager to configure.
3. Select the LPR Manager Options tab.
4. For Email notification settings, click On.
5. Click Apply.

**Related topics:**

- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a fixed AutoVu system.

**Activate hotlists on the LPR Manager**

You need to tell the LPR Manager which hotlists you want it to monitor.

Before you begin: You need to add and configure your hotlists. For more information, see "Phase 6: Configure hotlists" on page 37.

1. Log on to Config Tool.
2. From the Config Tool Home page, go to System > Roles, then click the LPR Manager you want to configure.
3. Select the Properties tab.
4. Under Hotlists, choose which hotlists you want the LPR Manager to manage.
   For more information, see "Properties" on page 184.
5. Click Apply.

**Related topics:**

- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a fixed AutoVu system.
Activate hotlist filtering

Specify what the LPR Manager should do if it detects a hotlist with invalid characters.

1. Log on to Config Tool.
2. From the Config Tool Home page, go to System > Roles, and then click the LPR Manager you want to configure.
3. Select the Options tab.
4. Configure how the LPR Manager should filter hotlist characters.
   For more information, see "Hotlist filtering" on page 195.
5. Click Apply.

Related topics:
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a fixed AutoVu system.

Set discovery port for fixed Sharp units

The LPR Manager uses the discovery port to find fixed Sharp units on the network. You configure the port in the LPR Manager Properties tab. You’ll also need to modify settings in the Sharp Admin.

1. Log on to Config Tool.
2. From the 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 Network, enter the port number used to discover fixed Sharps.
   Each LPR Manager must use a unique discovery port. For more information, see "Properties" on page 184.
5. Click Apply.

After you are done: The port number you chose must match the port number in the Sharp Admin. For more information, see "Extension" on page 234.

Related topics:
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a fixed AutoVu system.
Set which LPR images the Sharp sends to Security Center

You can choose which Sharp images are sent to Security Center from the LPR Manager Options tab, under Live.

1. Log on to Config Tool.
2. From the Config Tool Home page, go to System > Roles, and then click the LPR Manager you want to configure.
3. Select the Options tab, select Live, and click On.
4. Configure which Sharp images are sent to Security Center. For more information, see "Live" on page 188.
5. Click Apply.

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

Related topics:
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a fixed AutoVu system.

Turn on hotlist matching for fixed Sharp

You turn on hotlist matching for fixed Sharps from the LPR Manager Options tab, under Matching.

1. Log on to Config Tool.
2. From the Config Tool Home page, go to System > Roles, and then click the LPR Manager you want to configure.
3. Select the Options tab, then turn on Matching. For more information, see "Matching" on page 192.
4. Click Apply.

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

Related topics:
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a fixed AutoVu system.
Set fixed Sharp time zone and location

You can set the time zone and location of a fixed Sharp from the LPR unit Location tab. 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.

For more information, see "Location" on page 158.

Related topics:
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a fixed AutoVu system.

Configure updates for Sharps

You can send hotfixes and updates to Sharp units from Config Tool. For more information, see "Upgrading Patroller and Sharp units from Security Center" on page 115.

Related topics:
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a fixed AutoVu system.
Phase 5: Configure LPR unit

This is what you need to do to in Config Tool to create an LPR unit (fixed Sharp) manually. You can also link a camera entity to a fixed Sharp in order to monitor the video feed from the Sharp’s context camera.

Before you begin: Read about Config Tool and take a tour of the user interface. This section also shows you how to log on and off Config Tool. For more information, see “Security Center Config Tool interface tour” on page 10.

This section includes the following topics:
- "Create an LPR unit" on page 34
- "Link a camera to an LPR unit" on page 35

Create an LPR unit

The LPR Manager will automatically detect fixed Sharps on the network, and create LPR Unit entities for them. But if the Sharp is not on the same network as the LPR Manager, you’ll need to create an LPR Unit entity manually.

1  Log on to Config Tool.
2  From the Config Tool Home page, go to System > Roles, and then click the LPR Manager you want to configure.
3  Click the Add button ( ) to add an LPR unit.
   The LPR unit creation wizard appears.
4  In the Unit information page, do the following:
   •  Name. Name of the Sharp unit in Security Center. It is advisable to simply use the factory assigned unit name. This name happens to be the machine name by which the unit is identified on the network. It takes the form SHARPxxxx where xxxx is a four-digit number. This name is printed on a label that is placed either on the side of the unit or under the visor.
   •  IP address. IP address of the unit. To find the IP address, ping the unit using its factory assigned name.
   •  Port. This is the port that the LPR Manager uses to send commands to the unit. The default value is 8001. Typically, you do not need to change it.
   •  LPR Manager. Click the drop-down list and select the LPR Manager that is going to manage this unit.
5  Click Next and enter the Partition information.
   For more information on partitions, see the Config Tool help.
6  Click Next, Next, and Finish.
   The new LPR unit should appear under its LPR Manager.
Phase 5: Configure LPR unit

7 (Optional) Select the Properties tab and associate Omnicast cameras with the Sharp unit if necessary. For more information, see "Link a camera to an LPR unit" on page 35.

8 (Optional) Select the Location tab and specify the time zone and location of the Sharp unit. For more information, see "Location" on page 158.

9 (Optional) Select the Actions tab and program event-to-action for this Sharp unit. For more information on programming event-to-actions, see the Config Tool help.

10 Click Apply.

After you are done: In the Sharp Admin, configure the Sharp to send LPR data to Security Center. For more information, see "Extension" on page 234.

Related topics:
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 5: Configure LPR unit.

Link a camera to an LPR unit

You can link a video camera to a Sharp camera so that you can monitor what fixed Sharp units are reading. You can also use the Sharp as a video camera to stream live video.

Before you begin: You need an Omnicast license to add a video camera to Security Center. You’ll also need to add the camera to the Archiver before linking it to an LPR unit. Once the cameras are available in Security Center, you can link one of those cameras to the Sharp. For more information on Omnicast and Archiver, see the Config Tool help.

1 Log on to Config Tool.

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

3 Expand the LPR Manager, and then select the LPR unit you want to configure.

4 Select the Properties tab.

5 Under Devices, click the Add button ( ) to add a device.

   All available cameras on your system are listed in a dialog box.

6 Select one or more cameras from the list and click Add.

   For information on fine-tuning camera settings, see the Config Tool help.

7 Click Apply.

Live video from the selected cameras will be displayed along with the LPR image and the context image produced by the Sharp unit when an LPR event is displayed by a Monitoring task in the Security Desk.

Related topics:
- Go back to AutoVu fixed deployment overview.
• Go to top of Phase 5: Configure LPR unit.
Phase 6: Configure hotlists

This is what you need to do in Config Tool to add and configure hotlists. You’ll learn how to add a hotlist, and how to configure the settings that apply to individual hotlists.

Before you begin: Read about Config Tool and take a tour of the user interface. This section also shows you how to log on and off Config Tool. For more information, see "Security CenterConfig Tool interface tour" on page 10.

This section includes the following topics:

- "Add a hotlist" on page 37
- "Configure hotlist properties" on page 37
- "Configure advanced hotlist properties" on page 38
- "Hotlist hit notification features" on page 38

Add a hotlist

You add a hotlist entity from the Config Tool Home page.

1. Log on to Config Tool.
2. From the 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 Config Tool help.
3. Complete the Basic information.
   
   For more information, see the Config Tool help.
4. Complete the Partition information.
   
   For more information, see the Config Tool help.
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.

Related topics:

- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 6: Configure hotlists.

Configure hotlist properties

You configure the required hotlist properties (hotlist priority, hotlist path, attributes, and so on) from the hotlist Properties tab.
1 Log on to Config Tool.
2 From the Config Tool Home page, go to LPR > Hotlists.
3 Select a hotlist from the list.
4 Select the Properties tab.
5 Configure the hotlist sound file path, color, email address, and other hotlist properties.
   For more information, see "Properties" on page 161.
6 Click Apply.

Related topics:
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 6: Configure hotlists.

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 Config Tool.
2 From the Config Tool Home page, go to LPR > Hotlists.
3 Select a hotlist from the list.
4 Select the Advanced tab.
5 Configure the hotlist path and other hotlist properties.
   For more information, see "Advanced" on page 164.
6 Click Apply.

Related topics:
- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 6: Configure hotlists.

Hotlist hit notification features
AutoVu has a number of features to notify you when a hotlist hit occurs.

Types of hotlist hit email notifications
There are two different ways that Security Center can send email notifications about hotlist hits:
1 Send a notification to the email address that was entered in the hotlist’s Advanced tab.
   For more information, see "Advanced" on page 164.
Phase 6: Configure hotlists

2 Send a notification to the email address that was entered in the hotlist data file for that particular hotlist entry. The email address is contained in the hotlist source file (the .txt file) and each record in the hotlist can have an email address associated with it. For more information, see “Properties” on page 161.

About the notification email field in hotlist source files

In the hotlist source file (the .txt file) you can specify a single email address to which an email will be sent when a Hotlist hit occurs against this particular Hotlist entry. You can choose whatever name you want for the notification email address attribute but you must use the same attribute name for each Hotlist entity that contains notification email addresses.

What is in a hotlist hit notification email?

The hotlist hit notification email contains the hit information (matched plate number, patroller name, user, hotlist name and priority) in the message body and optional image attachments. You choose which images you want to send (license plate, context, overview) from the LPR Manager Email notification options. For more information, see "Email notification" on page 190.

About hotlist hit notification logs

You can log hotlist hit notifications to keep track of who has received hotlist email notifications from Security Center. The log entry includes the date and time (in UTC) the email was sent and the recipient email address.

For more information, see "Email notification" on page 190.

NOTE To comply with privacy laws, Security Center does not retain the notification email and its contents.

Related topics:

- Go back to AutoVu fixed deployment overview.
- Go to top of Phase 6: Configure hotlists.
AutoVu mobile deployment overview

This section provides an overview of how to install and configure a mobile AutoVu system for Law Enforcement.

IMPORTANT  This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

NOTE  The AutoVu product allows you to customize a deployment in a variety of ways. For this reason, only the tasks for a typical deployment are provided.

This section includes the following topics:

- "About the mobile deployment process overview" on page 41
- "AutoVu deployment prerequisites" on page 41
- "Understanding how Patroller unit entities are created" on page 41
- "Phase 1: AutoVu hardware installation" on page 42
- "Phase 2: AutoVu software installation and Sharp upgrade" on page 43
- "Phase 3: Configure Sharp units for a mobile AutoVu system" on page 44
- "Phase 4: Configure LPR Manager for a mobile AutoVu system" on page 45
- "Phase 5: Configure hotlists" on page 51
- "Phase 6: Configure Patroller unit settings from Security Center" on page 56
- "Phase 7: Configure Patroller" on page 58
About the mobile deployment process overview

The deployment process is divided into phases. Each phase explains at a high level what you need to do, and provides the basic steps for you to complete the task. For the more complex configuration tasks, you’ll find links to other sections in this guide (e.g. the Config Tool reference section) that provide the more detailed information you’ll need to complete the task.

AutoVu deployment prerequisites

This section provides an overview of the prerequisites for deploying an AutoVu system.

NOTE The AutoVu product allows you to customize a deployment in a wide variety of ways. For this reason, only the tasks for a typical deployment are provided.

Before you deploy AutoVu, do the following:

• Read the various release notes:
  • Security Center Release Notes
  • AutoVu Hardware Release Notes
  • AutoVu Patroller Release Notes
  For more information, see "Product documentation" on page iii.

• Have the information from your initial site survey on hand when you install the AutoVu hardware. For example, before installing the hardware you should know how high to install the Sharp camera, how many lanes you need to capture, and what pan/tilt angles are required to capture plates.

Understanding how Patroller unit entities are created

The Security Center LPR Manager role manages and controls Patrollers. It automatically detects Patrollers on the network and adds them to the Security Center system. The LPR Manager creates a Patroller entity when a Patroller application connects to Security Center via a designated LPR Manager.
Phase 1: AutoVu hardware installation

This is what you need to do to install mobile AutoVu hardware. You’ll see what a typical mobile installation looks like, read the various safety precautions and guidelines, and learn how to connect the related hardware components.

1. Read the hardware-related prerequisites.
   
   For more information, see:
   
   - "Hardware specifications and system requirements" on page 63
   - "About the hardware installation procedures in this guide" on page 63
   - "Safety precautions" on page 63

2. See an example of a mobile installation, and read the wiring instructions.
   
   For more information, see:
   
   - "Mobile installation guidelines" on page 94

3. Install the mobile AutoVu hardware.
   
   For more information, see:
   
   - "Mobile installation procedure" on page 95

Related topics:

- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 1: AutoVu hardware installation.
Phase 2: AutoVu software installation and Sharp upgrade

This is what you need to do to install and upgrade Security Center and Patroller, and upgrade the Sharp units you already have deployed in the field so you can use them with 5.1 SR2.

1. Install and upgrade Security Center.
   For more information, see "Installing Security Center" on page 104.

2. Install and upgrade Patroller.
   For more information, see "Installing Patroller" on page 105.

3. Upgrade Sharp services for use with 5.1 SR2.
   For more information on how to upgrade Sharp units for use with 5.1 SR2, contact your Genetec representative.

4. Upgrade firmware for SharpX units.
   For more information, see "Upgrading Patroller and Sharp units from Security Center" on page 115.

Related topics:

- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 2: AutoVu software installation and Sharp upgrade.
Phase 3: Configure Sharp units for a mobile AutoVu system

This is what you need to do to log on to the Sharp Admin and configure the Sharp. You’ll learn how to view the live video feed, configure the IP address and read strategy, and more.

**Before you begin:** Read about the Sharp Admin and take a tour of the user interface. This section also shows you how to log on and off the Sharp Admin. For more information, see "Sharp Admin interface tour" on page 16.

1. Log on to the Sharp Admin.
2. Go to the Live feed page to verify that the Sharp unit is working.
   For more information, see "Live feed" on page 237.
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 230.
      **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 144
   b. Under Camera settings, configure the settings for the type of Sharp you’re using.
      For more information, see "Camera settings" on page 231.
   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 "Analytics" on page 233.
   d. Under Extension, configure the Sharp to send LPR data to Patroller.
      For more information, see "Extension" on page 234.
   e. Configure the other settings as desired for your specific installation (e.g. set Sharp Admin encryption, turn off the Sharp LED, etc). For more information, see "Configuration" on page 229.

**Related topics:**
- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 3: Configure Sharp units for a mobile AutoVu system.
Phase 4: Configure LPR Manager for a mobile AutoVu system

This is what you need to do in Config Tool to configure the LPR Manager role for a mobile AutoVu system. The LPR Manager is the main software component of Security Center that controls LPR-related entities and tasks. You’ll learn how to set the root folder, configure database retention periods, configure the hotlist settings that apply to all hotlists controlled by the LPR Manager, and more.

Before you begin: Read about Config Tool and take a tour of the user interface. This section also shows you how to log on and off Config Tool. For more information, see "Security Center Config Tool interface tour" on page 10.

This section includes the following topics:

- "Create an LPR Manager" on page 45
- "Configure LPR Manager server, database, and database retention periods" on page 46
- "Configure LPR Manager Root folder" on page 47
- "Set Patroller user group managed by LPR Manager" on page 47
- "Connect Patroller to Security Center" on page 48
- "Configure updates for Patrollers and Sharps" on page 48
- "Turn on email notification for hotlist hits" on page 48
- "Activate hotlists on the LPR Manager" on page 49
- "Activate hotlist filtering" on page 49
- "Configure hotlist privacy settings" on page 50

Create an LPR Manager

The LPR Manager controls AutoVu-related entities and options. For more information, see "LPR Manager role" on page 183.

1. Log on to Config Tool.
2. From the Config Tool Home page, go to System > Roles, and then click the Add button (➕).
   The role creation wizard appears.
3. Select 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.
Phase 4: Configure LPR Manager for a mobile AutoVu system

- **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.

**Related topics:**
- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a mobile AutoVu system.

---

Configure LPR Manager server, database, and database retention periods

1 Log on to Config Tool.

2 From the 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.

For more information on databases, see the Config Tool help.

4 Select the Options tab, click General settings, and then specify the database retention periods.

For more information, see "General" on page 186.

5 Click Apply.

**Related topics:**
- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a mobile AutoVu system.
Configure LPR Manager Root folder

The root folder is the main folder on the computer hosting the LPR Manager.

1. Log on to Config Tool.
2. From the Config Tool Home page, go to System > Roles, and then click the LPR Manager you want to configure.
3. Select the Options tab, click General settings, and enter the path to the root folder.
   Once you have set the root folder, the LPR Manager creates the required subfolders. For more information, see "General" on page 186.
4. Click Apply.

Related topics:
- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a mobile AutoVu system.

Set Patroller user group managed by LPR Manager

For each LPR Manager role on your system, you need to set the Patroller user group that it should manage. You configure this option when you want Patroller users to log on to Patroller with a username and password.

Before you begin: You need to configure users and user groups in Config Tool. For more information, see the Config Tool help.

1. Log on to Config Tool.
2. From the Config Tool Home page, go to System > Roles, and then click the LPR Manager you want to configure.
3. Click the Properties tab.
4. Under User group for Patrollers, select the user group you want the LPR Manager to manage.
   NOTE If you want Patroller to ask for a username and password at log on, you need to open Patroller Config Tool to enable that option. For more information, see "General" on page 205.
5. Click Apply.

Related topics:
- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a mobile AutoVu system.
Phase 4: Configure LPR Manager for a mobile AutoVu system

Connect Patroller to Security Center

You need to connect Patroller to Security Center so that Patroller is discovered by the LPR Manager role. To do this, you need to configure settings in both Config Tool and Patroller Config Tool.

1 In Config Tool, do the following:
   a Log on to Config Tool.
   b From the Config Tool Home page, go to System > Roles, and then click the LPR Manager you want to configure.
   c Select Options, and then configure the settings under Live.
      For more information, see "Live" on page 188.

2 In Patroller Config Tool, do the following:
   a Open Patroller Config Tool.
   b Go to Security Center, and then configure the settings under Live connection.
      For more information, see "Live connection" on page 207.

Related topics:

- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a mobile AutoVu system.

Configure updates for Patrollers and Sharps

You can send hotfixes and updates to Patrollers and Sharp units from Config Tool. For more information, see "Upgrading Patroller and Sharp units from Security Center" on page 115.

Related topics:

- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 4: Configure LPR Manager for a mobile AutoVu system.

Turn on email notification for hotlist hits

Before you begin: To use this feature, you need to do the following:

- On the computer hosting the LPR Manager, you’ll need to configure the mail server in Server Admin. For more information, see the Config Tool help.
- Set the actual email address for each hotlist in each hotlist's Properties tab. For more information, see "Hotlist entity" on page 160.

To turn on hotlist email notification

1 Log on to Config Tool.
2 From the Config Tool Home page, go to System > Roles, and then click the LPR Manager you want to configure.
3 Select the LPR Manager Options tab.
4 For Email notification settings, click On.
5 Click Apply.

Related topics:
• Go back to AutoVu mobile deployment overview.
• Go to top of Phase 4: Configure LPR Manager for a mobile AutoVu system.

Activate hotlists on the LPR Manager

You need to tell the LPR Manager which hotlists you want it to monitor.

Before you begin: You need to add and configure your hotlists. For more information, see "Phase 5: Configure hotlists" on page 51.

1 Log on to Config Tool.
2 From the 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 Hotlists, choose which hotlists you want the LPR Manager to manage.
   For more information, see "Properties" on page 184.
5 Click Apply.

Related topics:
• Go back to AutoVu mobile deployment overview.
• Go to top of Phase 4: Configure LPR Manager for a mobile AutoVu system.

Activate hotlist filtering

Specify what the LPR Manager should do if it detects a hotlist with invalid characters.

1 Log on to Config Tool.
2 From the Config Tool Home page, go to System > Roles, and then click the LPR Manager you want to configure.
3 Select the Options tab.
4 Configure how the LPR Manager should filter hotlist characters.
   For more information, see "Hotlist filtering" on page 195.
5 Click Apply.
Phase 4: Configure LPR Manager for a mobile AutoVu system

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 Config Tool.
2  From the Config Tool Home page, go to LPR > General settings.
3  Select Applications, then configure the privacy settings
   For more information, see "Applications" on page 199.
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 164.

Related topics:

• Go back to AutoVu mobile deployment overview.
• Go to top of Phase 4: Configure LPR Manager for a mobile AutoVu system.
Phase 5: Configure hotlists

This is what you need to do in Config Tool to add and configure hotlists. You’ll learn how to add a hotlist, and how to configure the settings that apply to individual hotlists.

Before you begin: Read about Config Tool and take a tour of the user interface. This section also shows you how to log on and off Config Tool. For more information, see "Security Center Config Tool interface tour" on page 10.

This section includes the following topics:

- "Add a hotlist" on page 51
- "Configure hotlist properties" on page 52
- "Configure advanced hotlist properties" on page 52
- "Hotlist hit notification features" on page 52
- "Managing large hotlists" on page 53

Add a hotlist

You add a hotlist entity from the Config Tool Home page.

1. Log on to Config Tool.
2. From the 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 Config Tool help.
3. Complete the Basic information.
   For more information, see the Config Tool help.
4. Complete the Partition information.
   For more information, see the Config Tool help.
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.

Related topics:

- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 5: Configure hotlists.
Configure hotlist properties

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

1. Log on to Config Tool.
2. From the 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 161.
6. Click Apply.

Related topics:
- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 5: Configure hotlists.

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 Config Tool.
2. From the 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 164.
6. Click Apply.

Related topics:
- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 5: Configure hotlists.

Hotlist hit notification features

AutoVu has a number of features to notify you when a hotlist hit occurs.

Types of hotlist hit email notifications

There are two different ways that Security Center can send email notifications about hotlist hits:
1. Send a notification to the email address that was entered in the hotlist’s Advanced tab. For more information, see "Advanced" on page 164.

2. Send a notification to the email address that was entered in the hotlist data file for that particular hotlist entry. The email address is contained in the hotlist source file (the .txt file) and each record in the hotlist can have an email address associated with it. For more information, see "Properties" on page 161.

About the notification email field in hotlist source files

In the hotlist source file (the .txt file) you can specify a single email address to which an email will be sent when a Hotlist hit occurs against this particular Hotlist entry. You can choose whatever name you want for the notification email address attribute but you must use the same attribute name for each Hotlist entity that contains notification email addresses.

What is in a hotlist hit notification email?

The hotlist hit notification email contains the hit information (matched plate number, patroller name, user, hotlist name and priority) in the message body and optional image attachments. You choose which images you want to send (license plate, context, overview) from the LPR Manager Email notification options. For more information, see "Email notification" on page 190.

About hotlist hit notification logs

You can log hotlist hit notifications to keep track of who has received hotlist email notifications from Security Center. The log entry includes the date and time (in UTC) the email was sent and the recipient email address.

For more information, see "Email notification" on page 190.

NOTE To comply with privacy laws, Security Center does not retain the notification email and its contents.

Related topics:
- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 5: Configure hotlists.

Managing large hotlists

Hotlists with millions of entries (e.g. 2.5 million or more) require much more CPU processing power and memory than smaller hotlists. Large hotlists can also return more false hits depending on the number of Optical Character Recognition (OCR) equivalent characters (e.g. “B” and “8”, “1” and “L”, etc). Use the procedures in this section to maximize the efficiency of Patroller and Security Center when using large hotlists.
Phase 5: Configure hotlists

Turn on SimpleMatcher

SimpleMatcher reduces the LPR matching mechanism in order to minimize the number of false hits that can occur. For example, if a license plate includes a “B” character, the LPR matcher may also see this as an “8”. This can result in a number of false hits. Turning on SimpleMatcher reduces the chance of the LPR matcher mistaking a “B” for an “8”, as well as for other OCR equivalent characters.

1. Open Patroller Config Tool.
2. Go to Advanced > Hit hotlist, and turn on SimpleMatcher.

For more information, see "Hit hotlist" on page 222.

Modify LPR matcher settings

You can reduce or turn off OCR equivalence when using very large hotlists. High OCR may result in plate reads matching many other plates in the hotlist because of the OCR equivalent characters.

Set the number of OCR equivalent characters in the MatchersSettings.xml file in the Security Center program folder. You also need to open the Server Admin console to apply the changes, and then restart the Directory.

1. In the Genetec Security Center program folder, open MatchersSettings.xml.
2. Make changes to the PerLengthSetting OCR equivalents and differences:
   - NumberOCREquiAllowed=0, 1, or 2 (zero turns the feature off).
3. Save the file.
4. From a web browser, open the Server Admin console by typing //<server>/genetec/console#/Commands.
5. From the All commands page, click UpdateAutoVuGlobalSettings.
6. Close the Server Admin console.
7. From a web browser, open the Server Admin by typing //<server>/genetec.
8. Click the Directory tab.

Managing large hotlists with multiple LPR Managers

By default, Security Center uses a single process for every LPR Manager on the system. For example, even if you have ten different LPR Manager roles on the same computer, Security Center uses a single process called GenetecLicensePlateManager32.exe to run them. This can cause CPU memory issues if you are using large hotlists on several of the LPR Managers.

To better manage the memory load caused by the large hotlists, you can configure Security Center to create a separate process for each LPR Manager.
1. Log on to Config Tool.
2. From the Config Tool Home page, go to LPR, and then click the LPR Manager you want to configure.
3. Click the Identity tab, then click anywhere in the active window (e.g. click in the Name field).
4. Press Ctrl+Shift+A on your keyboard to open the Advanced settings.
5. In the Role group field, type a different name than the one displayed (the default LicensePlateManagement). For example, you can use LicensePlateManagement2 or any other name you like.
6. Click Apply.
7. (Optional) Press Ctrl+Shift+A again to close the Advanced settings.

This LPR Manager will now use a new GenetecLicensePlateManager32.exe process, which helps distribute the computer’s memory and optimizes performance.

After you are done: Repeat this procedure for as many LPR Managers as needed.

Related topics:

- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 5: Configure hotlists.
Phase 6: Configure Patroller unit settings from Security Center

This is what you need to do in Config Tool to configure a Patroller unit's sound management, acknowledgement buffer, and hit delay settings. 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 the Config Tool help.

**Before you begin:** Read about Config Tool and take a tour of the user interface. This section also shows you how to log on and off Config Tool. For more information, see "Security Center Config Tool interface tour" on page 10.

This section includes the following topics:
- "Configure sound management for Patroller units" on page 56
- "Configure acknowledgement buffer settings for Patroller units" on page 56
- "Configure hit delay for Patroller units" on page 57

**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 Config Tool.**
2. **From the 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 169.
4. **Click Apply.**

**After you are done:** 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 the Config Tool help.

**Related topics:**
- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 6: Configure Patroller unit settings from Security Center.

**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 Config Tool.**
2 From the 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 169.

4 Click Apply.

After you are done: 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 the Config Tool help.

Related topics:

- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 6: Configure Patroller unit settings from Security Center.

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 (assuming the plate is on a hotlist).

1 Log on to Config Tool.

2 From the 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 169.

4 Click Apply.

After you are done: 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 the Config Tool help.

Related topics:

- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 6: Configure Patroller unit settings from Security Center.
Phase 7: Configure Patroller

This is what you need to do in Patroller Config Tool to configure Patroller for Law Enforcement. You'll learn how to add Sharp cameras to the in-vehicle LAN, connect Patroller to Security Center, configure offload options, and more.

Before you begin: Read about Patroller Config Tool and take a tour of the user interface. This section also shows you how to log on and off Patroller Config Tool. For more information, see "Patroller Config Tool interface tour" on page 13.

This section includes the following topics:
- "Add the Sharp cameras to Patroller" on page 58
- "Connect Patroller to Security Center" on page 58
- "Configure offload options" on page 59
- "Configure the Patroller unit name and logon options" on page 59
- "Configure Patroller hit options" on page 60
- "Configure the Patroller navigation and map settings" on page 60
- "Customize the Patroller user interface" on page 61

Add the Sharp cameras to Patroller

After you have physically connected the Sharp hardware, you need to add the Sharps to the in-vehicle LAN. Patroller can auto-detect connected Sharp cameras and add them for you. You’ll then need to select the camera’s orientation.

For more information, see "Connecting Sharp units to Patroller" on page 137.

Related topics:
- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 7: Configure Patroller.

Connect Patroller to Security Center

Even if you are not monitoring LPR events in Security Desk, you’ll still need to perform this procedure at least once in order for Security Center to detect the Patroller unit.

For more information, see "Connect Patroller to Security Center" on page 48.

Related topics:
- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 7: Configure Patroller.
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, you need to establish a live connection between Patroller and Security Center. For more information, see “Connect Patroller to Security Center“ on page 48.

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 209.

After you are done: If you selected LocalFile as your offload method, and you intend to use a USB key to transfer the LPR data from the Patroller computer to the Security Center computer, you can configure a USB device to do it automatically. For more information, see "Setting up USB support" on page 140.

Related topics:
- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 7: Configure Patroller.

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 Config Tool when you create a user. The Patroller unit name is the name of the vehicle 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 205.

Related topics:
- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 7: Configure Patroller.
Configure Patroller hit options

You configure most of the options related to hotlist hits from Config Tool. However, 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 without requiring user interaction.
- **Display hits by priority.** Display hits by the priority specified in 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 "Hits" on page 213.

**Related topics:**

- Go back to **AutoVu mobile deployment overview.**
- Go to top of **Phase 7: Configure Patroller.**

Configure the Patroller navigation and map settings

If you're using Patroller with GPS and maps, you need to configure the navigation and mapping settings.

Before you begin: If you're using the MapInfo mapping type, you need to install the MapInfo files. For more information, see "Install MapInfo files" on page 113.

1. **Open Patroller Config Tool.**
2. Go to **Navigation > GPS**, turn on **Use GPS**, and then configure the remaining settings.
   
   For more information, see "GPS" on page 217.
3. Go to **Navigation > Maps**, select your **Mapping type**, and then configure the remaining settings.
   
   For more information, see "Maps" on page 219.
4. Go to **Advanced > Mapping maps**, and then turn on **Use maps.**
NOTE If you’re using MapInfo maps, also select your Map info version. If you’re not using MapInfo, this setting has no effect.

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 146.

Related topics:
- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 7: Configure Patroller.

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 starts minimized, and stays that way until a hit occurs.

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 220.

Related topics:
- Go back to AutoVu mobile deployment overview.
- Go to top of Phase 7: Configure Patroller.
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.

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click [here](#) for the most recent version of this document.

This section includes the following topics:

- "Hardware specifications and system requirements" on page 63
- "About the hardware installation procedures in this guide" on page 63
- "Safety precautions" on page 63
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.
Installing fixed AutoVu hardware

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

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

This section includes the following topics:

- "Fixed installation example" on page 67
- "Fixed installation guidelines" on page 69
- "Fixed installation procedure" on page 73
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
  
  **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.

---

**Fixed**

---

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

*Fuse not required if you use the power supply provided by Genetec. If you use a different power supply, install an inline 10 Amp Slow Blow 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" on page 69
- "If you need to shorten the Sharp cable" on page 70
- "Sharp positioning guidelines" on page 71

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.

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.

![Diagram showing Sharp camera angles](image)

**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

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.

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.

- 2.71 m/9 ft
- 6.46 m/21 ft
- 28.16 m/92 ft
- 2.03 m/6.7 ft
- 50 mm lens
- 2.72 m/9 ft
- 5.88 m/19 ft
- 19.71 m/64.6 ft
- 2.03 m/6.7 ft
- 35 mm lens
- 2.73 m/9 ft
- 5.26 m/17 ft
- 14.08 m/45.5 ft
- 2.03 m/6.7 ft
- 25 mm lens
- 2.82 m/9 ft
- 3.74 m/12 ft
- 6.76 m/22 ft
- 2.05 m/6.7 ft
- 16 mm lens
- 2.77 m/9 ft
- 4.34 m/14 ft
- 9.01 m/29.6 ft
- 2.05 m/6.7 ft
- 12 mm lens
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" on page 73
- "Install your Sharp XGA" on page 73
- "Install your Sharp EX" on page 75

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" on page 73
- "Step 2: Connect the Sharp" on page 74
- "Step 3: Mount the electrical enclosure" on page 74
- "Step 4: Finishing up" on page 75

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 69.

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.

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.

Install your Sharp EX

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

The installation procedure for the Sharp EX is the same as the Sharp XGA (see "Install your Sharp XGA" on page 73), but you’ll need to account for the extra external cameras. The following guidelines apply:

- The external cameras require their own mounts and power source. They cannot be powered through the Sharp EX processing unit.
- If you install the Sharp EX unit inside an enclosure, make sure the enclosure is properly ventilated to keep the Sharp EX from overheating. For more information on the Sharp EX operating temperature and other specifications, see "Hardware specifications and system requirements" on page 63.
- The external cameras are connected to the Sharp EX using TNC connectors. Properly tighten the connectors (by hand), and follow the manufacturer’s guidelines for sealing them. This usually involves placing heat-shrink tubing over the ferrule that crimps the shield and jacket. For the connection to be weatherproof, the female side and male side of the connection must be properly mated and sealed. Follow the guidelines provided
by the manufacturer for whichever connector and cable you use. For extra protection, you can also use butyl tape to seal the full mated cable.

**NOTE:** Push the heat sink tubing up to the backshell ring of the connector, not just over the crimp ferrule. This will prevent water from leaking through the braids of the coaxial shield.

- The TNC plug you use should be made for 75 ohm video coaxial cable, such as RG-59 cable.
Installing mobile AutoVu hardware

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

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

This section includes the following topics:

- "Mobile installation examples for Sharp" on page 78
- "Mobile installation guidelines for Sharp" on page 84
- "Mobile installation procedure for Sharp" on page 85
- "Mobile installation guidelines" on page 94
- "Mobile installation procedure" on page 95
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" on page 78
- "Advanced mobile installation example" on page 80
- "Sharp wiring diagram" on page 82

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:

<table>
<thead>
<tr>
<th>Component</th>
<th>What you should know</th>
</tr>
</thead>
</table>
| A: Sharp Camera | - Magnetic mount Sharps can also be used. For more information, see "Magnetic mount installation" on page 91.  
- 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 component:

<table>
<thead>
<tr>
<th>Component</th>
<th>What you should know</th>
</tr>
</thead>
</table>
| **A**: Sharp Camera | • Magnetic mount Sharps can also be used. For more information, see "Magnetic mount installation" on page 91.  
• 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. |
| **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 88.
- 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 87.

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

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 (pin 6) 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 (pin 6) on J1 connector
- By passes breakout unit fuse to power directly 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.

This section includes the following topics:

- "What you need" on page 85
- "Hardmount installation" on page 85
- "Magnetic mount installation" on page 91

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:

- **Weatherproof, non-corrosive sealant.** For protecting cable connections.
- **Stranded conductor copper wire.** For the optional Navigator unit (required for ignition and reverse signals).
- **Shielded dual-stranded conductor cable.** For the optional Navigator unit (required for odometry signal).

Hardmount installation

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

This section includes the following topics:

- "Prepare your vehicle" on page 86
- "Install your Sharp camera" on page 87
- "Install your breakout box" on page 87
- "(Optional) Install your Navigator unit" on page 88
- "(Optional) Install USB GPS antenna" on page 88
- "(Optional) Install tire cameras" on page 88
- "Connect cables and wires" on page 90
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.

- "Finishing up" on page 91

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.
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 the previous section (“Prepare your vehicle” on page 86).

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 unit

The Navigator unit 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 Navigator unit.

- The Navigator unit 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 unit on a flat, level surface.
- Install the Navigator unit 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 unit.

(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 unit (if you’re using one). If you’re not using a Navigator unit, 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, and do one of the following:
   - If you are using the Navigator unit, connect the GPS antenna to the designated connector on the unit. For more information, see component “D: Navigator unit” in "Advanced mobile installation example" on page 80.
   - If you are not using the Navigator unit, 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.
**IMPORTANT** 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.

**NOTE** 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.

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.

---

![Tire cameras installed on the rear trunk wall.](image1)

![Make sure your tire camera lenses are facing outward to properly capture tire images.](image2)
Connect cables and wires

Connect all your AutoVu cables (for more information, see "Mobile installation examples for Sharp" on page 78, and "Sharp wiring diagram" on page 82).

**NOTE** For more information on your vehicle's internal wiring, see your owner’s manual.

The following conditions apply:

- Cables/wires for powering the tire cameras and Navigator unit are not included. 12V DC power is required for both.
  
  **IMPORTANT** Do not connect the Navigator unit or tire cameras directly to the vehicle's battery. These components should only receive power when your vehicle's engine is running.

- You’ll need to use your own wires to connect the Navigator unit to the vehicle's ignition, reverse signal, and odometry. Use stranded conductor copper wire for the ignition and reverse signals, and shielded dual-stranded conductor cable for the odometry.

- Connectors are provided to connect your wires to the relays and inputs on the Navigator unit. Use the connectors as shown below:

  ![2-pole connector](image)

  **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.**

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

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

  **After connecting to the Navigator unit, make sure to tighten the securing screws.**
• Connect your wires as follows:

<table>
<thead>
<tr>
<th>Navigator connection</th>
<th>What it's used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relays 1 and 2</td>
<td>90V relays used for switching auxiliary equipment.</td>
</tr>
<tr>
<td>Inputs 1A and 2A</td>
<td>Analog inputs used to measure battery voltage, temperature, etc.</td>
</tr>
<tr>
<td>GND</td>
<td>Grounding</td>
</tr>
<tr>
<td>Inputs 1D and 2D</td>
<td>Digital inputs used for sensors handling events such as doors opening, etc.</td>
</tr>
<tr>
<td>IGN</td>
<td>Ignition input. State of the vehicle's power system.</td>
</tr>
<tr>
<td>GND</td>
<td>Grounding</td>
</tr>
<tr>
<td>REV</td>
<td>Reverse input. Connect to vehicle's reverse signal (required for inertial navigation).</td>
</tr>
<tr>
<td>- ODO and + ODO</td>
<td>Odometry inputs. Connect to the vehicle's odometry signal (required for inertial navigation).</td>
</tr>
</tbody>
</table>

**Finishing up**

1. Start your vehicle to verify that your AutoVu hardware, as well as your vehicle's other electrical devices, are working properly.
2. Seal the holes in the vehicle's roof with a weatherproof sealant, such as RTV silicone.
3. 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.

This section includes the following topics:

- "Install your Sharp camera" on page 92
- "Connect cables and wires" on page 93
Install your Sharp camera

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.
Connect cables and wires

1. 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.

2. Connect your devices as shown below.

   **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).

Start your vehicle to verify that your AutoVu hardware, as well as your vehicle’s other electrical devices, are working properly.
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 as described in "Step E: Connect the SharpX cable to the SharpX camera" on page 102.
- 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.
- For the procedures in Step A: Provide power to the LPR Processing Unit (part 1) and in Step D: Connect the SharpX power cable to the LPR Processing Unit, insert the wires into the poles so that there’s no exposed bare wire, but not too deep so that the tension clamp closes over the insulation rather than the wire itself.
**Mobile installation procedure**

This section includes the following topics:

- "What you need" on page 95
- "AutoVu SharpX connections" on page 95

**What you need**

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

- 2.5 mm flat head screwdriver. Used for securing wires to the provided connectors.
- RJ45 crimp tool. Used to crimp the CAT5e cable wires.
- Three stranded copper wires. Used to provide power to the LPR Processing Unit. Two wires should be 14 AWG, and the other should be between 20 AWG minimum to 14 AWG maximum.
- 15A in-line fuse. Protects the wiring to the vehicle battery.
- Weatherproof, non-corrosive sealant. For protecting cable connections.

**About third-party connectors**

This section describes the connectors that are included with the AutoVu SharpX system, but are not manufactured by Genetec.

- Cable connectors are manufactured by Weidmuller. For more information, go to [http://www.weidmueller.com/56339/Home/cw_index.aspx](http://www.weidmueller.com/56339/Home/cw_index.aspx) and search for the following part numbers:
  - 1043920000 (3-pole)
  - 1690910000 (5-pole)
  - 1690880000 (2 -pole)
- The RJ45 connector is manufactured by Tyco Electronics. For more information, go to [http://www.tycoelectronics.com](http://www.tycoelectronics.com) and search for part number 5-569552-3.
  
  For a detailed T568B crimp procedure, click the “Application Specifications” link on the part's webpage.

**AutoVu SharpX connections**

This section includes a diagram that shows the supported SharpX connections. Each connection is labelled A through G, and has specific steps you’ll need to follow. The remaining topics in this section provide the required information on each connection. For example, for more information on connection A in the diagram, see "Step A: Provide power to the LPR Processing Unit (part 1)" on page 98.
This section includes the following topics:

- "SharpX connection diagram" on page 96
- "Before you begin the installation" on page 97
- "Step A: Provide power to the LPR Processing Unit (part 1)" on page 98
- "Step B: Provide power to the LPR Processing Unit (part 2)" on page 99
- "Step C: Connect the SharpX CAT5e cable to the LPR Processing Unit" on page 99
- "Step D: Connect the SharpX power cable to the LPR Processing Unit" on page 101
- "Step E: Connect the SharpX cable to the SharpX camera" on page 102
- "Step F: Connect the LPR Processing Unit to the computer" on page 102
- "Step G: (Optional) Use relays to switch with state of ignition" on page 103

**SharpX connection diagram**

Use the diagram below and the links provided to learn more about each connection.
NOTE Only one SharpX camera is shown for illustration purposes. You’ll need to repeat the steps for connections C, D, and E for the second SharpX camera.

Click the links to jump to the desired topic:

- Before you begin
- Go to Step A
- Go to Step B
- Go to Step C
- Go to Step D
- Go to Step E
- Go to Step F
- Go to Step G

Before you begin the installation

Decide where in the vehicle you want to install the LPR Processing Unit, and then attach the included strain relief bracket accordingly. You can attach the strain relief bracket to the bottom or top of the LPR Processing Unit. After the installation is complete, tie the wires and cables to the bracket as needed to secure them.
Step A: Provide power to the LPR Processing Unit (part 1)

This section shows you how to connect the SharpX power cable to the LPR Processing Unit.  

**NOTE** SharpX connectors use push-in tension clamps to secure the wires.

Return to diagram, click here.

**Before you begin:** You’ll need a 2.5 mm flat head screwdriver, and three stranded copper wires.

1. Attach the 3-pole connector to the power port, then tighten the securing screws.

Make sure to tighten the securing screws.
2 Strip 10 mm (3/8”) of insulation from the stranded copper wires, push in the tension clamps with your screwdriver, insert the wires, then release the clamps. Gently tug the wires to make sure they are secure.

**Best practice:** Use a red wire for power (+), black wire for ground (GND), and yellow wire for ignition (IGN) to be consistent with similar Genetec installations.

---

**Step B: Provide power to the LPR Processing Unit (part 2)**

This section shows you how to connect the SharpX power cable to the vehicle.

**Return to diagram, click here.**

**Before you begin:** You’ll need a 15A in-line fuse ready.

**IMPORTANT** These instructions are not intended to replace the vehicle's owner manual. If you are unsure about the vehicle's internal wiring, refer to the owner manual before continuing.

1 Connect the wire from the LPR Processing Unit’s + pole, through the 15A in-line fuse, to the vehicle's 12V power source (permanent +12V).

   **NOTE** Install the fuse at the source of the vehicle's 12V system tapping point. The LPR Processing Unit is already protected internally by an electronic circuit breaker.

2 Connect the wire from the LPR Processing Unit's **GND** pole to the vehicle's chassis for grounding.

3 Connect the wire from the LPR Processing Unit's **IGN** pole to the vehicle's ignition signal (+12V active when at ON/RUN key position).

---

**Step C: Connect the SharpX CAT5e cable to the LPR Processing Unit**

This section shows you how to connect the SharpX CAT5e cable to the LPR Processing Unit. The SharpX camera cable is an “all-in-one” cable that contains the shielded CAT5e conductor wires you need to crimp and connect to the included RJ45 plug (also shielded).
This cable design allows you to cut the pigtail end of the Sharp cable to fit your specific installation. However, if you cut the cable, make sure to leave some slack for maintenance purposes.

**IMPORTANT** Read full crimp instructions at [www.tycoelectronics.com](http://www.tycoelectronics.com) for RJ45 part number 5-569552-3.

Return to diagram, click here.

1. Strip the SharpX camera cable to expose the CAT5e cable (and other wires) inside. Trim the polyester fill threads and aluminum foil as needed.

![Before](image1.png)

![After](image2.png)

1. Strip the CAT5e cable you exposed in Step 1. Make sure not to nick or cut the insulation of the interior wires.
2 Crimp the wires according to the TIA/EIA-568-B.1-2001 specification, using the T568B conductor arrangement. Remember that the cable and connector are shielded, so you need to fold the foil shield so it has contact with the RJ45’s metal shell.

![T-568B Diagram]

3 After you've attached the RJ45 connector, plug the CAT5e cable into the into the first Data Link port.

![Camera Interfaces Diagram]

4 Repeat these steps for the other SharpX camera as needed.

**Step D: Connect the SharpX power cable to the LPR Processing Unit**

This section shows you how to connect the SharpX power cable to the LPR Processing Unit.

**NOTE** SharpX connectors use push-in tension clamps to secure the wires.

Return to diagram, click here.

**Before you begin:** You'll need a 2.5 mm flat head screwdriver.

1 Attach the 5-pole connector to the camera port, then tighten the securing screws.

![Connector Diagram]
2 Strip 10 mm (3/8") of insulation from the wires you exposed in "Step C: Connect the SharpX CAT5e cable to the LPR Processing Unit" on page 99 (drain wire has no insulation), push in the tension clamps with your screwdriver, insert the wires, then release the clamps. Gently tug the wires to make sure they are secure.

3 Repeat these steps for your other SharpX camera(s) as needed.

**Step E: Connect the SharpX cable to the SharpX camera**

This section shows you how to connect the SharpX cable to the SharpX camera.

**CAUTION** Secure and tighten the cable connector to the SharpX camera, otherwise water may leak into the camera.

**IMPORTANT**

- 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.

1 Remove the plastic protector cap from the camera.
2 Put dielectric gel on the cable connector threads.
3 Align the notch on the cable connector with the notch on the camera port.
4 Attach the cable to the SharpX camera.
5 Align the connector threads and tighten the connector by turning the outer connector ring clockwise.
6 Tighten the connector as much as possible by hand. Don’t use a wrench or other tool to tighten it.

**Step F: Connect the LPR Processing Unit to the computer**

Connect the LPR Processing Unit to the in-vehicle computer using the provided Ethernet cable.
Return to diagram, click here.

**Step G: (Optional) Use relays to switch with state of ignition**

Relays switch on/off with state of ignition. Use 2-pole connectors with 16 AWG wire when switching the maximum current in relays (8A). Insert wires as described in "Step D: Connect the SharpX power cable to the LPR Processing Unit" on page 101.

Return to diagram, click here.
Installing Security Center

Installing Patroller

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

This section includes the following topics:

- "System requirements" on page 106
- "Before you install" on page 109
- "About the AutoVu Patroller installation package" on page 110
- "Installation overview" on page 111
- "Installing AutoVu Patroller" on page 112
System requirements

This section includes the following topics:

- "Patroller system requirements" on page 106
- "SQL Express database requirements" on page 107

Patroller system requirements

The system requirements for an AutoVu Patroller installation that includes four Sharps or less are as follows:

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Processor</td>
<td>• Intel® Core® Duo U2500 Ultra Low Voltage, 1.2 GHz, 2 MB Cache</td>
</tr>
<tr>
<td>Operating system</td>
<td>• Microsoft® Windows XP Pro 32-bit Service Pack 3 or later.</td>
</tr>
<tr>
<td></td>
<td>• Microsoft® Windows 7 Professional 32- or 64-bit.</td>
</tr>
<tr>
<td>Free disk space</td>
<td>• 80 GB (or more) of storage</td>
</tr>
<tr>
<td>SQL</td>
<td>• SQL 2005 Standard/Enterprise</td>
</tr>
<tr>
<td></td>
<td>• SQL 2008 Standard (32-bit)/Enterprise (32-bit).</td>
</tr>
<tr>
<td></td>
<td>• SQL Server 2008 Service Pack 1 is mandatory to use SQL 2008 Standard</td>
</tr>
<tr>
<td></td>
<td>/Enterprise editions</td>
</tr>
<tr>
<td></td>
<td>• SQL Express 2005/2008.</td>
</tr>
<tr>
<td></td>
<td>• 1GB of RAM without wheel imaging</td>
</tr>
<tr>
<td></td>
<td>• 2 GB of RAM with wheel imaging</td>
</tr>
<tr>
<td></td>
<td>• SQL Express 2008 R2</td>
</tr>
<tr>
<td></td>
<td>Required if using higher quality resolution for Sharp context and wheel</td>
</tr>
<tr>
<td></td>
<td>images. You can download SQL Express 2008 R2 at: http://</td>
</tr>
<tr>
<td>Web browser</td>
<td>• Internet Explorer, Google Chrome, or Mozilla Firefox are required to</td>
</tr>
<tr>
<td></td>
<td>use the Sharp Admin to configure Sharp units.</td>
</tr>
<tr>
<td></td>
<td>• All web browsers must have the Microsoft Silverlight plugin installed.</td>
</tr>
<tr>
<td>Monitor</td>
<td>• Touchscreen</td>
</tr>
<tr>
<td>Screen resolution</td>
<td>• 800 x 600 or higher</td>
</tr>
<tr>
<td>Network card</td>
<td>• 10/100 Ethernet</td>
</tr>
<tr>
<td>Other</td>
<td>• USB ports</td>
</tr>
<tr>
<td></td>
<td>• Sound support</td>
</tr>
</tbody>
</table>
The following programs are automatically installed when you run the setup.exe:

- Microsoft.NET Framework 3.5 SP1
- Microsoft CCR and DSS Runtime 2008 R2
- Microsoft Report Viewer 2008
- Windows Installer 4.5

**SQL Express database requirements**

The SQL Express license supports up to 4 GB (that is, approximately 80,000 reads) of data for hotlists, permit applications, or overtime applications without wheel imaging.

Contact your Genetec representative to determine the required database size for overtime applications with wheel imaging.

**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
Before you install

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

Read the Release Notes


Disable User Account Control (Windows 7 only)

Patroller will not install when the Windows User Account Control security option is enabled. You must disable it before installing AutoVu Patroller.

1. Log on to the Windows system as an administrator.
2. Open the Control Panel, and click User Accounts and Family Safety > Make changes to user account, then click Turn User Account Control on or off.
3. Clear the Use User Account Control (UAC) to help protect your computer check box to turn off UAC, and click OK.
4. Restart the computer when prompted.
5. Log on to the computer, and click Display.

Disable Aero Themes (Windows 7 only)

Patroller will not display correctly if you are using a Windows Aero Theme. You must select a theme other than Aero Theme before installing AutoVu Patroller.

1. Log on to the Windows 7 system.
2. Open the Control Panel, and click Display > Personalization.
3. Choose a theme from the Basic and High Contrast Themes list (for example, Windows 7 Basic).
About the AutoVu Patroller installation package

This section includes the following topics:

- "Where can I find the installation package" on page 110
- "Installer languages" on page 110
- "What’s not included" on page 110

Where can I find the installation package

The AutoVu Patroller 5.0 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. Customers may provide their own mapping data for in-vehicle applications. Open mapping data, such as ESRI mapping data, can be transformed to be compatible with MapInfo maps; this excludes Google Earth or Virtual Earth mapping data, as we cannot extract or transform these mapping mediums. Services to transform customer mapping data are subject to one day of SVC-REMOTE fee.

**Customized hotlists, permit lists, and overtime 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.
Install AutoVu Patroller components in the following order:

<table>
<thead>
<tr>
<th></th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Read &quot;Before you install&quot; on page 109. This section describes the things you should know and do before you install or upgrade AutoVu Patroller.</td>
</tr>
<tr>
<td>2</td>
<td>&quot;Install AutoVu Patroller&quot; on page 112.</td>
</tr>
<tr>
<td>3</td>
<td>&quot;Download latest hotfixes&quot; on page 113.</td>
</tr>
<tr>
<td>4</td>
<td>(MapInfo users only) &quot;Install MapInfo files&quot; on page 113.</td>
</tr>
</tbody>
</table>
Installing AutoVu Patroller

This section explains how you can install and upgrade AutoVu Patroller. This section includes the following topics:

- "Install AutoVu Patroller" on page 112
- "Download latest hotfixes" on page 113
- "Install MapInfo files" on page 113

Install AutoVu Patroller

Before you begin: Read "Before you install" on page 109.

1. Insert the AutoVu installation DVD in your computer’s DVD drive, or double-click Setup.hta 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 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 click Next. Or, to choose a different installation folder, click Change.
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 Maps Configuration Selection window, select whether to install maps or not.
12. In the Database Server Selection window, select one of the following options:
   - Install a new database server. Select this option if SQL database server is not installed on the computer. This option installs Microsoft® SQL Server 2008 Express Edition and creates a database instance called SQLEXPRESS.
   - Use an existing database server. Select this option if SQL database server is installed on the computer, and you would like to use this database. In the Database Server list, select the existing SQL Server name.
13. Click Next. If you are prompted to change the SQL Server database to mixed mode, click yes.
NOTE Mixed mode enables both Windows Authentication and SQL Server Authentication, and is required for Patroller users that don’t have Windows administrator privileges to access the SQL database server.

14 Click Install.
15 When the installation is complete, click Finish.

After you are done: "Download latest hotfixes" on page 113.

Download latest hotfixes

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 112.

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 5.1 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 "Upgrading Patroller and Sharp units from Security Center" on page 115.

After you are done: (for MapInfo users) "Install MapInfo files" on page 113.

Install MapInfo files

Before you begin: Make sure that you installed the “Maps Engine” during Patroller installation in the Map Configuration Selection page.

To use MapInfo, you’ll need to copy the MapInfo files to the Maps folder.
1 In the Patroller Mobile Client folder, create a folder named Maps.
   EXAMPLE C:\Program Files\Genetec AutoVu X.X\MobileClient\Maps
2 Copy your MapInfo files into the maps folder.
Upgrading AutoVu

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

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click [here](#) for the most recent version of this document.

This section includes the following topics:

- "Upgrading Patroller and Sharp units from Security Center" on page 115
- "Upgrading Patroller" on page 120
- "Upgrade FAQ for Patroller users" on page 123
Upgrading Patroller and Sharp units from Security Center

This section explains how to use Config Tool to update various AutoVu components. You can update Patroller units with hotfixes and new audio files for hit alerts, and update Sharp units with new services and firmware upgrades.

**NOTE** For Sharp cameras that are already deployed in the field, you need to first upgrade them to 5.1 SR2 before you can use this feature. Some older Sharp units do not support this feature even after you upgrade them to 5.1 SR2 (e.g. Sharp 1.5 and Sharp 2.0 units with 512 MB of RAM). For more information on upgrading Sharp units to 5.1 SR2, contact your Genetec representative.

This section includes the following topics:

- "Before you begin" on page 115
- "Update AutoVu components" on page 117

**Before you begin**

Before you can update AutoVu components, you need to do the following:

1. Read "About AutoVu update files" on page 115.
2. Read "About zipping sound files" on page 115
3. Read "About adding sound files to the Genetec zip file" on page 116
4. "Enable updates and create update folder" on page 116

**About AutoVu update files**

You receive Genetec updates as a zip file (.zip) that contains one or more update files (Sharp firmware upgrades, Patroller hotfixes, etc). You need to copy the zip file to a specific folder on the Security Center computer. Security Center extracts and processes the contents of the zip file to see which AutoVu components are eligible for an update. You can then choose in Config Tool which update you want to perform.

Security Center only processes updates that are contained in zip files. This means that if you want to use the updater service to send Patrollers new sound files for hits, you have to zip the sound files first, and then copy them to the appropriate folder on the Security Center computer. For more information, see "About zipping sound files" on page 115.

**About zipping sound files**

You need to zip sound files in a specific way so that they are placed in the correct folder on the Patroller machine. For example, on the Patroller computer, sound files are placed by default in the folder `C:\Program Files\Genetec AutoVu X.X\MobileClient\Config\Sounds`. Therefore, when you zip sound files to send to Patroller, you have to zip them so they extract to this particular folder.
NOTE You can change the default Sound file folder path in Config Tool, but you must make sure that the zip file extracts to the correct folder. For more information, see Hotlist - "Advanced" on page 164.

About adding sound files to the Genetec zip file

If you receive a zip file from Genetec with updates, hotfixes, etc, you can add sound files to it so that the files are sent to Patroller along with the updates. However, the sound files will be extracted (along with the other contents of the zip file) to the root AutoVu folder (e.g. C:\Program Files\Genetec AutoVu X.X\MobileClient).

This means that you need to do one of the following in order for Patroller to be able to play the new sounds:

- Manually copy and paste the sound files from the root folder to the Sounds folder on the Patroller computer (e.g. copy the files to C:\Program Files\Genetec AutoVu X.X\MobileClient\Config\Sounds).
- Change the Sound File folder path in Config Tool so that it points to the root folder instead of the Sounds folder. For more information, see Hotlist - "Advanced" on page 164.

Enable updates and create update folder

In order to send updates to Patrollers and Sharp units, you need to enable the feature and set the listening port for the updates. You do this in Config Tool.

1. Log on to Config Tool.
2. From the Config Tool Home page, go to LPR > Units, select the LPR Manager that controls the units you want to update, and then click Options.
3. Turn on the Update provider and specify the listening port. For more information, see "Update provider" on page 195.

When you turn on the Update provider, Security Center creates a new folder called Updates under the LPR Root Folder on your computer. This new folder is where you copy the zip files that contain the updates.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotlists</td>
<td>1/26/2011 10:10 AM</td>
<td>File folder</td>
</tr>
<tr>
<td>Offload</td>
<td>9/27/2011 4:30 PM</td>
<td>File folder</td>
</tr>
<tr>
<td>PatrollerSettings</td>
<td>2/16/2011 3:40 PM</td>
<td>File folder</td>
</tr>
<tr>
<td>Formats</td>
<td>4/9/2011 1:12 AM</td>
<td>File folder</td>
</tr>
<tr>
<td>Updates</td>
<td>10/11/2011 10:06 AM</td>
<td>File folder</td>
</tr>
<tr>
<td>Users</td>
<td>2/10/2011 3:40 PM</td>
<td>File folder</td>
</tr>
<tr>
<td>Zones</td>
<td>10/26/2011 2:15 PM</td>
<td>File folder</td>
</tr>
</tbody>
</table>
Update AutoVu components

This section explains how to update AutoVu components from Config Tool. You can update any of the following components:

- **Patroller.** Update Patroller with hotfixes or new hit alert sounds.
- **Plate Reader.** Update the Plate Reader service, which is the main software component of the Sharp.
- **Sharp Firmware.** Update the Sharp firmware, which upgrades certain internal hardware components on the Sharp.
- **Updater Service.** Update the service responsible for the update process.

**Before you begin:** Do the following:

- Get the required updates from Genetec. If you’re only sending new hit alert sounds to Patroller, you need to zip them first.
- Connect to the components you want to upgrade. For example, if you want to upgrade Patroller, or upgrade mobile SharpX units, Patroller must be connected to Security Center as described in "Live connection" on page 207.

**To update AutoVu components:**

1. On the computer hosting the LPR Manager role, copy the zip file containing the updates into the corresponding Upgrade folder located under the LPR Root Folder. For example, if you’re updating Sharp firmware, copy the zip file to `C:\LPR root folder\Updates\Sharp Firmware\Upgrade`.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patroller</td>
<td>9/19/2011 9:57 AM</td>
<td>File folder</td>
</tr>
<tr>
<td>Plate Reader</td>
<td>11/9/2011 9:44 AM</td>
<td>File folder</td>
</tr>
<tr>
<td>Sharp Firmware</td>
<td>10/11/2011 10:06 AM</td>
<td>File folder</td>
</tr>
<tr>
<td>Updater Service</td>
<td>10/11/2011 10:06 AM</td>
<td>File folder</td>
</tr>
</tbody>
</table>

   Each of these folders contains an Upgrade folder. Copy your zip file into the folder that corresponds to the component you’re upgrading.

   When you copy the zip file into the corresponding Upgrade folder, after a few seconds you’ll see the file name change from `.zip` to `.processed`. This means that the LPR Manager has processed the update, and is ready to send it to the appropriate AutoVu component(s).

2. **Log on to Config Tool.**
3 From the Config Tool Home page, go to LPR > General settings > Updates. You’ll see an active Update button next to all eligible updates.

![Update button in Config Tool](image)

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

**NOTE** The Update all feature updates only the components on the active tab.

5 Under Status, monitor the status of the update.

**NOTE** If you see the message “Waiting for connection...” it means that Security Center is not connected to the component you’re trying to update (e.g. the Patroller vehicle is not in range of the WiFi network).

**After you are done:** The following will occur for each AutoVu component:

- **Patroller.** After the update has been downloaded to Patroller, the Patroller operator must accept the update in the Patroller application (similar to the update process for Microsoft Windows). An update icon appears in the Patroller notification bar. When the Patroller operator clicks the update icon, the update is installed, and the Patroller application restarts.

- **Sharp.** A mobile Sharp update is processed through Patroller, and the Patroller operator must accept the update as if it were a Patroller update (see Patroller). The only difference is that the Sharp unit is restarted rather than Patroller. A fixed Sharp update does not require any further user interaction. The fixed Sharp is restarted and continues working normally.
- Update services. After a service update, the Sharp unit (fixed or mobile) is restarted.
- Firmware upgrade. After a firmware upgrade, the Sharp unit (fixed or mobile) is restarted.
Upgrading Patroller

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

This section includes the following topics:

- "Before you upgrade" on page 120
- "Upgrade overview" on page 121
- "Upgrade Patroller database" on page 122
- "Upgrade FAQ for Patroller users" on page 123

Before you upgrade

This section lists the things you must know and do before upgrading AutoVu Patroller.

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 at: http://downloads.genetec.com/SecurityCenter/5.1/SR2/AutoVu/EN.AutoVu
Patroller Release Notes 5.1 SR2.pdf.

Backup Patroller database

Before you upgrade, it is best practice to back up your entire Patroller database.

1 Start Patroller.
   a Click the Windows Start menu.
   b Navigate to All Programs > Genetec AutoVu > Patroller Applications.
   c Select Patroller.
2 Right-click in the Patroller window.
3 From the Administration tools menu, navigate to Tools > Database > Backup.

Close Patroller

You must close AutoVu Patroller before upgrading to the latest Patroller version. You can
close Patroller using the Options button in the interface.

1 In the Patroller application, select Options, and click the System button (a light switch
   icon).
2 Select Exit application.
Upgrade overview

Upgrade AutoVu Patroller components in the following order:

<table>
<thead>
<tr>
<th>a</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Read &quot;Before you upgrade&quot; on page 120.</td>
</tr>
<tr>
<td>2</td>
<td>&quot;Upgrading Patroller&quot; on page 121.</td>
</tr>
</tbody>
</table>
| 3 | Adjust any settings that have not been carried over from the previous version, and manually transfer any associated files as necessary. For more information on setting adjustments, see the following: 
   - "Where can I find the configuration file from the earlier version?" on page 123. 
   - "Are my settings transferred to the latest version?" on page 123. |
| 4 | "Upgrade Patroller database" on page 122. |
| 5 | Upgrade Sharp units for use with 5.1 SR2. For more information, contact your Genetec representative. |

Upgrading Patroller

Before you begin: Read "Before you upgrade" on page 120.

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

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

1. Insert the AutoVu installation DVD in your computer’s DVD drive. If the InstallShield Wizard does not appear, double-click Setup.hta in the Patroller root directory.
2. A message appears indicating that an earlier version of Patroller is installed and asking you to confirm that you would like to start the upgrade process. Click OK.
3. Click Next to begin the upgrade or click Cancel to stop the installation.
4. Read and accept the License Agreement, and click Next.
5. Select the default installation folder, and click Next. Or, to choose a different installation folder, click Change.
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 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.

10 Click Next. If you are prompted to change the database to mixed mode, click yes.

11 Click Install, and then click Finish.

After you are done: "Upgrade Patroller database" on page 122.

Upgrade Patroller database

Use this procedure to delete all of the data in the Patroller database and upgrade the database to a the new version. You’ll need to perform this procedure each time you upgrade Patroller.

1 Open Patroller administrative tools.
   a In the notification area on the taskbar, right-click the AutoVu icon.
   b Select an item from the menu.

2 Navigate to Tools > Drop Database and Exit.

3 Click Yes in the Drop Database message window.

The database is deleted, and Patroller closes.

After you are done: The PlateReaderServer must also be upgraded when you upgrade Patroller. For more information on how to upgrade Sharp units for use with 5.1 SR2, contact your Genetec representative.
Upgrade FAQ for Patroller users

This section answers some frequently asked questions about the Patroller upgrade process to version 5.1.

This section includes the following topics:

- "Creating a Zones file in Patroller versions 4.4 and later" on page 123
- "Where can I find the configuration file from the earlier version?" on page 123
- "Are my settings transferred to the latest version?" on page 123

Creating a Zones file in Patroller versions 4.4 and later

From Patroller version 4.4 and on, permits, permit restrictions, and overtime rules are configured in the Security Center Config Tool. The configuration settings are still saved to the zones.xml file in the [root:]\AutoVu\Zones folder.

You can import the zones.xml file from AutoVu 4.1 to 4.3 into Security Center by copying the zones.xml file to the Root folder of the AutoVu LPR Manager. Once the file is copied, AutoVu LPR Manager automatically creates the corresponding overtime, permit, and permit restriction entities in Security Center.

Related topics:

- “Migrating from AutoVu 4.3 and earlier” in the Security Center 5.0 GA Installation and Upgrade Guide.
- “Unification of AutoVu systems”, in the Security Center Administrator Guide.

Where can I find the configuration file from the earlier version?

When you upgrade Patroller, copies of the configuration files from the earlier version are copied to a new Patroller root folder, in a folder named OldConfigFiles. You can open these files in a text editor and refer to them as you update your settings.

EXAMPLE  C:\Program Files\Genetec AutoVu\Patroller Applications 5.0\MobileClient\OldConfigFiles

NOTE  The configuration files from the earlier versions remain in their original directory.

Are my settings transferred to the latest version?

If the setting is still available in the latest version of Patroller, then the setting will be transferred during the upgrade process.

IMPORTANT  When upgrading Patroller from 5.1 GA to 5.1 SR2, the Mapping type option is reset to None. After upgrading Patroller, you'll need to reconfigure this option, see "Maps" on page 219.
Advanced configuration tasks

This chapter describes the advanced procedures required to configure an AutoVu system. It also describes some extra tasks and features you can use to further customize an AutoVu system for your specific installation.

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click [here](#) for the most recent version of this document.

This section includes the following topics:

- "About advanced configuration" on page 125
- "Configure the Sharp for an FTP connection" on page 126
- "Using a SharpX – Multi system" on page 129
- "Configuring Sharp Admin security" on page 131
- "Connecting Sharp units to Patroller" on page 137
- "Setting up USB support" on page 140
- "Using a SharpX system with multiple LPR Processing Units" on page 144
- "Install the GPS driver" on page 146
- "Switching images on the Sharp" on page 148
- "Enabling privacy on individual hotlists" on page 149
- "Moving Patroller or LPR units between LPR Managers" on page 151
About advanced configuration

The majority of the configuration tasks you need to get your AutoVu system up and running are covered in the following chapters:

- Chapter 3, “AutoVu fixed deployment overview” on page 22.
- Chapter 4, “AutoVu mobile deployment overview” on page 40.

This chapter is dedicated to the more complex tasks, where you may need to configure settings in multiple applications, or tasks that are not considered essential to configuring a typical AutoVu system. For example, one of the topics in this section shows you how to change the static IP addresses on your SharpX LPR Processing Unit. This is not a common scenario for most users, but it is essential if you want to use more than one LPR Processing Unit in your vehicle (e.g. if you have a six-camera SharpX configuration).
Configure the Sharp for an FTP connection

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

This section includes the following topics:

- "Configure the Sharp for FTP" on page 126
- "Modify the FTP XML" on page 127

Configure the Sharp for FTP

1. Log on to the Sharp Admin.
2. Go to the Configuration page.

3. Under Extension, configure the following:
Configure the Sharp for an FTP connection

- **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
<?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>
```

**NOTE** Please note the following:

- Hotlist matching is not supported.

- **LocalDate, LocalTime, UTCDate, UTCTime, and TimeZone** display the Windows date and time properties.

- **CameraName** is set in the Patroller Config Tool. For more information, see “Connecting Sharp units to Patroller” on page 137.

- **SourceName** is the Sharp name (e.g. Sharp1234).
Configure the Sharp for an FTP connection

- ContextImage and PlateImage are encoded into text.
- Guid is the unique identification of the event read.
- If using FTP extension with GPS coordinates, you'll need to add longitude and latitude fields.

**EXAMPLE**

```xml
<?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>```
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:

- "What is the SharpX – Multi?" on page 129
- "Connect and configure cameras for a SharpX – Multi 4-port system" on page 129

What is the SharpX – Multi?

The SharpX system consists of a SharpX camera unit and an LPR Processing Unit (sometimes 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 Admin.

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 Admin with SharpX" on page 17
- "Camera settings" on page 231

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. As a result, the SharpX connected to Interface 3 will use the processor’s full power and 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.
Configuring Sharp Admin security

The first time you connect to the Sharp Admin, it is over a non-encrypted HTTP connection. After you connect, you can then configure the Sharp Admin 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?" on page 131
- "Configure encryption with a Genetec certificate" on page 131
- "Configure encryption with a signed certificate" on page 135

Why use encryption?

When you log on to the Sharp Admin 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 Admin 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 Admin).

1. Log on to the Sharp Admin.
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 Admin 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 134.
- Disregard the warning and continue to the Sharp Admin.

NOTE The warning does not indicate that the Sharp Admin 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 Admin’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 Admin using an encrypted HTTPS connection.

1. Log on to the Sharp Admin.
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.

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 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 Admin.
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 Admin, 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 Admin** using HTTPS in the address bar instead of HTTP.

Your connection to the Sharp Admin is now encrypted.

After you are done: From the Sharp Admin’s Status page, click Change password, and change the default password from “Genetec” to something else.
Connecting 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 them to Patroller and Security Center. 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: Log on to the Sharp Admin, and configure the Sharp camera(s) for a mobile integration. For more information, see "Phase 3: Configure Sharp units for a mobile AutoVu system" on page 44.

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 on the Sharp.
      You configure the Sharp discovery port from the Sharp Admin Configuration page, under Extension. For more information, see "Extension" on page 234.
      NOTE The default discovery port for all Sharps shipped by Genetec 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.

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 cameras. In this case, go to Step b to add your second camera. If you don’t have a SharpX - Multi, go directly 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  (Optional) Make sure the Discovery port matches the discovery port value for the Sharp camera.

8  Click **Apply**.
Setting up USB support

You can set up USB support on the Security Center and Patroller computer to automate the process of transferring files to and from a USB device. This involves setting up a special folder on the Patroller computer, and configuring certain settings on both Patroller and Security Center computers.

When hotlists and configuration files are created, Patroller also creates a ManualTransfer folder under the Root folder. When you configure USB support, Patroller configuration files and offload files are copied to this folder.

This section includes the following topics:
- Set up USB support on the Security Center computer on page 140
- Set up USB support on the Patroller computer on page 141

Set up USB support on the Security Center computer

To set up USB support on the Security Center computer, do the following:

- Install USB batch files on the Security Center computer.
- Set Root folder and the USB drive letter on the Security Center computer.

  NOTE The new hotlist text file is not managed by USB support. Copy the updated text file used by hotlist to the server.

Install USB batch files on the Security Center computer

1. In the Patroller installation package, go to \Tools\USB Batch Files.
2. Select the language.
   This sets the language of the of the USB dialog box.
3. Open the ServerPC folder, and double-click InstallToCDrive.cmd.
   The folder ServerPC is copied to the Security Center computer’s C:\ drive.
4. On the Security Center computer, go to C:\ServerPC, and create a shortcut to FileTransfer.vbs on the desktop.
Set Root folder and the USB drive letter on the Security Center computer

Before you begin: You’ll need the following information:

- The drive letter used for the USB device. Insert your USB device in the Security Center computer, and take note of the letter the computer assigns to the USB drive.
  IMPORTANT When you configure USB support, make sure you always use the same USB drive letter, especially if your computer has multiple USB ports.

- Path to the LPR Manager Root folder on the Security Center computer. You can find this information in Config Tool. From the Config Tool Home page, go to LPR > Units > Options > General Settings. You’ll see the path next to Root folder (e.g. C:\LPR root folder).

To set the root folder and USB drive letter:

1. Go to C:\ServerPC.
2. Open PatrollerFiles_to_USB.cmd, and edit the LPR Manager root folder and USB drive paths to match your settings.

   EXAMPLE
   xcopy /e/v/y "C:\AutoVu\ManualTransfer\*.*" "E:\ManualTransfer\"

3. Open USB_OffloadFiles_To_GSC.cmd, and edit the USB drive and the Offload folder paths to match your settings.

   EXAMPLE
   move "E:\Offload\*.*" "C:\AutoVu\Offload\"

On the Security Center computer, when you click on the shortcut FileTransfer.vbs, the file transfer dialog box appears. From the dialog, you can choose to Copy the Patroller configuration to the USB key or Offload the Patroller data from the USB key.

NOTE Before you copy Patroller configuration files to a USB device, make sure that the LPR Manager has finished parsing the hit rules.

Set up USB support on the Patroller computer

To set up USB support on the Patroller computer, do the following:

- Install USB batch files on Patroller
- (Optional) Install USB autorun
- Set Offload folder and the USB drive letter on Patroller

Install USB batch files on Patroller

1. In the Patroller installation package, go to Tools\USB Batch Files\.
2. Select the language folder.
Setting up USB support

This sets the language of the USB dialog box.

3. Copy the PatrollerPC folder to your USB device.

4. Insert the USB device into the Patroller USB drive.

5. Open the PatrollerPC folder, and double-click InstallToCDrive.cmd.
   The folder PatrollerPC is copied on the Patroller computer’s C:\ drive.

6. On the Patroller computer, go to C:\PatrollerPC, and create a shortcut to FileTransfer.vbs on the desktop.

(Optional) Install USB autorun

Use this procedure to configure the Patroller computer to automatically display the File Transfer dialog box when you insert a USB device into the Patroller computer’s drive.

1. From the USB device, open PatrollerPC\APO USB Autorun.

2. Double-click setup.exe, and then follow the on-screen instructions. Click next and install.
   The USB Autorun icon appears in the notification area on the taskbar.

3. From the PatrollerPC folder, copy Autorun.inf and Patroller.vbs to the root of your USB drive.
   
   EXAMPLE   If your USB drive letter is “E”, then the files should be at E:\Autorun.inf and E:\Patroller.vbs.

4. (Optional) The default Autorun delay for the File Transfer window is 5 seconds. If you want to modify this setting, do the following:
   a. On the taskbar, right-click the APO USB Autorun icon.
   b. Select Preferences >Autorun delay, and set your desired delay time.

Set Offload folder and the USB drive letter on Patroller

Before you begin: You’ll need the following information:

- Path of the Patroller MobileClient folder (e.g. C:\Program Files\Genetec AutoVu X.X\MobileClient).
- Drive letter used for the USB device. Insert your USB device in the server and verify the letter assigned to the USB drive.

1. On the Patroller computer, go to C:\PatrollerPC.

2. Open OffloadFiles_to_USB.cmd, and edit the Offload folder and the USB drive paths to match your settings.

   EXAMPLE
   move "C:\Offload\*.*"  "E:\Offload\"

3. Save the batch file.
4. Open `USB_To_Patroller.cmd`, and edit the USB drive and the AutoVu program folder paths to match your settings.

**EXAMPLE**

```bash
copy /e/v/y "E:\ManualTransfer\*.*" "C:\Program Files\Genetec AutoVu\Patroller Applications X.X\MobileClient"
```

5. Save the batch file.

On the Patroller computer, when you insert the USB device into the USB port, the file transfer dialog box appears. From the dialog box, you can choose to **Apply the Patroller configuration from the USB key** or **Move the Offload data to the USB key**.

**NOTE** If the window does not appear, on the Patroller computer desktop, click on the `Patroller.vbs` shortcut.
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" on page 144
- "Change the LPR Processing Unit’s default IP addresses" on page 145

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:

<table>
<thead>
<tr>
<th>Component</th>
<th>Default IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Board Computer 1 (SBC1)</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>Single Board Computer 2 (SBC2)</td>
<td>192.168.10.2</td>
</tr>
<tr>
<td>Genetec Video Processor 1 (GVP1)</td>
<td>192.168.10.3</td>
</tr>
<tr>
<td>Genetec Video Processor 2 (GVP2)</td>
<td>192.168.10.4</td>
</tr>
<tr>
<td>Camera Unit 1 (CAMU1)</td>
<td>192.168.10.5</td>
</tr>
<tr>
<td>Camera Unit 2 (CAMU2)</td>
<td>192.168.10.6</td>
</tr>
<tr>
<td>Mobile Processing Unit (MPU)</td>
<td>192.168.10.7</td>
</tr>
<tr>
<td>Camera Unit 3 (CAMU3)</td>
<td>192.168.10.8</td>
</tr>
<tr>
<td>Camera Unit 4 (CAMU4)</td>
<td>192.168.10.9</td>
</tr>
</tbody>
</table>

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, but 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 Admin.
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 Admin 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 Configuration page.

4. Under Network settings, click Edit, and then select Static and change the IP address. For more information, see "Network settings" on page 230.

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 230.

6. Restart the Sharp unit.

This resolves all IP address conflicts, and you can proceed with configuring your SharpX 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 the 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 217.
Switching images on the Sharp

Some Sharp cameras are shipped with multiple versions of Security Center embedded on the hard drive. 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):
   
   - **Username:** enter gopher
   - **Password:** enter AutoVu_g0pher

4. In the notification area on the Windows taskbar, close the **Watchdog** and **PlateReader-Server** applications.
   
   - Right-click the **Watchdog** icon, then click Exit.
   - 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 future 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.
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 199). The only difference is that you can enable privacy on specific hotlists, rather than on all hotlists managed by the LPR Manager.

Why enable privacy on a specific hotlist?

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

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 X.X).
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 Config Tool.
4. From the Config Tool Home page, go to LPR > General settings > Applications.
5. Under Privacy, turn all the settings off.
6. Click Apply.
7. From the 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.
You can use the Move unit tool in 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 the Sharp Admin 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 Config Tool.

To move an LPR or Patroller unit:
1. **Log on to Config Tool.**
2. **From the 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  Go to Security Center > Live connection, 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 "Live connection" on page 207.

• For LPR units:
  c  Log on to the Sharp Admin.
  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 234.

• For hotlists, permit lists, and Patroller user groups (if applicable):
  e  Log on to Config Tool.
  f  From the 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.
  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.
Config Tool reference

This section describes the main 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.

IMPORTANT This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

NOTE This Config Tool reference is an abridged version of the main Security Center reference section found in the Security Center Administrator Guide, or Config Tool help.

This section includes the following topics:

- "Common configuration tabs" on page 154
- "Hotlist entity" on page 160
- "LPR Unit entity" on page 167
- "Patroller entity" on page 169
- "User entity" on page 172
- "User group entity" on page 179
- "LPR Manager role" on page 183
- "LPR administration task" on page 197
Common configuration tabs

Some configuration tabs are commonly used by the majority of entities in the system. These configuration tabs are described only once in this section.

The following tabs are covered in this section:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
<td>Name, description, logical ID, and relationships of the selected entity with other entities in the system.</td>
</tr>
<tr>
<td>Cameras</td>
<td>Cameras associated to the selected entity.</td>
</tr>
<tr>
<td>Custom fields</td>
<td>Custom fields for the selected entity.</td>
</tr>
<tr>
<td>Location</td>
<td>Time zone and geographical location for the selected entity.</td>
</tr>
</tbody>
</table>

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 a single place. For more information, see System – “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 an example, see Video unit – “Identity” in the *Security Center Administrator Guide*. 
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 – “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.

![Location Tab Screenshot]

**Time zone**

The time zone is used to display the entity events in the entity’s local time zone. In AutoVu, 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.

To set the latitude and longitude:

1. Click Select.
   A map window appears.
2. Navigate to the location of your entity on the map.
   You can click and drag to zoom in, zoom out, and pan.
3. Click Select in the map window.
   The cursor changes to a cross.
4. Click on the desired location on the map.
   A red pushpin appears on the map.
5. Click OK.

The latitude and longitude fields are filled with the coordinates of the location you clicked on the map.
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 hotlist, it is called a hotlist hit.

**System:** AutoVu IP license plate recognition

**Task:** Administration – 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. |
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.

- **Priority.** Choose a hotlist a 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 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).

  **IMPORTANT** This file must be accessible from the computer hosting the LPR Manager.

- **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.

- **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).
  - **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.
  - **Default 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.
  - **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.
- **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).

- **Time 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, 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.

- **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 as the Hotlist Hit and Review Hits screen in Patroller, appears in that color.

- **Use wildcards.** Indicates that the hotlist database contains wildcards. This setting tells Security Center that the records in that hotlist database only include 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 wildcard hotlist, it is best practice to do the following:

- Do not use more than one wildcard hotlist per Patroller.
- Hotlists are applied at the role level. Use only one wildcard hotlist per LPR manager role.
- Limit the number of entries to a hundred plates.

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 and hotlist entries have 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 hit email notifications. When a hotlist hit occurs, 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 Options tab.

- **Sound file.** Choose the sound that is played on Patroller when a hit occurs. If no sound file is entered, Patroller uses the default sound file installed with the application.

  **IMPORTANT**  For this feature to work, you need to manually copy the sound file to the Patroller computer. Copy the file to \Program Files\Genetec AutoVu\Patroller Applications X.X\MobileClient\Config\Sounds.

- **Enable editor support.** Allow a user to edit the hotlist or permit list in Security Desk using the Hotlist and permit editor task.
IMPORTANT  Please note the following about the Hotlist and permit editor:

- In order to edit a hotlist in Security Desk, the Hotlist and permit editor privilege must be granted to the user.
- Only the first 100,000 rows of a hotlist are loaded into Security Desk.
- 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.

- Override privacy for emails. Bypasses any privacy settings applied to hotlists at the Config Tool System level. Overriding privacy allows the LPR Manager to send an email with real hit data to the specified email address.

- 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.

  NOTE  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.

  NOTE  This option requires a continuous wireless connection between Patroller and Security Center.
**LPR Unit entity**

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. |
Properties

The Properties tab displays hardware and software information about the Sharp unit. You cannot edit this information. From the Properties tab you can restart the Sharp unit. You can also link to the LPR camera in the unit to an Omnicast camera or the Sharp's own context camera.

- **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.
- **Reboot.** Click to restart a fixed Sharp from Security Center.
  
  **IMPORTANT** For this feature to work, the Sharp must be configured to accept the Reboot command. The Accept remote reboot requests command is in the Sharp Portal Configuration page.

- **Devices.** Link the LPR camera to an Omnicast camera.
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)

<table>
<thead>
<tr>
<th>Identity</th>
<th>Name, description, logical ID, and relationships of this entity with other entities in the system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
<td>Assigns an LPR Manager to this entity and configures its sectors and rows.</td>
</tr>
<tr>
<td>Custom fields</td>
<td>Custom field values for this Patroller.</td>
</tr>
<tr>
<td>Location</td>
<td>Time zone and geographical location of this unit.</td>
</tr>
</tbody>
</table>

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** You can use the Copy configuration tool to copy the sound management, acknowledgement buffer, and hit delay settings to another Patroller entity. For more information on the Copy configuration tool, see the Security Center Config Tool help.

- **Properties.** Lists the Patroller machine properties.
  - *IP address.* IP address of the Patroller.
  - *Version.* Version number.
  - *Type.* Patroller installation type.
  - *Serial number.* Serial number of the Patroller.
- **Machine name.** Name of the Patroller computer.

- **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 license plate.
  - **Play sounds even when minimized.** Plays sounds even if the Patroller application is minimized to the taskbar.

- **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 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 (assuming the plate is on a hotlist).
  - **Duplicate hotlist hit delay.** Set the delay in minutes.
User entity

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

<table>
<thead>
<tr>
<th>Identity</th>
<th>Name, description, logical ID, and relationships of this entity with other entities in the system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
<td>User’s general profile.</td>
</tr>
<tr>
<td>Security</td>
<td>User’s security profile.</td>
</tr>
<tr>
<td>Privileges</td>
<td>User’s privileges.</td>
</tr>
<tr>
<td>Workspace</td>
<td>User’s default Security Desk workspace configuration.</td>
</tr>
<tr>
<td>Custom fields</td>
<td>Custom field values for this user.</td>
</tr>
</tbody>
</table>
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

As an administrator, you can change any user’s password. To change your own password, use the Change password command from the System menu instead.
**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.

**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.

**Security**

The *Security* tab lets you configure the user’s security profile.
User level

Security Center uses the user level (1 = highest) to 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. 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.

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.

Remote user control

This section lists the Security Desk workstations that this user is allowed to control remotely in order to display of entities.

Every PC monitor controlled by the Security Desk application is assigned a unique monitor ID (displayed in the notification tray). Using a CCTV keyboard, a user can display an entity on a remote Security Desk workstation by specifying its monitor ID, tile ID, and the logical ID of an entity he/she wishes to display.

NOTE The Security Desk workstations 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, so on and so forth.

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.
Workspace

The *Workspace* tab lets you configure the user’s Security Desk workspace.

![Workspace tab interface](image)

**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.
Force a user to start in full screen mode

If a user's job is to focus on monitoring live video, you can force the Security Desk to open in full screen mode by default.

1 Start by denying the privilege *Change client views* to the user.
   This privilege prevents the user from using the F11 command that toggles Security Desk between windows mode and full screen mode.

2 Change the properties of the Security Desk shortcut in *Genetec Security Center 5.1 programs* folder.
   a Open the Security Desk Properties dialog box.
   b Select the Shortcut tab, and add the option `/forcefullscreen` (or `/ff`) to the end of the string found in Target.

   ![Security Desk Properties dialog box](image)

   c Click Apply.
   The next time a user starts Security Desk using this shortcut, the application will start in full screen mode. The command to toggle between full screen and windows mode (F11) will be disabled.
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

<table>
<thead>
<tr>
<th>Identity</th>
<th>Name, description, logical ID, and relationships of this entity with other entities in the system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
<td>User group’s common email address and members.</td>
</tr>
<tr>
<td>Security</td>
<td>User group’s security attributes than can be inherited by its members.</td>
</tr>
<tr>
<td>Privileges</td>
<td>Privileges that can be inherited by the group members.</td>
</tr>
<tr>
<td>Custom fields</td>
<td>Custom field values for this user group.</td>
</tr>
</tbody>
</table>
Properties

The *Properties* tab lets you view and configure the members of the user group.

![Image of Properties tab]

**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.
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**

Security Center uses the *user level* (1=highest) to 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. 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 implicitly locked by that user. This means that other users cannot snatch the control away from him unless their user level is higher. The control over the PTZ camera is automatically relinquished after 5 seconds of inactivity.

**Archive viewing limitation**

This parameter serves to restrict this user group members’ ability to view archived video to the last $n$ days.
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.
The **LPR Manager** role manages and controls Patrollers and fixed Sharp units. The LPR Manager manages the data *(reads and hits)* collected by the LPR units that it controls, and updates Patrollers.

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.

The LPR Manager stores all LPR data *(reads, hits, images, vehicle status, GPS data, and so on)* collected from the LPR units that it manages into a central database for data mining and reporting. The LPR Manager is also responsible for updating the Patrollers in the field with hotfixes, hotlist updates, and so on.

**System:** AutoVu IP license plate recognition

**Task:** Role view

<table>
<thead>
<tr>
<th>Identity</th>
<th>Name, description, and relationships of this role with other entities in the system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
<td>General parameters within which this role should operate.</td>
</tr>
<tr>
<td>Resources</td>
<td>Server and database configuration for this role.</td>
</tr>
<tr>
<td>Options</td>
<td>General AutoVu settings and optional features.</td>
</tr>
</tbody>
</table>
**Properties**

Use the *Properties* tab to specify which hotlists, permits, fixed and mobile Sharps, and Patroller user groups the LPR Manager is responsible for.

- **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, and matches the hotlists against the reads collected from fixed Sharp units to produce hits.

- **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.

  **NOTE** Only Patrollers configured for city and university parking enforcement require permits.

- **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 *DiscoveryPort* setting on the Sharp.

  **IMPORTANT** Each LPR Manager must use a unique *discovery port*.

- **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.

  If the Patroller Logon option is configured to *SecureLoginName* or *SecureLoginName-AndPassword* in Patroller Settings Viewer, 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.

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 role.

Database

All database management principles are the same for the LPR Manager role as with any other role.

Options

The Options tab is used to configure additional AutoVu features. The availability of certain features depends on what is supported by your Security Center license.
General

Use the General settings to configure how long the data from the LPR Manager is kept in the LPR Manager database. This is also where you create the root folder for the LPR Manager.

**IMPORTANT** Please read the following notes 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 AutoVu LPR Manager, each LPR Manager must have a different root folder.

- **Patroller route retention period.** Minimum number of days the Patroller route data (GPS positions) is kept in the database. Maximum is 2000 days.
- **Hit retention period.** Minimum number of days the hit data is kept in the database. Maximum is 2000 days.
- **Read retention period.** Minimum number of days the license plate reads are kept in the database. Maximum is 2000 days.
- **Event retention period.** Minimum number of days the LPR events (License plate read, License plate matched) are to be kept in the database. Maximum is 2000 days.
• **Root folder.** The main folder on the computer hosting the LPR Manager. This is where all the LPR Manager configuration files are created, saved, and exchanged between the Patrollers it manages.

The LPR Manager root folder includes the following subfolders:

- **Hotlist.** Contains the hotlists that are downloaded to Patroller.
- **ManualTransfer.** Contains the configuration and data files updates that are transferred manually from a USB device between Security Center and Patroller.
- **Users.** Contains the list of users who are allowed to connect to Patroller.
- **Offload.** Contains the data offloaded by Patroller.
- **PatrollerSettings.** Contains the LPR settings defined in the General Settings – Applications tab of the LPR task.
- **Permits.** Contains the permit lists that are downloaded to Patroller.
- **Updates.** 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 directly.
- **Zones.** Subfolder containing the overtime rules, permit restrictions, and parking facilities that are downloaded to Patroller.
LPR Manager role

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.
- **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 with the read data, the high resolution close-up image of the license plate.
  - *Context image.* Include with the read data, the wide angle context image of the vehicle.
- **Channel Security.** Choose to encrypt the communication channel between Security Center and Patroller.
  
  IMPORTANT Encryption must be enabled both in the Security Center Config Tool and in Patroller Config Tool.
  - *Encrypt Communication Channel.* Encrypt communication between the Patroller and Security Center.
- *Accept Non Encrypted Messages.* Security Center will accept incoming connections from Patrollers that do not have the encryption option enabled.

**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.
Email notification

The Email notification setting turns on email notifications for hotlist hits.

Before you begin: To use this feature, you need to do the following:

- On the computer hosting the LPR Manager, you'll need to configure the mail server in Server Admin.
- If you want to send a hotlist hit notification to a single address, then you'll need to set the actual email address for each hotlist in the hotlist Advanced tab.
- If you want to send a hotlist hit notification to the specific email address defined for each hotlist entry, then you'll need to add the email address attribute to the hotlist attributes.

The configurable parameters are:

- Annotation email address. Use this feature when you want to send notifications to the email address that was entered in the hotlist data file for that particular hotlist entry. Enter name of the email address attribute field.

  **IMPORTANT** You can choose whatever name you want for the notification email address attribute but you must use the same attribute name for each Hotlist entity that contains notification email addresses.
- **Email components.** Choose the images you want to attach to the hotlist hit notification and whether to hide the license plate numbers in the message body.
  - *License plate image.* High resolution close-up images of license plate.
  - *Context image.* A wider angle color image of the vehicle.
  - *Overview image.* Overview camera taken from a separate camera, such as in a Street Sweeper context.
  - *License plate.* Hide, using asterisk (*), the Read plate number and Matched Plate number in the message body of the notification email.
- **Log emails in.** Select the check box to log hotlist hit notification emails. Type the full path to the log file.
Geocoding

The *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 the geocoding function if your Patrollers are equipped with GPS (AutoVu Navigator) but not equipped with maps.

- **Map type.** Displays the map type set in the Security Center license. If MapInfo is the map type, then the following options are displayed:
  - **MapInfo workspace (MapInfo only).** Folder where the MapInfo files (Maps.mws and associated files) are found. This folder must be on the same computer where the LPR Manager is installed.
  - **MapInfo version.** If using MapInfo version 6 and onward, you must select New.

Matching

The *Matching* setting matches the license plate reads from fixed LPR units to hotlists.

**IMPORTANT** You'll need to select the hotlists you want to match from the System LPR Hotlist tab.
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.** Folder where the XML templates are located.
- **XML export folder.** Folder where the exported files are saved.
- **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:

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>h</td>
<td>Hour</td>
</tr>
<tr>
<td>m</td>
<td>Minute</td>
</tr>
<tr>
<td>s</td>
<td>Second</td>
</tr>
<tr>
<td>:</td>
<td>Must use a colon (:) between the hour, minute, and second units.</td>
</tr>
</tbody>
</table>
LPR Manager role

- Date format. Enter the date format used in the export files.
  To identify the units of a date, use the following notation:

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>Month in numerals</td>
</tr>
<tr>
<td>MM</td>
<td>Month in numerals with leading zero.</td>
</tr>
<tr>
<td>MMM</td>
<td>Month abbreviation. For example Apr for April.</td>
</tr>
<tr>
<td>y</td>
<td>Year without century. For example, y displays 11 for 2011.</td>
</tr>
<tr>
<td>yyy</td>
<td>Year with century. For example, yyyy displays 2011</td>
</tr>
<tr>
<td>d</td>
<td>Date</td>
</tr>
<tr>
<td>dd</td>
<td>Date with leading zero.</td>
</tr>
<tr>
<td>ddd</td>
<td>Day of week three letter abbreviation. For example, d displays Wed for Wednesday.</td>
</tr>
<tr>
<td>ddddd</td>
<td>Day of week. For example, ddddd displays Wednesday.</td>
</tr>
<tr>
<td>Delimiters</td>
<td>Can use space or dash (-) between units in the date.</td>
</tr>
<tr>
<td>Example</td>
<td>ddddd MM dd, yyy displays Wednesday April 06, 2011.</td>
</tr>
</tbody>
</table>
**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.

- **XML template file.** Specify where the XML templates are located.
- **XML data folder.** Specify where the data files are found.

**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.

**Hotlist filtering**

The *Hotlist filtering* settings allow you to choose what to do whenever a hotlist is modified. The LPR Manager can detect if the new or modified hotlist includes entries that contain invalid (non-alphanumeric) characters. You can configure the LPR Manager to either delete...
the invalid hotlist entries, 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.

- **Plate number valid characters.** Select the Language you want the plate characters to be filtered by from the drop-down list.

- **Invalid plate number.** Configure how the LPR Manager handles invalid hotlist records. Select one of the following:
  - **Modify record.** (Default setting). Leaves any non-alphanumeric characters in the plate number blank. For example, the plate number “123#%Z” becomes “123Z”.
  - **Remove record.** Deletes the hotlist entry 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.
The LPR task allows you to configure the general settings for LPR (license plate recognition) and the related entities that are not found in the Logical view.

System: AutoVu IP license plate recognition

Required license option: AutoVu

Category: Administration

The LPR task includes the following views:

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Units</td>
<td>Shows the LPR Manager roles and the units they control as a hierarchy.</td>
</tr>
<tr>
<td>Hotlists</td>
<td>Lists all hotlists in alphabetical order.</td>
</tr>
<tr>
<td></td>
<td>For more information, see &quot;Hotlist entity&quot; on page 160.</td>
</tr>
<tr>
<td>Overtime rules</td>
<td>This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.</td>
</tr>
<tr>
<td>Parking facilities</td>
<td>This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.</td>
</tr>
<tr>
<td>Permit restrictions</td>
<td>This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.</td>
</tr>
<tr>
<td>Permits</td>
<td>This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.</td>
</tr>
<tr>
<td>General settings</td>
<td>Lets your configure the general settings pertaining to access control and to install and configure custom card formats.</td>
</tr>
</tbody>
</table>
Units

The LPR – Units view shows the LPR Manager roles and the units they control in a hierarchy.

![Image of LPR administration task](image)

A. Selected view (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" on page 199
- "Hotlist" on page 201
- **Overtime rule.** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click [here](#) for the most recent version of this document.
- **Permit.** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click [here](#) for the most recent version of this document.
- "Annotation fields" on page 202
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 categories a Patroller user must pick 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 count 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. Configure the following:
  - *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. For more information, see "Advanced" on page 164.

- **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 Hit report.
Hotlist

The Hotlist tab allows you to define the custom fields that will appear in Patroller when the user enters a new wanted or rejects or accepts a hit. The settings downloaded along with the selected hotlists to Patrollers when the Patroller user logs on. The attributes are also available as filter options for hit reports in Security Desk.

- **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.
- **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.
- **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.
- **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.
- **Enable “No infraction” button.** Select this option to enable the No infraction button in the Patroller hit form. This button allows the Patroller user to skip the hit form after enforcing a hit.
Annotation fields

The **Annotation fields** tab allows you to define additional selectors to appear in Security Desk **Hits** report.

To be valid, the selector must relate to information contained in the hit. For example, if you configure the *CarColor* enforced hit attribute, the user will be asked to enter the car color when enforcing a hit.

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.
NOTE 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 "Upgrading Patroller and Sharp units from Security Center" on page 115.

- **Update all.** Update all units that are controlled by the currently-selected LPR Manager. The *Update all* button updates only the units on the current tab, not all units on all tabs. For example, if you’re on the *Patroller and Sharp units* tab, you’ll update all Patrollers and Sharp units on the list.
- **Patrollers and Sharp units.** Displays the Patrollers and Sharp units (fixed and mobile) eligible for an update.
- **Update services.** Displays the Sharp services eligible for an update.
- **Firmware upgrade.** Displays the Sharps that are eligible for a firmware upgrade.
Patroller Config Tool reference

This section describes all the Patroller Config Tool options you can use to customize Patroller for your particular AutoVu system.

IMPORTANT This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

Many of the options described are not required for a typical AutoVu deployment. For more information on a typical deployment process, see the following chapters:

• Chapter 3, “AutoVu fixed deployment overview” on page 22.
• Chapter 4, “AutoVu mobile deployment overview” on page 40.

This section includes the following topics:

• "General" on page 205
• "Security Center" on page 207
• "Plugin" on page 211
• "Cameras" on page 212
• "Hits" on page 213
• "Navigation" on page 217
• "User interface" on page 220
• "Advanced" on page 222
The General settings page allows you to configure basic Patroller options such as the Patroller unit's name, how users should log on, etc.

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click [here](#) for the most recent version of this document.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Patroller name** | Enter the name of the Patroller unit as you want it to be seen in Security Center. **Note** Please note the following:  
• The Patroller name is different from your Security Center username. You log on to Patroller with your Security Center username, which is created when you create users and user groups in Config Tool. The Patroller name you create here is the name of the Patroller unit or vehicle as it will appear in Config Tool and Security Desk. For more information on creating users and user groups, see the Config Tool help.  
• You must be connected to Security Center (e.g. in range of the company WiFi network) to configure the Patroller name. |
| **Login type**  | Select how to log on to Patroller:  
• NoLogin. No username or password required.  
• Windows Login. Similar to NoLogin in that the Patroller user doesn't need to enter a username or password. Patroller automatically uses the Windows credentials to logon.  
• SecureLoginName. Only username required.  
• SecureLoginNameAndPassword. Username and password required.  
You create usernames and passwords in Config Tool when configuring users and user groups. |
<p>| <strong>Database name</strong> | Enter the name of the Patroller database. <strong>Note</strong> You can easily create a new Patroller database by changing the database name. |
| <strong>Connection string</strong> | The string to connect to the Patroller database. <strong>Note</strong> You shouldn’t need to configure this option since SQL is installed automatically, or an existing SQL instance is used, when you install Patroller. |</p>
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advanced</strong></td>
<td><strong>Max logout</strong>&lt;br&gt;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.</td>
</tr>
<tr>
<td><strong>Store reads for</strong></td>
<td>Set the amount of time that reads are stored in the 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.</td>
</tr>
<tr>
<td><strong>Store hits for</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Record search</strong></td>
<td>Set the amount of time that records (reads or hits) are searchable by the 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.</td>
</tr>
<tr>
<td><strong>Record display</strong></td>
<td>Set the amount of time that a record can be displayed. Default is 12 hours.</td>
</tr>
<tr>
<td><strong>Folder path</strong></td>
<td>Type the folder path where the database files are created and replicated.</td>
</tr>
<tr>
<td><strong>Offload query timeout</strong></td>
<td>Define the timeout duration for the offload queries. The default timeout is 1800 seconds.</td>
</tr>
</tbody>
</table>
Security Center

The Security Center page is where you configure how Patroller connects to Security Center, and how data is offloaded to Security Center.

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

This section includes the following topics:

- "Live connection" on page 207
- "Offload" on page 209

Live connection

Configure how Patroller connects to Security Center.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 209.  
  Best practice: 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.                                                                |
| Encrypt communication channel | Turn on to encrypt communication between Patroller and Security Center.  
  To use this feature, you must also encrypt communication in Config Tool on the LPR Manager Properties page, under Live. For more information, see "Live" on page 188. |
### Update provider port

Specify the port that Security Center uses to send hotfixes and other updates for Patroller and connected Sharp units.

To use this feature, you must also specify the same port number in Security Center. In Config Tool, go to the LPR Manager Properties page, turn on the Update provider, and then enter the port number.

For more information, see "Update provider" on page 195.

### 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. The default transfer period is every 240 minutes.

**Note** You can disable Periodic transfer for specific hotlists (not permit lists) in Config Tool on the hotlist’s Advanced page. For more information, see "Advanced" on page 164.
Offloading is how you transfer reads, hits, and other Patroller data to Security Center. This section explains the different offload options.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offload method</td>
<td>Select your offload method:</td>
</tr>
<tr>
<td></td>
<td>• None. Does not offload data.</td>
</tr>
<tr>
<td></td>
<td>• LocalFile. You can configure Patroller to offload data to a file on the in-vehicle computer. After you have offloaded the data, you can then copy the data to a USB key, and transfer it to the Security Center computer. For more information on how to automate the process of transferring LPR data to a USB device, see &quot;Setting up USB support&quot; on page 140</td>
</tr>
<tr>
<td></td>
<td>• WcfTransfer. 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 the company parking lot or garage and in range of the company's WiFi network. You also use this procedure when you offload data to a network drive rather than your local drive.</td>
</tr>
</tbody>
</table>

Note Please note the following about using WcfTransfer:

• 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" on page 186

• If you try to offload, and a connection to Security Center is not available, the offload is done on your local in-vehicle computer. You can then transfer the offload data to the Security Center using a USB key.

<table>
<thead>
<tr>
<th>Local offload path</th>
<th>If using LocalFile 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).</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMPORTANT</td>
<td>Do not specify the folder. Patroller creates the offload folder on the drive you specify.</td>
</tr>
</tbody>
</table>

| Use encryption     | Turn on to encrypt the offloaded data.                                                                                                       |
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 5.1, and copy the OffloadPublicKey.xml file to your clipboard.
2. On the Patroller computer, go to C:\Program Files\Genetec AutoVu 5.1\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 5.1\MobileClient\OffloadPublicKey.xml).

### Setting | Description
---|---
**Public key** | 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 5.1, and copy the OffloadPublicKey.xml file to your clipboard.
2. On the Patroller computer, go to C:\Program Files\Genetec AutoVu 5.1\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 5.1\MobileClient\OffloadPublicKey.xml).

**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 file (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 Offload method and Action after offload are set 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.
The Plugin page is where you enable and configure AutoVu custom solutions. If you select None, no plugin settings are displayed.

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I trak</td>
<td>• Debug log. Turn on to generate a HitInfo.txt debug log file.</td>
</tr>
<tr>
<td></td>
<td>• URL. Displays the URL of the ITrak WebService.</td>
</tr>
<tr>
<td>Miami parking</td>
<td>• Url. Displays the URL.</td>
</tr>
<tr>
<td>Scofflaw mdt</td>
<td>• Plate type. Displays the plate type with one letter. This is only for Philadelphia specifications.</td>
</tr>
<tr>
<td></td>
<td>• Queries path. Displays the path on the local machine for storing text files with accepted hits.</td>
</tr>
<tr>
<td>Survey</td>
<td>• Division. Set this option to use a specific hit accept survey.</td>
</tr>
</tbody>
</table>
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.

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

### Setting | Description
--- | ---
**Units** These are the Sharp units connected to your in-vehicle LAN. Use the Start discovery button to add all cameras that are physically connected.
- **Start discovery.** Automatically detect installed Sharp cameras and add them to the network. You will need to specify each camera’s orientation.
- **Add camera ( ).** 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 (e.g. 192.168.10.1 for a SharpX). You also need to specify the camera’s orientation, meaning where it’s installed on the vehicle (e.g. right, left, front center, etc).
  - 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).
- **Delete camera ( ).** Remove a Sharp camera from the network.
- **Edit camera ( ).** Edit the properties of a Sharp camera on the network.

For more information on how to add Sharp units to Patroller, see "Connecting Sharp units to Patroller" on page 137.

**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 pause plate reading when you first log on to Patroller.

**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. If you decide to change one port, remember to also change the other. For more information on configuring the Sharp, see "Configuration" on page 229.
The Hits page allows you to configure options related to hits and hotlists, such as the hit display priority, New Wanted options, etc.

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

### General

Configure options common to both hotlists and permit lists.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow consecutive hits</td>
<td>Turn on to allow multiple hits with the same information (plate number and state) to appear in a row. When this option is off, Patroller won’t register a hit for the same vehicle twice.</td>
</tr>
<tr>
<td>Pause reads while enforcing</td>
<td>Turn on to pause plate reading while you’re accepting/enforcing hits. When off, Patroller continues to read plates while you’re accepting hits.</td>
</tr>
<tr>
<td>Allow popup hit</td>
<td>Turn on for Patroller to display hits on screen as they occur. Turn off for hits to accumulate in the background.</td>
</tr>
<tr>
<td>First hit on top</td>
<td>Choose the order that hits are displayed. Turn on to display the first hit at the top of the list. Turn off to display the most recent hit at the top of the list.</td>
</tr>
</tbody>
</table>

### Hotlists

Configure hotlist and New Wanted options.

**NOTE** If you want to set New Wanted attributes and categories, you need to do it in Config Tool. For more information, see "Hotlist" on page 201.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable new wanted</td>
<td>Turn on to allow Patroller users to add New Wanted hotlist entries.</td>
</tr>
<tr>
<td>Enable new wanted management</td>
<td>Turn on to allow Patroller users to edit and delete New Wanted entries from the database.</td>
</tr>
<tr>
<td>Enable comments for new wanted</td>
<td>Turn on to activate a text box where you can enter a comment when entering a New Wanted hotlist item.</td>
</tr>
</tbody>
</table>
### Hits

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| New wanted expiry options (days) | Select one or more expiration options for New Wanted entries. For example, if you create the entries “1”, “5”, and “10”, when Patroller users enter a New Wanted item, they can choose for that item 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 expiration option from the list. |
| Bypass hit enforcement       | Turn this feature 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 hotlist hits    | Turn this option on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction.  
  **Note** If you’ve configured a hit accept or hit reject survey, it is ignored when this option is enabled. |
| Display hits by priority     | Turn on to display hits by the priority specified in Config Tool. For example, if “Hotlist A” has a higher priority then “Hotlist B”, hits generated from Hotlist A will be displayed first. |

### Permits

Enable permits and shared permits (if applicable), and turn hit enforcement on/off.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use permit</td>
<td>Turn on to enable the use of permits.</td>
</tr>
<tr>
<td>Bypass permit hit enforcement</td>
<td>Turn this feature 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.</td>
</tr>
</tbody>
</table>
| Auto enforce permit hits       | Turn this option 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. |
## Overtime

Configure options for overtime parking enforcement, including wheel imaging settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use overtime</td>
<td>Turn on to enable the use of overtime rules.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Click to configure the <em>Advanced overtime settings</em>:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Link read persistence duration.</strong> Specify the amount of time (in hours) that a particular record is displayed to the user. Records older than this value will disappear from the user at the start of the next shift. The default duration is 12 hours.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Minutes to due vehicles.</strong> Specify the amount of time before the vehicles are due. The default value is 5 hours.</td>
</tr>
<tr>
<td>Bypass hit enforcement</td>
<td>Turn this feature 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.</td>
</tr>
<tr>
<td>Auto enforce overtime hits</td>
<td>Turn this option 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.</td>
</tr>
<tr>
<td>Use tire images</td>
<td>Turn on to use overtime with wheel imaging. Wheel images are saved to the in-vehicle computer.</td>
</tr>
</tbody>
</table>
**Setting** | **Description**
--- | ---
**Wheel imaging enforced** | Select whether wheel imaging is enforced or not from the drop-down list:
- **Mandatory.** The user is required to select wheel imaging for both passes in order to enforce a hit.
- **Optional.** The user can enforce a hit without selecting wheel imaging.

**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.

**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.

**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.
The Navigation page allows you to configure options related to Patroller’s location and movement, such as GPS functionality, map usage, etc.

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

---

### GPS

Enable GPS and configure GPS options.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use GPS</strong></td>
<td>Turn on to activate communication with the GPS device.</td>
</tr>
<tr>
<td><strong>Consecutive invalid GPS strings before restart</strong></td>
<td>Specify the number of consecutive invalid GPS strings allowed before the device is restarted. The default number is 10.</td>
</tr>
<tr>
<td><strong>Noise</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>GPS initialization string</strong></td>
<td>Displays the initialization commands to be sent to the GPS device when you login to the application.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Specify the COM port number of the GPS device as seen in Windows Device Manager.</td>
</tr>
<tr>
<td></td>
<td>• If you’re using the USB GPS, the name of the device in Device Manager is <em>Prolific USB-to-Serial Comm Port</em>.</td>
</tr>
<tr>
<td></td>
<td>• If you’re using the GPS antenna that connects to the Navigator box, the name of the device in Device Manager is <em>u-blox 5 GPS and GALILEO Receiver</em>.</td>
</tr>
<tr>
<td><strong>Baud rate</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NavBox</td>
<td>Turn this setting on to enable the Navigator box. <strong>Note</strong> If you’re using the Navigator box for odometry as well as GPS, you also need to turn on the Use odometry option.</td>
</tr>
<tr>
<td>Port</td>
<td>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 <em>Silicon Labs CP210x USB to UART Bridge</em>.</td>
</tr>
<tr>
<td>Shutdown delay</td>
<td>Specify the number of seconds to wait after the vehicle's ignition is turned off before shutting down Patroller. To disable this feature, enter “0”.</td>
</tr>
<tr>
<td>Use odometry</td>
<td>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.</td>
</tr>
<tr>
<td>Use reverse</td>
<td>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.</td>
</tr>
<tr>
<td>Scale</td>
<td>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.</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>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.</td>
</tr>
<tr>
<td>Read when car is stopped</td>
<td>Specify whether or not to continue reading plates when the Patroller vehicle is stopped. For example, in a City Parking Enforcement scenario, Patroller vehicles may stop and reverse frequently.</td>
</tr>
</tbody>
</table>
Maps

Choose which type of mapping service to use, and configure GPS related mapping options.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mapping type</strong></td>
<td>Select the map type from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• None. Do not use maps.</td>
</tr>
<tr>
<td></td>
<td>• MapInfo. The default map type for AutoVu.</td>
</tr>
<tr>
<td></td>
<td>• OpenStreetMap. For Data source, choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Internet. If you have a constant internet connection in the vehicle (e.g. 3G wireless), choose this option for live maps.</td>
</tr>
<tr>
<td></td>
<td>• Local file. Mapping data comes from a file located on the in-vehicle computer’s hard drive. If you choose this option, type the location of the file in the Local cache file field.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong> For more information on using OpenStreet maps, contact your Genetec representative.</td>
</tr>
<tr>
<td><strong>Show vehicle route</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>GPS distance tolerance</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>GPS odometry calibration tolerance</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Max distance error</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

IMPORTANT This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

General

Configure the settings related to how Patroller is displayed.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System unit</td>
<td>Displays speed and distance in metric or U.S. system (e.g. km/h or mph).</td>
</tr>
<tr>
<td>Default plate state</td>
<td>Displays the default state or province when users enter plates manually.</td>
</tr>
<tr>
<td>Circle plate</td>
<td>Turn on for Patroller to circle license plates in the context images.</td>
</tr>
<tr>
<td>Show overview label</td>
<td>Turn on to display the overview label if the overview image exists.</td>
</tr>
<tr>
<td>Enable reviews</td>
<td>Turn on to allow users to review reads or hits in the Patroller user interface.</td>
</tr>
<tr>
<td>Show hotlist status indicator</td>
<td>Turn on to display the hotlist status LED which informs users if a hotlist is being downloaded, or if there are any download/parsing errors.</td>
</tr>
<tr>
<td>Show download list on startup</td>
<td>Turn on to automatically pop up the screen displaying download file information, such as hotlists, when the download is complete and the status LED turns green.</td>
</tr>
</tbody>
</table>

System

Configure the settings related to how Patroller behaves.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable minimize button</td>
<td>Turn on allow the Patroller window to be minimized.</td>
</tr>
<tr>
<td>Enable system tray menu</td>
<td>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).</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Start application minimized</strong></td>
<td>Turn on to start Patroller minimized. This option is not recommended if users need to log on to Patroller with a username and/or password.</td>
</tr>
<tr>
<td><strong>Silent mode</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Enable main buttons</strong></td>
<td>Turn on to enable the Disabled, Hit, Zone, ShowDue, Manual Capture, and Cameras buttons.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  For the Street Sweeper plugin, this setting must be disabled.</td>
</tr>
<tr>
<td><strong>Show taskbar when fullscreen</strong></td>
<td>Turn on to show the Windows taskbar when Patroller is in fullscreen mode.</td>
</tr>
<tr>
<td><strong>Enable printing</strong></td>
<td>Turn on to enable printing of read/hit information from the Patroller window.</td>
</tr>
<tr>
<td><strong>Show username in tray</strong></td>
<td>Turn on to show the Patroller user’s Security Center username in the notification bar.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>  If you’re using Patroller for City Parking Enforcement or University Parking Enforcement, you can turn this option off to make room for long overtime rule, or permit restriction names.</td>
</tr>
</tbody>
</table>
Advanced

The Advanced page allows you to configure advanced Patroller options. Most AutoVu deployments do not require advanced options to be modified.

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

**IMPORTANT** Advanced settings in Patroller Config Tool are used mostly by Genetec Technical Support for diagnostic and debugging 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, you should contact your Genetec representative before you attempt to modify them.

### Analytics

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display following analytics fields</td>
<td>Display additional information in the Patroller information panel for a read or hit. Type one of the following (case-sensitive) to active the feature:</td>
</tr>
<tr>
<td></td>
<td>• Motion Detection. When Patroller reads a plate, it detects and displays if the vehicle is approaching or moving away.</td>
</tr>
<tr>
<td></td>
<td>• Vehicle Type. Certain license plates include character symbols that identify specific vehicle types (e.g. taxi, transport, etc). Patroller reads these symbols, and displays the vehicle type along with the other read/hit information.</td>
</tr>
</tbody>
</table>

### Hit

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm real time</td>
<td>Turn on to require a confirmation of a hit status (enforced, not enforced) in the real-time mode.</td>
</tr>
</tbody>
</table>

### Hit hotlist

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use simple matcher</td>
<td>Turn on the SimpleMatcher feature. Simple matcher reduces the LPR matching mechanism in order to minimize the number of false hits that can occur, especially in Law Enforcement installations using very large hotlists.</td>
</tr>
</tbody>
</table>
## Mobile patroller hit

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable plate editing</td>
<td>Turn on to allow editing of license plate numbers when you receive a hit. From the hit screen, click or tap the plate text string to open the editor.</td>
</tr>
</tbody>
</table>

## User interface

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable manual capture</td>
<td>Turn on to enable the Manual Capture option in Patroller. Users can manually enter a license plate for capture.</td>
</tr>
</tbody>
</table>
Sharp Admin reference

This section describes all the Sharp Admin options you can use to customize a Sharp unit 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 the following chapters:

- Chapter 3, “AutoVu fixed deployment overview” on page 22.
- Chapter 4, “AutoVu mobile deployment overview” on page 40.

**NOTE** The settings shown in the Sharp Admin are different depending on what type of Sharp unit you’re connecting to. For example, if you’re connecting to a SharpX, you’ll see the number of available inputs on the LPR Processing Unit. That information won’t be displayed if you’re connecting to a Sharp XGA.

This section includes the following topics:

- "Status" on page 225
- "Configuration" on page 229
- "Live feed" on page 237
- "Diagnostics" on page 239
Status

The Status page displays information on the status of the Sharp unit you're connected to. You'll find information such as the Sharp name, serial number, GPS coordinates (if it's a fixed Sharp), and license. The Status page is also where you can reboot the Sharp unit, and export diagnostic data.

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click [here](#) for the most recent version of this document.

This section includes the following topics:

- "Properties" on page 225
- "License" on page 226
- "GPS coordinates" on page 226
- "Clock" on page 226
- "Actions" on page 227
- "System resources" on page 227

## 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).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the Sharp unit name.</td>
</tr>
<tr>
<td>Serial number</td>
<td>Displays the Sharp hardware serial number.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the type of Sharp unit (e.g. Sharp XGA, SharpX, etc).</td>
</tr>
<tr>
<td>Inputs</td>
<td>Displays the number of physical inputs on the SharpX LPR Processing Unit.</td>
</tr>
<tr>
<td>Relays</td>
<td>Displays the number of physical relay inputs on the SharpX LPR Processing Unit.</td>
</tr>
<tr>
<td>GPS</td>
<td>Displays whether or not GPS is supported on a Sharp XGA (with attached GPS antenna).</td>
</tr>
<tr>
<td>Lens</td>
<td>Displays the unit lens depth available for context images and LPR images.</td>
</tr>
<tr>
<td>Illuminator</td>
<td>Displays the illuminator on the Sharp (e.g. 850 nm)</td>
</tr>
</tbody>
</table>
License

Displays whether or not the Sharp has a valid AutoVu license.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays if unit license is valid.</td>
</tr>
</tbody>
</table>

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. For more information, see "Location" on page 158.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Longitude</td>
<td>Displays the current GPS longitude coordinates if GPS functionality is supported.</td>
</tr>
<tr>
<td>Latitude</td>
<td>Displays the current GPS latitude coordinates if GPS functionality is supported.</td>
</tr>
</tbody>
</table>

Clock

The Sharp unit's internal clock.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays if there is a drift between the local and the remote clock.</td>
</tr>
<tr>
<td></td>
<td>• Local clock. Clock on the machine that is running the Sharp Admin. For example, the machine you used to open Internet Explorer and connect to the Sharp.</td>
</tr>
<tr>
<td></td>
<td>• Remote clock. The Sharp unit’s internal clock.</td>
</tr>
</tbody>
</table>

Best practice: You should always synchronize the clocks (click Synchronize now), especially if you are using an FTP extension. By doing this, you ensure that the timestamp attached to reads will be accurate.
**Actions**

Displays several actions you can perform.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reboot Sharp</strong></td>
<td>Click to reboot the Sharp unit. You will be asked to confirm reboot. If you reboot the Sharp, you’ll lose connection to the Sharp Admin. Wait a few minutes for the Sharp to reboot, and then refresh the Web page to log on again.</td>
</tr>
<tr>
<td><strong>File versions</strong></td>
<td>Displays the versions of the various services running on the Sharp. You can use this information to confirm your Sharp is up to date.</td>
</tr>
<tr>
<td><strong>Export diagnostic data</strong></td>
<td>Click to export the unit diagnostic data. Select a folder, and then click Save.</td>
</tr>
<tr>
<td><strong>Change password</strong></td>
<td>Click to change the password you use to log on to the Sharp Admin. 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 &quot;Portal Security&quot; on page 230</td>
</tr>
<tr>
<td><strong>Show Extension details</strong></td>
<td>When you have an extension configured (see &quot;Extension&quot; on page 234), this will display information about that extension’s status.</td>
</tr>
<tr>
<td><strong>Configure the other unit</strong></td>
<td>If you are connected to a SharpX · Multi, this opens a new Sharp Admin 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.</td>
</tr>
</tbody>
</table>

**System resources**

Displays the status of the Sharp hardware.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU</strong></td>
<td>Displays the Sharp CPU usage.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Usage (%)</strong></td>
<td>The current CPU usage.</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td>Displays the memory drives.</td>
</tr>
<tr>
<td><strong>Free space (MB)</strong></td>
<td>Displays the amount of free space left on the memory drives.</td>
</tr>
<tr>
<td><strong>Total space</strong></td>
<td>Displays the total space (in MB) available on the memory drives.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Used (%)</strong></td>
<td>Displays how much percentage of memory is currently being used on each drive.</td>
</tr>
</tbody>
</table>
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 Admin to use HTTPS encryption, select the Context (e.g. Oregon, Quebec, etc), specify the read strategy (e.g. slow or fast moving vehicles), and more.

IMPORTANT  This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

This section includes the following topics:

- "Network settings" on page 230
- "Portal Security" on page 230
- "Camera status LED" on page 231
- "Support wheel imaging" on page 231
- "Camera settings" on page 231
- "Analytics" on page 233
- "Extension" on page 234
- "Inputs" on page 235
- "Triggers" on page 236
Network settings

Configure the Sharp network settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Click Edit, select a network setting mode from the drop-down list, and then click Save. You can select one of the following modes:</td>
</tr>
<tr>
<td></td>
<td>• DHCP. Select DHCP if you're connecting the Sharp to a DHCP server, which assigns the required IP address. When you're on a DHCP server with DNS capability, you'll be able to connect to the Sharp using the Sharp name (e.g. Sharp1234) rather than the IP address (e.g. 198.162.10.100). For example, you would select DHCP if you're configuring a SharpX system with a router in the vehicle. In this case, the router assigns the IP address.</td>
</tr>
<tr>
<td></td>
<td>• Static. This is the default state of the Sharp, and is used in most situations. The default static IP addresses for the Sharps are:</td>
</tr>
<tr>
<td></td>
<td>• 198.162.10.100 (Sharp)</td>
</tr>
<tr>
<td></td>
<td>• 198.162.10.1 (SharpX SBC1)</td>
</tr>
<tr>
<td></td>
<td>• 198.162.10.2 (SharpX SBC2)</td>
</tr>
<tr>
<td>IP address</td>
<td>Enter the new IP address you want to assign to the Sharp unit.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>If you changed the subnet when selecting a new static IP address, enter the new subnet mask.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Enter the gateway.</td>
</tr>
</tbody>
</table>

**Portal Security**

Configure the Sharp Admin to accept HTTPS encrypted connections (HTTP is the default).

**NOTE** Changes will take effect after a unit reboot.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Sharp Admin security methods</td>
<td>Select one of the following networking protocol options:</td>
</tr>
<tr>
<td></td>
<td>• HTTP (Hypertext Transfer Protocol)</td>
</tr>
<tr>
<td></td>
<td>• HTTPS (Hypertext Transfer Protocol Secure)</td>
</tr>
</tbody>
</table>
Camera status LED

Turn the camera LED on or off.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run in covert mode</td>
<td>Select this option to turn off the LED on the front of the Sharp unit,</td>
</tr>
<tr>
<td></td>
<td>making it less conspicuous.</td>
</tr>
</tbody>
</table>

Support wheel imaging

This section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture high definition wheel</td>
<td>Select the video format type from the drop-down list:</td>
</tr>
<tr>
<td>images</td>
<td>• NTSC</td>
</tr>
<tr>
<td>Video format</td>
<td>• PAL</td>
</tr>
</tbody>
</table>

Camera settings

Configure the Sharp camera settings. This settings are different depending on whether you're connected to a Sharp, Sharp EX, or SharpX.

This section includes the following topics:

• "Sharp" on page 232
• "Sharp EX" on page 232
• "SharpX" on page 232
Sharp

If you're connected to a Sharp XGA or VGA, you'll see the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture high definition</td>
<td>Standard definition context images are 320 x 240 (pixels). Select this</td>
</tr>
<tr>
<td>context images</td>
<td>setting to capture images in 640 x 480.</td>
</tr>
</tbody>
</table>

Sharp EX

If you're connected to a Sharp EX, you'll see the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video format</td>
<td>Select the video format of the external camera(s) you connect to the Sharp</td>
</tr>
<tr>
<td></td>
<td>EX video input(s):</td>
</tr>
<tr>
<td></td>
<td>• NTSC. 720 x 480 @ 29.97 fps.</td>
</tr>
<tr>
<td></td>
<td>• PAL. 720 x 576 @ 25 fps.</td>
</tr>
<tr>
<td>Capture mode</td>
<td>Select the mode that represents how the cameras are connected to the Sharp</td>
</tr>
<tr>
<td></td>
<td>EX video inputs:</td>
</tr>
<tr>
<td></td>
<td>• Input 1: LPR and context. You have one camera connected to Video 1 on the</td>
</tr>
<tr>
<td></td>
<td>Sharp EX. The camera functions as both an LPR and context camera.</td>
</tr>
<tr>
<td></td>
<td>• Inputs 1 and 2: LPR and context. You have two cameras connected. Both</td>
</tr>
<tr>
<td></td>
<td>cameras function as LPR and context cameras.</td>
</tr>
<tr>
<td></td>
<td>• Input 1: LPR, Input 2: Context. You have two cameras connected. The camera</td>
</tr>
<tr>
<td></td>
<td>on Video 1 functions as the LPR camera, and the camera on Video 2 functions</td>
</tr>
<tr>
<td></td>
<td>as the context camera.</td>
</tr>
</tbody>
</table>

SharpX

If you're connected to a SharpX, and you see two interfaces (Interface 1 and Interface 2, or Interface 3 and Interface 4), it means that you're connected to one of the SBCs (single board computer) on a SharpX - Multi system. 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. This means you're connected to the SBC controlling the SharpX camera units that are physically connected to the first pair of camera interfaces.
  To configure the LPR Processing Unit's other SBC, click Configure the other unit located on the Status page, under Actions. For more information, see "Actions" on page 227.
- **Interface 3 and Interface 4.** These correspond to the camera interfaces 3 and 4 on the faceplate of the LPR Processing Unit. This means you're connected to the SBC controlling the SharpX camera units that are physically connected to the second pair of camera interfaces.

To configure the LPR Processing Unit's other SBC, click **Configure the other unit** located on the Status page, under Actions. For more information, see "Actions" on page 227.

### Setting Description

**Model**
Select a SharpX camera model from the drop-down list:
- **None.** Select this only if you're using a SharpX XGA camera unit on one of the interfaces, and you want the unit to run at its full 30 fps capability. For more information, see "Using a SharpX – Multi system" on page 129.
- **VGA.** You have a SharpX VGA connected on this interface.
- **XGA.** You have a SharpX XGA connected on this interface.

**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.

### Analytics

Configure which plates the Sharp will be reading (e.g. Quebec, Oregon, etc), 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 (e.g. some license plates include the issuing state or province).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Read plate state</strong></td>
<td>Select this option if you want the Sharp unit to read the plate origin.</td>
</tr>
<tr>
<td><strong>Context</strong></td>
<td>Select which plates the Sharp will be reading.</td>
</tr>
</tbody>
</table>
Configuration

Extension

Configure where the Sharp sends LPR data (Patroller, Security Center, or to an FTP server).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Extension</strong></td>
<td>Select the extension type from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• None. The default state. You must choose one of the options.</td>
</tr>
<tr>
<td></td>
<td>• FTP. Send LPR data to an FTP server. For more information, see</td>
</tr>
<tr>
<td></td>
<td>&quot;Configure the Sharp for an FTP connection&quot; on page 126.</td>
</tr>
<tr>
<td></td>
<td>• Patroller. Send LPR data to Patroller.</td>
</tr>
<tr>
<td></td>
<td>• Security Center. Send LPR data to Security Center.</td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>• For FTP only. Enter the FTP server name and location for the</td>
</tr>
<tr>
<td></td>
<td>LPR data. You’ll need the server name, port number (if different</td>
</tr>
<tr>
<td></td>
<td>than the standard FTP server port 21), and the name of the folder.</td>
</tr>
<tr>
<td></td>
<td>For example, ftp://&lt;ServerName&gt;:&lt;PortNumber&gt;/&lt;FolderName-OnServer&gt;/</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>• For FTP only. Enter the username for the FTP server.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>• For FTP only. Enter the password for the FTP server.</td>
</tr>
<tr>
<td><strong>Template</strong></td>
<td>• For FTP only. For more information, see &quot;Configure the Sharp for an FTP</td>
</tr>
<tr>
<td></td>
<td>connection&quot; on page 126.</td>
</tr>
<tr>
<td><strong>Upload context image</strong></td>
<td>• For FTP only. Send the context image to the FTP server.</td>
</tr>
<tr>
<td><strong>Upload LPR image</strong></td>
<td>• For FTP only. Send the LPR image to the FTP server.</td>
</tr>
<tr>
<td><strong>Connect to Security Center</strong></td>
<td>• For Security Center only. Select this option to initiate the connection to Security Center.</td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td>• For Security Center only. Enter the IP address of the Security Center</td>
</tr>
</tbody>
</table>

Read strategy

Select a read strategy from the drop-down list:

- **Fast moving vehicle.** Use this for mobile configurations (e.g. SharpX), or for fixed Sharps overlooking a highway where vehicles are travelling at moderate to high speeds.
- **Slow moving plate.** Use this for Sharps installed where vehicles are travelling slowly, or are stopped for a period of time (e.g. parking lot gates or toll stations).
Inputs

Displays the status of the SharpX LPR Processing Unit inputs. These inputs are typically used for tire imaging.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Letter of the input.</td>
</tr>
</tbody>
</table>
**Triggers**

Displays the status of the SharpX LPR Processing Unit relays. These relays are typically used for triggering mechanical events such as lowering a street sweeper’s brushes.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
<td>Shows whether the input is on or off.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reading is conditional on input state</strong></td>
<td>When you enable this setting, the Sharp will raise “best reads” if the conditions in the “Input” and “State” fields are met. For example, if you turn this setting on, and you set Input to “B” and State to “Off”, the Sharp raises best reads when input B is off. When this setting is disabled, then the Sharp raises best reads for all plates.</td>
</tr>
<tr>
<td><strong>Input</strong></td>
<td>Select an input from the drop-down list. Only required if the Reading is conditional on input state option is selected.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>Select a state for the input from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• On</td>
</tr>
<tr>
<td></td>
<td>• Off</td>
</tr>
<tr>
<td></td>
<td>Only required if the Reading is conditional on input state option is selected.</td>
</tr>
</tbody>
</table>
Live feed

The Live feeds 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.

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

This section includes the following topics:

- "Camera" on page 237
- "Information" on page 237

### Camera

Displays the different cameras available.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Camera</strong></td>
<td>Select the camera type from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• None. Default state. After you have finished viewing the live feeds, you</td>
</tr>
<tr>
<td></td>
<td>should set this back to None in order to conserve CPU power.</td>
</tr>
<tr>
<td></td>
<td>• Context camera. Displays the camera's normal video images.</td>
</tr>
<tr>
<td></td>
<td>• Tire camera. Displays the tire camera images (if applicable).</td>
</tr>
<tr>
<td></td>
<td>• LPR camera. Displays the LPR camera that captures license plates.</td>
</tr>
<tr>
<td></td>
<td>Click the screen to define a region of interest. Each click creates a corner</td>
</tr>
<tr>
<td></td>
<td>of the region of interest.</td>
</tr>
</tbody>
</table>

![Refresh button](image)

Click this button to refresh the live feed.

**Clear region of interest**

If you’ve created a region of interest, click this to delete it.

### Information

Provides information about the live feed.
NOTE  You can select the text in any of the text boxes and press Ctrl+C on your keyboard to copy the information to your clipboard.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>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.</td>
</tr>
<tr>
<td>Best read</td>
<td>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.</td>
</tr>
<tr>
<td>Plate state</td>
<td>Displays the plate state or province if the Sharp was able to read it from the license plate. You must enable this feature in &quot;Analytics&quot; on page 233.</td>
</tr>
<tr>
<td>FPS</td>
<td>Displays the current and average frames per second of the Sharp camera.</td>
</tr>
<tr>
<td>Exposure</td>
<td>Displays the exposure value of the lens.</td>
</tr>
<tr>
<td>Total number of best reads</td>
<td>Displays the number of best reads that have been taken with the Sharp since the Plate Reader service was started.</td>
</tr>
</tbody>
</table>
The Diagnostics page is where you run reports and generate logs about the status of the Sharp unit. You can export this data to a CSV file from the Actions section on the Status page. For more information, see "Actions" on page 227.

**IMPORTANT** This document/section was not complete at the time of publication. We are constantly updating our guides as new information becomes available. Click here for the most recent version of this document.

This section includes the following topics:

- "Search fields" on page 239
- "Sources to log" on page 239
- "Search criteria" on page 240

### Search fields

These are the fields in the search area.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time the event occurred.</td>
</tr>
<tr>
<td>Severity</td>
<td>Displays the severity of the event. You can choose which severity types to display in your &quot;Search criteria&quot; on page 240.</td>
</tr>
<tr>
<td>Source</td>
<td>The service that generated the error or message.</td>
</tr>
<tr>
<td>Message</td>
<td>Detailed message about the error and/or event.</td>
</tr>
<tr>
<td>Exception</td>
<td>Displays the software exception that generated the log entry. The exception gives extra information on where in the code the error occurred.</td>
</tr>
</tbody>
</table>

### 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 (e.g. you can search for events related to information, warnings, errors, and performance, or for all these events).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Select which severity settings to include in the search:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>Filters query on the source of the log. Only logs containing this string will be shown.</td>
</tr>
<tr>
<td>Message</td>
<td>Filter query on the message. Only logs containing this string will be shown.</td>
</tr>
<tr>
<td>From/To</td>
<td>Select a date-and-time range for events.</td>
</tr>
<tr>
<td>Distinct entries only</td>
<td>Logs with identical messages will be displayed only once.</td>
</tr>
</tbody>
</table>
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" on page 242
- "LED status on the SharpX camera unit" on page 245
LED status on the LPR Processing Unit

This section includes the following topics:

- "System status" on page 242
- "Camera data-link status" on page 243

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.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
<th>PWR</th>
<th>STAT 1</th>
<th>STAT 2</th>
<th>FAULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Unit powered off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Reflash</td>
<td>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.</td>
<td>On</td>
<td>On</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>POST</td>
<td>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.</td>
<td>See description</td>
<td>See description</td>
<td>See description</td>
<td>See description</td>
</tr>
<tr>
<td>Get DHCP</td>
<td>The unit is waiting for a DHCP lease over the network (it is configured in &quot;external DHCP mode&quot;).</td>
<td>On</td>
<td>5 quick flashes then pause, every 3 seconds</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Thermal Shutdown</td>
<td>The internal temperature is outside the operational limits. Power is no longer supplied to most components. No Ethernet network connectivity is possible.</td>
<td>Toggles once per second</td>
<td>Off</td>
<td>Off</td>
<td>Toggles once per second</td>
</tr>
<tr>
<td>Power Fault</td>
<td>A fault was detected on the main power source.</td>
<td>Toggles once per second</td>
<td>Off</td>
<td>Off</td>
<td>On</td>
</tr>
</tbody>
</table>
Camera data-link status

The following table describes how the Data-Link LEDs behave in response to the SharpX system's status.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
<th>Data (amber)</th>
<th>Link (green)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data idle</td>
<td>No Ethernet data is being received/transmitted between the camera and the trunk unit.</td>
<td>Off</td>
<td>N/A</td>
</tr>
<tr>
<td>Data transmit</td>
<td>Ethernet data is being received/transmitted between the camera and the trunk unit.</td>
<td>Blink</td>
<td>N/A</td>
</tr>
<tr>
<td>Not registered</td>
<td>The camera is not registered with the trunk unit yet. It may take up to 30 seconds for a camera to be registered.</td>
<td>N/A</td>
<td>Off</td>
</tr>
</tbody>
</table>
LED status on the LPR Processing Unit

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
<th>Data (amber)</th>
<th>Link (green)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered</td>
<td>The camera is registered with the trunk unit, and can exchange control messages with the LPR engine.</td>
<td>N/A</td>
<td>On</td>
</tr>
</tbody>
</table>
The following table describes how the SharpX camera unit’s LED behaves in response to the SharpX system’s status.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
<th>LED (red/green)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Unit is powered off</td>
<td>Off</td>
</tr>
<tr>
<td>Reflash</td>
<td>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.</td>
<td>Green (steady)</td>
</tr>
<tr>
<td>Get DHCP</td>
<td>The unit is waiting for a DHCP lease over the network (either from the LPR Processing Unit or an external server, depending on configuration).</td>
<td>Blinks green rapidly (e.g. twice per second).</td>
</tr>
<tr>
<td>Normal</td>
<td>The camera is running normally.</td>
<td>Flashes green briefly every second.</td>
</tr>
<tr>
<td>Covert</td>
<td>The camera is configured in covert mode. It will still blink green a couple of times at power-up.</td>
<td>Off</td>
</tr>
<tr>
<td>Thermal</td>
<td>The internal temperature is outside the operational limits. Power is no longer supplied to most components. No Ethernet network connectivity is possible.</td>
<td>Toggles slowly every second.</td>
</tr>
<tr>
<td>Thermal Shutdown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Illuminator Fault</td>
<td>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.</td>
<td>Blinks red rapidly (e.g. twice per second).</td>
</tr>
<tr>
<td>Firmware Fault</td>
<td>A critical fault was detected in the control board microcontroller.</td>
<td>Red (steady)</td>
</tr>
</tbody>
</table>
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" on page 247
- "AutoVu SharpX parts" on page 250
AutoVu Sharp parts

This section includes the following topics:

- "Fixed AutoVu Sharp parts list" on page 247
- "Mobile AutoVu Sharp parts list" on page 247
- "Understanding the Sharp part number" on page 249

Fixed AutoVu Sharp parts list

These are the parts included with a fixed AutoVu system.

<table>
<thead>
<tr>
<th>Part number</th>
<th>Part name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU-S-XXX-XXXXXX(^a)</td>
<td>Sharp camera</td>
</tr>
<tr>
<td>AU-H-PWRACINT</td>
<td>Power supply (optional)(^b)</td>
</tr>
<tr>
<td>AU-H-FIXCBLXXPE(^c)</td>
<td>Sharp fixed cable</td>
</tr>
</tbody>
</table>

\(^a\) For more information on your Sharp part number, see "Understanding the Sharp part number" on page 249.
\(^b\) 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.

<table>
<thead>
<tr>
<th>Part number</th>
<th>Part name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU-S-XGA-XXXXXX</td>
<td>Sharp camera</td>
</tr>
<tr>
<td>AU-H-MAGMNT</td>
<td>Sharp magnetic mount (optional)</td>
</tr>
<tr>
<td>AU-H-SBCBL05</td>
<td>Sharp cable to breakout box</td>
</tr>
<tr>
<td>AU-H-BOBUNIT</td>
<td>Breakout box</td>
</tr>
<tr>
<td>AU-H-BATCBL</td>
<td>Breakout box power cable to battery</td>
</tr>
<tr>
<td>AU-H-ILFUSE15A</td>
<td>Power cable in-line fuse</td>
</tr>
<tr>
<td>AU-H-CIGCBL</td>
<td>Cigarette lighter power cable (optional)</td>
</tr>
<tr>
<td>AU-H-ETHCBL14</td>
<td>Ethernet cable</td>
</tr>
<tr>
<td>Part number</td>
<td>Part name</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>AU-H-SHPHMBOT</td>
<td>Hardmount bottom component (optional)</td>
</tr>
<tr>
<td>AU-H-SHPHMTOP</td>
<td>Hardmount top component (optional)</td>
</tr>
<tr>
<td>AU-H-NAVBOX</td>
<td>Navigator unit (optional)</td>
</tr>
<tr>
<td>AU-H-USBCBL15</td>
<td>Type A to type B USB cable (optional)</td>
</tr>
<tr>
<td>AU-H-PCASE1510</td>
<td>Pelican case (optional)</td>
</tr>
<tr>
<td>AU-H-GPSANT</td>
<td>GPS antenna (optional)</td>
</tr>
<tr>
<td>AU-H-UWDSEAL</td>
<td>Universal window seal (optional)</td>
</tr>
<tr>
<td>AU-H-VID4T9L6</td>
<td>Tire camera (optional)</td>
</tr>
<tr>
<td>AU-H-VIDTICBL</td>
<td>Tire camera cable to breakout box (optional)</td>
</tr>
<tr>
<td>N/A</td>
<td>Ruggedized touchscreen PC</td>
</tr>
</tbody>
</table>
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.

Sample Sharp part number.

```
AU-S-XGA-W 12 850-P B G
```

- **Sharp 2.0 type**
  - XGA
  - VGA

- **Body color**
  - W = White body (standard)
  - B = Black body

- **LPR lens**
  - 12 = 12mm lens
  - 16 = 16mm lens
  - 25 = 25mm lens
  - 35 = 35mm lens
  - 50 = 50mm lens

- **Illuminator**
  - 590 = 590nm
  - 780 = 780nm
  - 850 = 850nm

- **Mount type**
  - P = Pelco
  - T = Pan/tilt (standard)
  - X = None

- **Mounting position**
  - T = Top
  - B = Bottom (standard)

- **Option**
  - G = GPS (Sharp XGA only)

**NOTE:** A top mounting position means that the pan/tilt mount is installed on top of the Sharp, so you can install the Sharp under a bridge, gantry, or similar object.
AutoVu SharpX parts

This section includes the following topics:

- "AutoVu SharpX parts list" on page 250
- "Understanding the SharpX part number" on page 251

AutoVu SharpX parts list

These are the parts included with a mobile AutoVu system using a SharpX system.

<table>
<thead>
<tr>
<th>Part number</th>
<th>Part name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU-X-XXX-XXXXX&lt;sup&gt;a&lt;/sup&gt;</td>
<td>SharpX camera unit</td>
</tr>
<tr>
<td>AU-H-XTU-X1</td>
<td>SharpX system LPR Processing Unit. One processor supporting one camera.</td>
</tr>
<tr>
<td>AU-H-XTU-X2</td>
<td>SharpX system LPR Processing Unit. Two processors supporting two cameras.</td>
</tr>
<tr>
<td>AU-H-XTU-X2M</td>
<td>SharpX - Multi system LPR Processing Unit. One multi-thread processor supporting two cameras.</td>
</tr>
<tr>
<td>AU-H-XTU-X4M</td>
<td>SharpX - Multi system LPR Processing Unit. Two multi-thread processors supporting four cameras.</td>
</tr>
<tr>
<td>AU-H-XCBL05</td>
<td>SharpX to Processing Unit Cable (5 m)</td>
</tr>
<tr>
<td>AU-H-XTU-MNT1V or AU-H-XTU-MNT1H&lt;sup&gt;b&lt;/sup&gt;</td>
<td>SharpX LPR Processing Unit standard mounting bracket.</td>
</tr>
<tr>
<td>N/A</td>
<td>Ruggedized touchscreen PC</td>
</tr>
<tr>
<td>(Optional) AU-H-XMNT-CAMU</td>
<td>SharpX camera portable mounting bracket - Pan Tilt Universal</td>
</tr>
<tr>
<td>(Optional) AU-H-XMNT-CAMH</td>
<td>SharpX camera hardmount mounting bracket - Pan Tilt</td>
</tr>
<tr>
<td>(Optional) AU-H-XMNT-CAMLB</td>
<td>SharpX light bar bracket (light bar make and model required)</td>
</tr>
<tr>
<td>(Optional) AU-H-XVISOR</td>
<td>SharpX Camera Visor</td>
</tr>
</tbody>
</table>
a. For more information on your SharpX part number, see "Understanding the SharpX part number" on page 251.
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.

Sample SharpX part number.

- AU-X-XGA-W 12 850

- **SharpX type**
  - XGA
  - VGA

- **Body color**
  - W = White body (standard)
  - B = Black body

- **LPR lens**
  - 12 = 12mm lens
  - 16 = 16mm lens
  - 25 = 25mm lens
  - 35 = 35mm lens
  - 50 = 50mm lens

- **Illuminator**
  - 590 = 590nm
  - 780 = 780nm
  - 850 = 850nm
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 control health history
Type of maintenance task that reports on access control unit malfunction events.

See also Health history.

access control unit
Type of entity that represents an access control panel that can communicate over an IP network.

See also Access Manager and Synergis Master Controller.

Access control unit configuration
Type of Security Desk task that reports on access control unit properties (firmware, IP address, time zone, and so on).

Access control unit events
Type of Security Desk task that reports on events pertaining to selected access control units.

Access Manager
Type of role that manages and monitors access control units on the system.

access point
Any monitored point that can be used to enter or exit a secured area, usually a door side or an elevator floor. Note that an elevator floor can only be used as an entry point.

access rule
Type of entity that defines the access control logic which grants or denies passage to a cardholder through an access point, based on a schedule.

Access rule configuration
Type of Security Desk task that reports on entities and access points affected by a given access rule.
Access troubleshooter  
Tool that helps you detect and diagnose access configuration problems. It allows you to find out about the following:
• Who are allowed to use an access point at a given time
• Which access points a cardholder is allowed to use at a given time
• Why a given cardholder can or cannot use an access point at a given time.

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.
(2) The right a cardholder has to pass through an access point at a given date and time.

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 Security Desk 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.

Advanced Systems Format
Advanced Systems Format or ASF (formerly Advanced Streaming Format) is a Microsoft streaming format associated with Windows Media Player.

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  Security Desk 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.

alarm panel  Another name for intrusion panel.

See also intrusion panel.

Alarm report  Type of Security Desk task that allows you to search and view current and past alarms.

antipassback  Access restriction placed on a secured area that prevents a cardholder from entering an area that they have not yet exited from, and vice-versa.

Archive storage details  Type of Security Desk task that reports on the video files (file name, start and end time, file size, protection status, and so on) used to store video archive, and which allows you to change the protection status of those files, among other things.

Archiver  Type of role that is responsible for the discovery, status polling, and control of video units. The Archiver also manages the video archive, and performs motion detection when it is not done on the unit itself.

See also Auxiliary Archiver, and video unit.

Archiver events  Type of Security Desk task that reports on events pertaining to selected Archiver roles.

Archives  Type of Security Desk task that allows you to find and view available video archives by camera and time range.

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.

When Synergis is enabled, the area entity can also be used to configure a secured area with access rules and access control behavior.

See also antipassback and interlock.
**Area activities**  
Type of Security Desk task that investigates area related activities (access granted, access denied, first person in, last person out, antipassback violation, and so on).

**Area presence**  
Type of Security Desk task that provides a snapshot of all cardholders and visitors currently present in a selected area.

**ASF**  
See Advanced Systems Format.

**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.

**asynchronous video**  
Simultaneous playback video from more than one camera that are not synchronized in time.

**audio decoder**  
Device or software that decodes compressed audio streams for playback.  
Synonym of "speaker".

**audio encoder**  
Device or software that encodes audio streams using a compression algorithm.  
Synonym of "microphone".

**Audit trails**  
Type of Security Desk task that reports on the configuration changes and 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.

### Auxiliary Archiver

Type of role that supplements the video archive produced by the Archiver. Unlike the latter, the Auxiliary Archiver is not bound to any particular discovery port. Therefore, it is free to archive any camera in the system, including the federated ones. The Auxiliary Archiver depends on the Archiver to communicate with the video units. It cannot operate on its own.

*See also* Archiver and discovery port.

### B

#### Badge designer

Tool that allows you to design and modify badge templates.

#### Badge printer

Tool that allows you to print badges in bulk, based on a badge template and a list of cardholders or credentials.

#### badge template

Entity type used to configure a printing template for badges.

#### bit rate

Data transfer rate expressed in kilobits per second (Kbps).

#### 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.

#### bookmark

Short text used to mark a specific position in a recorded video sequence that can be used to search for that video sequence at a later stage.

#### Bookmarks

Type of Security Desk task that searches for bookmarks related to selected cameras within a specified time range.

#### 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.
| **camera** | Type of entity that represents a single video source on the system. The video source can be an IP camera or an analog camera connected to the video encoder of a video unit. Multiple video streams can be generated from the same video source. |
| **Camera events** | Type of Security Desk task that reports on events pertaining to selected cameras within a specified time range. |
| **camera sequence** | Type of entity that defines a list of cameras that are displayed one after another in a rotating fashion within a single tile in Security Desk. |
| **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.* |
| **card and pin** | An access point mode that requires a cardholder to swipe their card and then enter a personal identification number (PIN). |
| **cardholder** | Type of entity that represents a person who can enter and exit secured areas by virtue of their credentials (typically access cards) and whose activities can be tracked. |
| **Cardholder access rights** | Type of Security Desk task that reports on which cardholders and cardholder groups are granted or denied access to selected areas, doors, and elevators. |
| **Cardholder activities** | Type of Security Desk task that investigates cardholder activities (access denied, first person in, last person out, antipassback violation, and so on). |
| **Cardholder configuration** | Type of Security Desk task that reports on cardholder properties (first name, last name, picture, status, custom properties, and so on). |
| **cardholder group** | Type of entity that configures the common access rights of a group of cardholders. |
| **Cardholder management** | Security Desk task that allows you to create, modify, and delete cardholders, as well as manage their credentials, including temporary replacement cards. |
| **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 permit and overtime rule.

City Parking Enforcement with Wheel Imaging  A "City Parking Enforcement" installation of a Patroller application that also includes wheel imaging. The use of maps (MapInfo only) and of the Navigator is mandatory.

See also City Parking Enforcement.

compatibility pack  See Omnicast compability 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.

costext 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.

controlled exit  Credentials are necessary to leave a secured area.

Controller Admin  Web-based administration tool hosted on every Synergis Master Controller unit, used to configure, administer, and upgrade the controller firmware.

See also Synergis Master Controller, controller module.

controller module  Processing component of Synergis Master Controller with IP capability, pre-loaded with the controller firmware and the web-based administration tool, Controller Admin.

See also Synergis Master Controller, Controller Admin, four-port RS-485 module.

Copy configuration tool  Tool that copies the configuration of one entity to many other entities.

covconert 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.

covconert hotlist  Hotlist hidden from the AutoVu Patroller users. Reads matching a covert hotlist generate covert hits.

credential  Type of entity that represents a proximity card, a biometrics template, or a PIN required to gain access to a secured area. A credential can only be assigned to one cardholder at a time.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential activities</td>
<td>Type of Security Desk task that investigates credential related activities (access denied due to expired, inactive, lost, or stolen credential, and so on).</td>
</tr>
<tr>
<td>credential code</td>
<td>A textual representation of the credential showing the credential data (typically the Facility code and the Card number). For credentials using custom card formats, the user can choose what to include in the credential code.</td>
</tr>
<tr>
<td>Credential configuration</td>
<td>Type of Security Desk task that reports on credential properties (status, assigned cardholder, card format, credential code, custom properties, and so on).</td>
</tr>
<tr>
<td>Credential enrollment</td>
<td>Security Desk task that allows you to enroll large numbers of card credentials into the system, either by scanning them at a designated card reader, or by entering a range of values.</td>
</tr>
<tr>
<td>custom event</td>
<td>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.</td>
</tr>
<tr>
<td>custom field</td>
<td>User defined property associated to an entity type to store additional information that is useful to your particular organization.</td>
</tr>
<tr>
<td>Daily usage per patroller</td>
<td>Type of Security Desk 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.</td>
</tr>
<tr>
<td>dashboard</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>See also widget.</td>
</tr>
<tr>
<td>database</td>
<td>Collection of data that is organized so that its contents can easily be accessed, managed, and updated.</td>
</tr>
<tr>
<td>database server</td>
<td>An application that manages databases and handles data requests made by client applications. Security Center uses Microsoft SQL Server as its database server.</td>
</tr>
<tr>
<td>debounce</td>
<td>The amount of time an input can be in a changed state (for example, from active to inactive) before the state change is reported. Electrical switches often cause temporarily unstable signals when changing states, possibly confusing the logical circuitry. Deboncing is used to filter out unstable signals by ignoring all state changes that are shorter than a certain period of time (in milliseconds).</td>
</tr>
</tbody>
</table>
dewarping  
Transformation used to straighten a digital image taken with a fish-eye lens.

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 server and main server, and expansion 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 high availability and Directory server.

Directory server  
Any one of the multiple servers simultaneously running the Directory role in a high availability configuration.

See also server, Directory, and high availability.

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.

door  
Type of entity that represents a physical barrier. Often, this is an actual door but it could also be a gate, a turnstile, or any other controllable barrier. Each door has two sides named by default “A” and “B”. Each side is an access point (entrance or exit) to a secured area.

Door activities  
Type of Security Desk task that investigates door related activities (access denied, door forced open, door open too long, hardware tamper, and so on).

door contact  
A door contact monitors the state of a door, whether it is open or closed. It can also be used to detect improper state (door open too long).

door controller  
See access control unit.
**door side**  
Every door has two sides, named by default "A" and "B". Each side is an access point to an area. For example, passing through side A leads into an area, and passing through side B leads out of that area. For the purposes of access management, the credentials necessary to pass through a door in one direction are not necessarily the same to pass through in the opposite direction.

**Door troubleshooter**  
Type of Security Desk task that lists all the cardholders who have access to a particular door side or elevator floor at a specific date and time.

**Driver Development kit**  
Driver Development Kit (DDK). An SDK for creating device drivers.

**duress**  
A special code used to disarm an alarm system that quietly alerts the monitoring station that the alarm system was disarmed under threat.

**E**

**edge recording**  
Video is recorded on the unit itself, eliminating the need to constantly stream video to a centralized server.

*See also* Archiver.

**electric door strike**  
An electric device that releases the door latch when current is applied.

**elevator**  
Type of entity that provides access control properties to elevators. For an elevator, each floor is considered an entry point for the area corresponding to that floor.

**Elevator activities**  
Type of Security Desk task that investigates elevator related activities (access denied, floor accessed, unit is offline, hardware tamper, and so on).

**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* server and main 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.

**four-port RS-485 module**

RS-485 communication component of Synergis Master Controller with four COM ports, each of which can handle up to eight interface modules.

*See also* Synergis Master Controller, controller module, interface module.

**frame**

A single video image.
free access  Access point state where no credentials are necessary to enter a secured area. The door is unlocked. This is typically used during normal business hours, as a temporary measure during maintenance, or when the access control system is first powered up and is yet to be configured.

free exit  Access point state where no credentials are necessary to leave a secured area. The person releases the door by turning the doorknob, or by pressing the REX button, and walks out. An automatic door closer shuts the door so it can be locked after being opened.

G64  G64 is the native data format used by all archiving roles (Archiver and Auxiliary Archiver) to store video files. This data format incorporates all information related to the video data, including audio, bookmarks, timestamps, motion and event markers, and supports watermarking.

See also ASF, video file, and video watermarking.

Genetec Plan Manager Server  Windows service that runs Plan Manager Server modules.

See also Plan Manager Server.

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.

g geocoder  AutoVu feature that translates a pair of longitude and latitude into a street address.

ghost camera  Entity used as a stand in camera that is automatically created by the Archiver when video archives are detected for a camera whose definition has been deleted from the Directory, either accidentally or because the physical device no longer exists. Ghost cameras cannot be configured. They only exist so users can reference the video archive that would otherwise not be associated to any camera.

See also camera.
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* OGC, WMS KML.

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 host, sharing guest.

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* partition, sharing guest, global entity.

**GUID**  
A globally unique identifier, or GUID, is a special type of identifier used in software applications to provide a unique reference number.

**H**  
**H.264**  
H.264/MPEG-4 AVC (Advanced Video Coding) is a standard for video compression.

**hardware zone**  
A subtype of zone entity where the IO linking is done by hardware. A hardware zone is controlled by a single access control unit and works only in mixed and offline mode. Hardware zones cannot be armed or disarmed from Security Desk.

*See also* zone and virtual zone.
Health history

Type of maintenance task that reports on health issues. See also "Health statistics", "Health Monitor".

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 rule, permit, and permit restriction.

Hits

Type of Security Desk task that investigates 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 Security Desk 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-frame  Synonym of intra-frame and key frame.

See also key frame.

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.

Import tool  Tool that allows you to import cardholders, cardholder groups, and credentials from a CSV (Comma Seperated Values) file.

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 Security Desk task that allows you to search, review, and modify incident reports.
interface module

An auxiliary board that communicates with Synergis Master Controller over IP or RS-485, and provides input and output connections to readers and other third-party security components.

See also Synergis Master Controller, four-port RS-485 module.

interlock

Access restriction placed on a secured area that permits only one door to be open at any given time. When one perimeter door is open, all other perimeter doors are locked.

intra-frame

Synonym of I-frame and key frame.

See also key frame.

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 Security Desk task that investigates 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 Security Desk task that investigates 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

Security Desk task that allows you to add and reconcile license plate reads to a parking facility inventory.

Inventory report

Type of Security Desk 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 configuration

Type of Security Desk task that reports on the IO configurations (controlled access points, doors, and elevators) of access control units.
## 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.*

## IP camera

A video unit incorporating a camera.

*See also video unit.*

## 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

### key frame

A key frame (or I-frame, or intra-frame) is a frame that contains a complete image by itself as opposed to a usual frame that only holds information that changed compared to the previous frame. It is used as reference in video image compression.

### 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 (MapInfo only) 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.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>license plate inventory</td>
<td>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.</td>
</tr>
<tr>
<td>license plate read</td>
<td>License plate number captured from a video image using LPR technology. See also License Plate Recognition and hit.</td>
</tr>
<tr>
<td>License Plate Recognition</td>
<td>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.</td>
</tr>
<tr>
<td>live hit</td>
<td>A hit matched by the Patroller and immediately sent to the Security Center over a wireless network.</td>
</tr>
<tr>
<td>live read</td>
<td>A license plate captured by the Patroller and immediately sent to the Security Center over a wireless network.</td>
</tr>
<tr>
<td>load balancing</td>
<td>Distribution of workload across multiple computers. See also high availability and failover.</td>
</tr>
<tr>
<td>logical ID</td>
<td>Unique IDs assigned to each entity in the system for ease of reference. Logical IDs are only unique within a particular entity type.</td>
</tr>
<tr>
<td>Logical view</td>
<td>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.</td>
</tr>
<tr>
<td>Logons per Patroller</td>
<td>Type of Security Desk task that reports on the logon records of a selected Patroller.</td>
</tr>
<tr>
<td>long term</td>
<td>Type of parking regulation characterizing an overtime rule. The &quot;long term&quot; regulation uses the same principle as the &quot;same position&quot; 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.</td>
</tr>
<tr>
<td>LPR</td>
<td>See License Plate Recognition.</td>
</tr>
<tr>
<td>LPR camera</td>
<td>A camera connected to an LPR unit that produces high resolution close-up images of license plates. See also context camera and SharpX.</td>
</tr>
</tbody>
</table>
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 License Plate Recognition, Sharp unit, AutoVu LPR Processing Unit, and LPR Manager.

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 server, expansion server, and Directory 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

Type of entity that represents either a Web page or an interactive diagram (a compiled .Net map).

Map Data Server

Plan Manager server module that manages the Plan Manager database. It must run on the Plan Manager’s main server.

See also Plan Manager Server.

Map Generator

Plan Manager server module that imports raster and vector maps to Plan Manager database.

See also Plan Manager configuration.
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 that can appear on a map, such as a camera, a door, an intrusion panel, or a colored polygon. A map object can display status information or you can click on it to perform additional actions, such as view a video feed from a camera, zoom in on an area of interest, unlock a door and so on.

See also hotspot, map link, and Plan Manager Client.

Map Tile Server

Plan Manager server module that sends map files to Security Desk.

See also Plan Manager Client and Plan Manager Server.

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”.

Media Router

The central role that handles all stream (audio and video) requests in Security Center. It establishes streaming sessions between the stream source (camera or Archiver) and its requesters (client applications). Routing decisions are based on the location (IP address) and the transmission capabilities of all parties involved (source, destinations, networks, and servers).

metadata

Metadata is data about data. Any data that describes or enriches the raw data.

Migration tool

Tool used to migrate Omnicast 4.x systems to Security Center 5. This tool must be executed on every server computer where Omnicast 4.x components are installed.

mixed mode

Access control unit operation mode where all access control decisions are made by the unit locally based on information downloaded from the Access Manager during unit synchronization. Access events are reported to the Access Manager in real-time.

See also offline mode, online mode.

M-JPEG

Motion JPEG (M-JPEG) is an informal name for a class of video formats where each video frame of a digital video sequence is separately compressed as a JPEG image.

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, 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, Web Client.* |
| **monitor ID** | ID used to uniquely identify a workstation screen controlled by Security Desk. |
| **Monitoring** | Type of Security Desk task that allows you to monitor and respond to real time events pertaining to selected entities of interest. |
| **motion detection** | The software component that watches for changes in a series of video images. The definition of what constitutes motion in a video can be based on highly sophisticated criteria. |
| **Motion search** | Type of Security Desk task that searches for motion detected in specific areas of a camera’s field of view. |
| **motion zone** | User defined areas within a video image where motion should be detected. |
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.

MPEG-4

A patented collection of methods defining compression of audio and visual (AV) digital data.

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 geocoding to vehicles and reads.

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.

OCR equivalence

The prediction of possible characters for inexact reading by Optical Character Recognition (OCR) technology.

offline mode

Access control unit operation mode when the communication with the Access Manager has been lost. The unit makes access control decisions locally, based on information downloaded from the Access Manager during unit synchronization. Access events are logged in the unit and are uploaded to the Access Manager when the network connection is re-established.

See also mixed mode and online mode.

OGC

Open Geospatial 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. |
| **online mode** | Access control unit operation mode where the unit is under the direct real-time control of the Access Manager. The Access Manager makes all access control decisions. This mode is not available with HID VertX and Edge units. |

See also **mixed mode** and **offline mode**.

| **Optical Character Recognition** | Optical Character Recognition (OCR) is the technology used to translate the characters found in images into machine editable text. |
| **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 **parking zone** and **hit rule**.

| **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 Manager, and LPR camera.

**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.

**People counting**

Security Desk task that keeps count in real time of the number of cardholders in all secured areas of your system.

**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 permit, permit hit, and parking zone.*

**Plan Manager**  
Security Center feature that lets you create and integrate interactive maps into your system, for access control, video streaming and intrusion detection. It uses digital maps to represent the physical locations of monitored inputs such as cameras, doors, areas and zones.

**Plan Manager Client**  
Plan Manager client component that runs as an add-on to 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 Tile Server and map object.*

**Plan Manager configuration**  
Administrative task used to set up Plan Manager Server and configure the map hierarchy.

*See also Plan Manager Server.*

**Plan Manager Server**  
Plan Manager server component that includes three modules: Map Data Server, Map Generator, and Map Tile Server.

*See also Map Data Server, Map Generator, Map Tile Server, and Plan Manager configuration.*
**PlateReaderServer**

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 PlateReaderServer also handles the communications with the Patroller and the LPR Manager. If an external wheel imaging camera is connected to the Sharp unit, the PlateReaderServer also captures wheel images from this camera.

*See also* Sharp unit, Patroller, and LPR Manager.

**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.

**Portable Archive Player**

Self-contained video player that can play exported Security Center video files on computers that do not have Security Center installed.

*See also* video file.

**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 task and public 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 task and private task.

Q

R

read  See license plate read.

reader  A sensor that reads the credential for an access control system. For example, this can be a card reader, or a biometrics scanner.

Reads  Type of Security Desk task that reports on license plate reads performed within a selected time range and geographic area.

Reads/hits per day  Type of Security Desk task that reports on license plate reads performed within a selected time range and geographic area.

Reads/hits per zone  Type of Security Desk task that reports on the number of reads and hits per day for a selected date range.

recording mode  The criteria by which the Archiver schedules the recording of video streams.

There are four possible recording modes:

- Off (no recording allowed)
- Manual (record only on user requests)
- Continuous (always record)
- On motion/manual (record according to motion detection settings or on user request).
**recording state**

Current recording status of a given camera. There are four possible recording states:

- Enabled
- Disabled
- Currently recording (unlocked)
- Currently recording (locked).

**redirector**

Server assigned to host a redirector agent created by the Media Router role.

**redirector agent**

Agent created by the Media Router role to redirect data streams from one IP endpoint to another.

**redundant archiving**

Option that allows a copy of all the video streams of an Archiver role to be archived simultaneously on the standby server as a protection against data loss.

**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.

**request to exit**

Request to exit (REX).

1. Door release button normally located on the inside of a secured area that when pressed, allows a person to exit the secured area without having to show any credential. This can also be the signal from a motion detector.

2. The signal received by the controller for a request to exit.

**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**

Entity used to configure the transmission capabilities between two end points in a network for the purpose of routing media streams.

**Route playback**

Type of Security Desk task that replays the route followed by a Patroller on a given date on a map.
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 primary server and failover.

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 Server, Mobile Admin, Mobile app, 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* Genetec Server, main server, and expansion 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 partition, Global Cardholder Synchronizer.

sharing host

Security Center system that owns partitions that are shared with other Security Center systems, called sharing guests.

*See also* global partition.

Sharp Admin

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 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 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* LPR camera, context camera, Sharp XGA, Sharp VGA, Sharp EX, SharpX, and PlateReaderServer.
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.

stream

stream.

(1) Video stream.

(2) Entity representing a specific video quality configuration on a camera.
| **strict antipassback** | Antipassback option. When enabled, a passback event is generated when a cardholder attempts to leave an area that they were never granted access to. When disabled, Security Center only generates passback events for cardholders entering an area that they never exited.  
*See also* timed antipassback. |
| **synchronous video** | Simultaneous live video or playback video from more than one camera that are synchronized in time. |
| **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. |
| **Synergis Master Controller** | Genetec’s access control unit that supports a variety of third party readers and interface modules over IP and RS-485. The controller is seamlessly integrated to Security Center, and retains its full decision-making capabilities even in offline mode (disconnected from the Access Manager).  
*See also* access control unit, controller module, four-port RS-485 module. |
| **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 Security Desk task that monitors the status of all entities of a given type in real time, and allows you to interact with them. |
| **T** | |
| **tailgating** | A person who enters a secure area without swiping a credential, by following behind another person who has swiped their credential. |
| **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, selector, and report pane.

**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.

**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.

**Time and attendance**  
Type of Security Desk task that reports on who has been inside a selected area and the total duration of their stay within a given time range.

**timed antipassback**  
Antipassback option. When Security Center considers a cardholder to be already in an area, a passback event is generated when the cardholder attempts to access the same area again during the time delay defined by Timeout. When the time delay has expired, the cardholder can once again pass into the area without generating a passback event.

*See also* strict antipassback.

**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, video unit, LPR unit, Access Manager, Archiver, LPR Manager, and Intrusion Manager.

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 (MapInfo only) 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 user group and Active Directory.

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 a user to help determine who should be given priority when two users are trying to access the same resource, such as a camera PTZ. The smaller the value, the higher the priority.

See also 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 user, user group, access right, and partition.

validation key

Serial number uniquely identifying a computer that must be provided to obtain the license key.

See also license key.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>vehicle identification number</td>
<td>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.</td>
</tr>
<tr>
<td>video analytics</td>
<td>The software technology that is used to analyze video for specific information about its content. Examples of video analytics include counting the number of people going through a door, license plate recognition, detection of unattended objects, or the direction of people walking or running.</td>
</tr>
<tr>
<td>video archive</td>
<td>Video archive includes both the recorded audio/video footage and the database that documents those recordings (source camera, timestamps, events, bookmarks, and so on).</td>
</tr>
<tr>
<td>video encoder</td>
<td>Device that converts an analog video source to a digital format using a standard compression algorithm (H.264, MPEG-4, MPEG-2 or M-JPEG). The video encoder is one of the many devices found on a video unit.</td>
</tr>
<tr>
<td>video file</td>
<td>File created by an archiving role (Archiver or Auxiliary Archiver) to store archived video. The file extension is G64. You need the Security Desk or the Portable Archive Player to read video files.</td>
</tr>
<tr>
<td>Video file player</td>
<td>Type of Security Desk task that browses through your file system for video files (G64) and allows you to play, convert to ASF, and verify the authenticity of these files.</td>
</tr>
<tr>
<td>video sequence</td>
<td>Any recorded video stream of a certain duration.</td>
</tr>
<tr>
<td>video unit</td>
<td>Type of entity that represents a video encoding device capable of communicating over an IP network and incorporating one or more video encoders. They come in a wide variety of brands and models. Some support audio, others support wireless communication. The high end models come with their own recording and video analytics capabilities.</td>
</tr>
<tr>
<td>video watermarking</td>
<td>Process by which a digital signature (watermark) is added to each recorded video frame to ensure its authenticity. If anyone later tries to make changes to the video (add, delete or modify a frame), the signatures will no longer match, thus, showing that the video has been tampered with.</td>
</tr>
</tbody>
</table>
**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* zone, hardware zone.

**Visit details**  
Type of Security Desk task that investigates the stay (check-in and check-out time) of current and past visitors.

**Visitor activities**  
Type of Security Desk task that investigates visitor activities (access denied, first person in, last person out, antipassback violation, and so on).

**Visitor management**  
Security Desk task that allows you to check in, check out, and modify visitors, as well as manage their credentials, including temporary replacement cards.

**visual tracking**  
Visual tracking is a feature in Security Desk that allows you to follow an individual across different areas of your company without ever losing sight of that individual, as long as the places this person goes through are monitored by cameras. This feature displays transparent overlays on the video to show you where you can click to switch to adjacent cameras.

**VSIP port**  
The VSIP port is the name given to the discovery port of Verint units. A given Archiver can be configured to listen to multiple VSIP ports.

*See also* discovery port.

**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.
<table>
<thead>
<tr>
<th><strong>Wiegand</strong></th>
<th>An electrical interface standard and format used between a reader and controller (from the original Wiegand card reader).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows Communication Foundation</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>WMS</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>See also GIS and OGC.</td>
</tr>
<tr>
<td><strong>X</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Y</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Z</strong></td>
<td></td>
</tr>
<tr>
<td><strong>zone</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>See also IO linking, hardware zone, and virtual zone.</td>
</tr>
<tr>
<td><strong>Zone activities</strong></td>
<td>Type of Security Desk task that investigates zone related activities (zone armed, zone disarmed, lock released, lock secured, and so on).</td>
</tr>
<tr>
<td><strong>Zone Manager</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Zone occupancy</strong></td>
<td>Type of Security Desk task that reports on the number of vehicles parked in a selected parking zone, and the percentage of occupancy (for university parking only).</td>
</tr>
<tr>
<td></td>
<td>See also University Parking Enforcement.</td>
</tr>
</tbody>
</table>
Index

A

about
  AutoVu, 2
  AutoVu Sharp, 4
  AutoVu SharpX, 4
  Patroller, 7
  Patroller Config Tool, 7
  Security Center, 6
  Sharp Portal, 7
activating
  user profiles, 173
active tasks, list, 177
archive viewing, user limitations, 175, 181
AutoVu
  about, 2
AutoVu hardware
  mobile installation examples, 78
  mobile installation guidelines, 84
  mobile installation procedure, 85
AutoVu SettingsViewer
  see Sharp Portal, 224
AutoVu Sharp
  about, 4
  installing hardware, 66
    parts list, 247
    restart, 17
AutoVu SharpX
  about, 4
  installing hardware, 77
    parts list, 250
    restart, 17

C

changing
  user password, 173
close
  Patroller Config Tool, 13
concurrent logons, limiting, 174
Configscope
  see analytics, 233
configuring
  full screen mode, 178
  hotlists, 37, 51
  LPR Manager for fixed AutoVu system, 27
  LPR Manager for mobile AutoVu system, 45
  Security Center/Patroller communication, 188
  user password expiration, 174
ConnectToGateway
  see connect to Security Center, 207
contacting technical support, iv

d
deactivating
  user profiles, 173
demo license, acquring, iv
deploying
  fixed AutoVu system, 22
  mobile AutoVu system, 40
document information, ii
documentation
  See production documentation

E

enabling task cycling, 177

F

fixed AutoVu deployment
  about, 23
  hardware installation overview, 24
  hotlists, 37
    adding, 37
    configuring advanced properties, 38
configuring basic properties, 37
hit notification options, 38
LPR Manager
configuration overview, 27
configuring database, server, retention periods, 28
configuring LPR units, 34
configuring root folder, 29
configuring Sharp updates, 33
connecting to fixed Sharps, 29
creating, 27
discovery port, setting, 31
hotlist, activating, 30
hotlist, email notification, 30
hotlist, filtering, 31
hotlist, matching, 32
linking camera to LPR unit, 35
sending images to, 32
setting Sharp time zone, 33
prerequisites for deploying, 23
Sharp configuration overview, 26
Sharp upgrade overview, 25
software installation overview, 25
full screen mode
configuring as default, 178

G
géocoding, about, 192
GPS driver, installing, 146
Guidelines
mobile AutoVu installation, 84

H
Hardmount
installation, 85
hardware
fixed installation, 66
installation prerequisites, 63
mobile installation, 77
safety precautions, 63
specifications and system requirements, 63
hotlists
adding, 37, 51
configuring advanced properties, 38, 52
configuring basic properties, 37, 52
hit notification options, 38, 52
managing large hotlists, 53

I
Illustrations
mag-mount AutoVu mobile installation, 93
mobile AutoVu installation (advanced), 80
mobile AutoVu installation (basic), 78
Installation procedures
mobile installation, 85
hardmount, 85
magnetic mount, 91
installing
fixed AutoVu hardware, 66
GPS driver, 146
mobile AutoVu hardware, 77
Patroller, 112
Security Center, 104
interface tour
Patroller Config Tool, 13
Security Center Config Tool, 10
Sharp Portal, 16

L
latitude and longitude, setting, 159
LED status
SharpX camera, 245
SharpX data-link, 243
SharpX LPR Processing Unit, 242
level, users, 175, 181
limiting
concurrent user logons, 174
log off
Security Center Config Tool, 11
Sharp Portal, 17
log on
Security Center Config Tool, 10
Sharp Portal, 16
supervised, 175, 182
user schedules, 174
LPR Manager
configuring
Security Center/ Patroller communication, 188
configuring database, server, retention periods, 28
configuring LPR units, 34
configuring root folder, 29
configuring Sharp updates, 33
connecting to fixed Sharps, 29
creating, 27
discovery port, setting, 31
enabling hotlist filtering, 195
geocoding, 192
hotlist, activating, 30
hotlist, filtering, 31
hotlist, matching, 32
importing data, 189
linking camera to LPR unit, 35
matching license plate reads, 192
moving units between, 151
providing Patroller updates, 195
sending images to, 32
setting Sharp time zone, 33
XML exporting, 193
XML importing, 195

M
Magnetic mount
installation, 91
maps
not working, 123
matching license plate reads, 192
mobile AutoVu deployment
about, 41
hardware installation overview, 42
hotlists, 51
adding, 51
configuring advanced properties, 52
configuring basic properties, 52
hit notification options, 52
modifying LPR matcher, 54
LPR Manager
configuration overview, 45
configuring database, server, retention periods, 46
configuring Patroller and SharpX updates, 48
configuring root folder, 47
connecting Patroller to Security Center, 48
creating, 45
hotlist, activating, 49
hotlist, configuring privacy, 50
hotlist, email notification, 48
hotlist, filtering, 49
setting Patroller user group, 47
Patroller, 56
adding Sharp cameras to, 58
configuring acknowledgement buffer, 56
configuring hit delay, 57
configuring hit options, 60
configuring navigation options, 60
configuring offload options, 59
configuring sound management, 56
configuring unit name and logon options, 59
connecting to Security Center, 58
customizing user interface, 61
prerequisites for deploying, 41
Sharp configuration overview, 44
Sharp upgrade overview, 43
software installation overview, 43
Mobile AutoVu installation
advanced example, 80
basic example, 78
guidelines, 84
procedure, 85
wiring information, 80
Move unit tool, using, 151

O
offload
configuring USB support for, 140–143
configuring, general, 59
FileTransfer.vbs, shortcut, 141
open
Patroller Config Tool, 13

P
password
changing, 173
expiration, 174
Patroller
about, 7
adding Sharp cameras to, 58
configuring acknowledgement buffer, 56
configuring hit delay, 57
configuring hit options, 60
configuring navigation options, 60
configuring offload options, 59
configuring sound management, 56
configuring unit name and logon options, 59
connecting Sharp units to, 137
connecting to Security Center, 58
customizing user interface, 61
downloading hotfixes, 113
installation overview, 111
installing, 112
installing MapInfo, 113
SQL Express requirements, 107
system requirements, 106
Patroller Config Tool
about, 7
close, 13
interface tour, 13
open, 13
restoring default settings, 15
using the interface, 14
Plate event accumulator
see connecting Sharp units, 137
Plate Reader Server
see Sharp Portal, 224
Power cable connections
mobile AutoVu installation, 80
prerequisites
for hardware installation, 63
prerequisites for mobile deployment, 23, 41
product documentation
about, iii
where to find, iii

R
remote user, controlling, 175
Restart
AutoVu Sharp, 17
AutoVu SharpX, 17

S
safety precautions, hardware, 63
schedule
user logon, 174
Security Center
about, 6
Security Center Config Tool
interface tour, 10
log off, 11
log on, 10
using the interface, 12
setting
user group privileges, 182
user levels, 175, 181
user privileges, 176
Sharp
hardware connections, 67
installation example, 67
wiring diagram, 68
Sharp Portal
about, 7
interface tour, 16
log off, 17
log on, 16
using the interface, 18
using with SharpX, 17
web browser requirements, 106
SharpX
camera LED status, 245
connecting to Patroller, 137
hardware connections, 95
LED status, 242
sound management, Patroller, 56
SQL Express requirements, 107
SQL server memory, increasing, 107
status, user profiles, 173
supervised log on, about, 175, 182
system requirements, Patroller, 106

T
task cycling, enabling, 177
technical support, contacting, iv
Typical installation
mobile, 78

U
upgrading
Patroller, 120
Patroller from Security Center, 115
reset mapping type, 123
Sharp units from Security Center, 115
USB support, for offload, 140–143
user
activating, 173
changing password, 173
controlling remote workstations, 175
deactivating, 173
enabling task cycling, 177
entering personal information, 173
limitations, archive viewing, 175, 181
limiting concurrent logons, 174
logon schedules, 174
password expiration, 174
setting level, 175, 181
setting privileges, 176
supervised log on, 175, 182
user group
 members, 180
 setting privileges, 182
user password
 changing, 173
 configuring expiration, 174
user privileges
 about, 176

V
viewing
 active task list, 177

W
warnings, 63
web browser requirements
 Sharp Portal, 106
What you need
 mobile installation, 85
which settings are transferred, 123
Wiring information
 mobile AutoVu installation, 80

X
XML
 exporting, 193
 importing, 195