Patroller Administrator Guide 6.3

Genetec

Copyright notice

Document information

Document title: Patroller Administrator Guide 6.3

Document number: EN.400.007-V6.3(2)

Document update date: November 18, 2016

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

About this guide

This guide provides you with a complete source of information about how to install and configure Patroller for License Plate Recognition (LPR). It explains the basic settings you must configure before your system can be used. Last-minute updates can be found in the *Patroller Release Notes*.

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

Notes and notices

The following notes and notices might appear in this guide:

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

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

Contents

Chapter 5: Patroller Config Tool Reference

Chapter 6: Patroller SimpleHost

1

Getting started

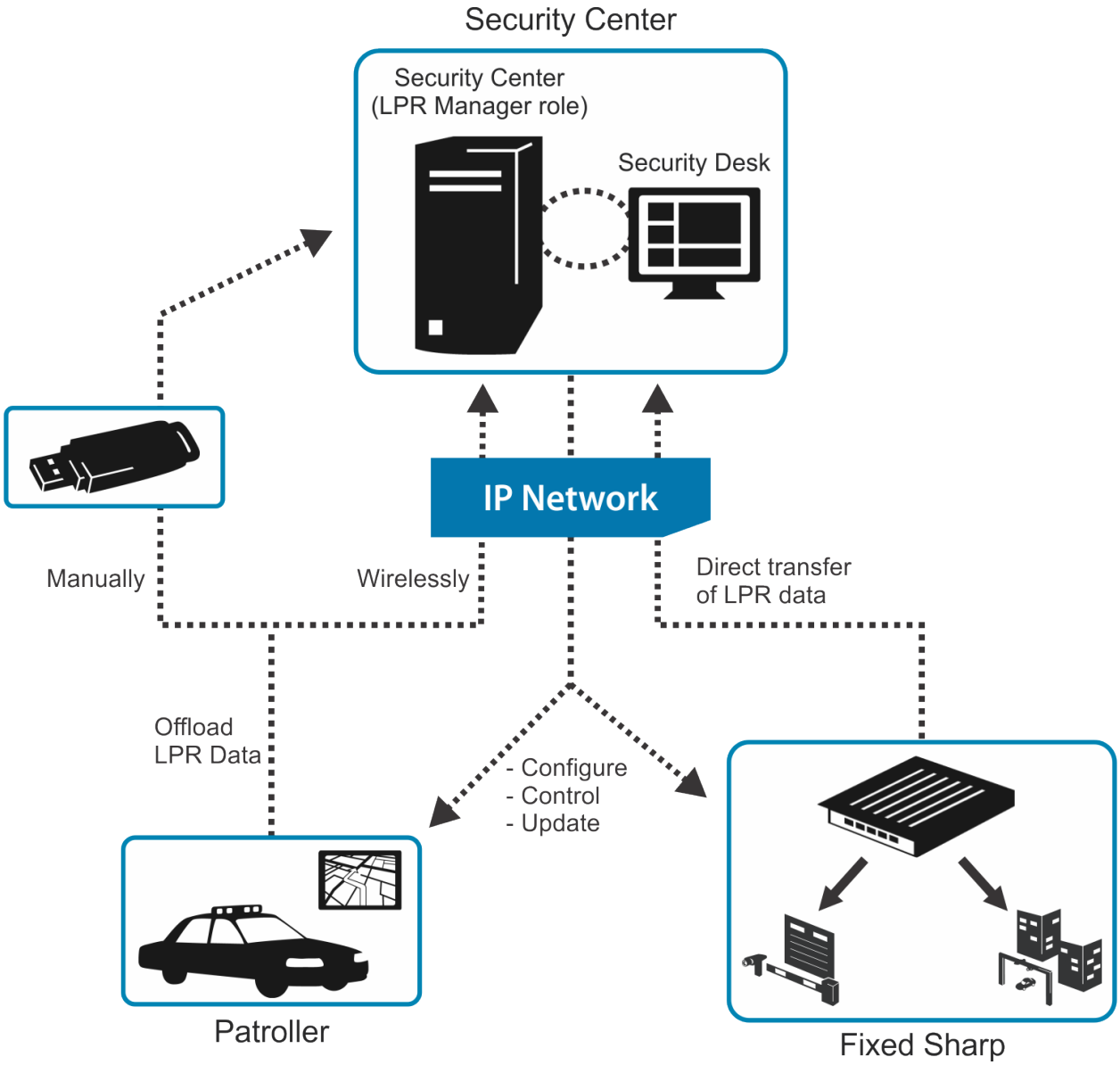
This section includes the following topics:

About 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:



Opening Patroller Config Tool

Patroller Config Tool is installed on your C drive with Patroller. It does not appear in your Windows Start menu. You must navigate to the proper folder on your computer.

To open Patroller Config Tool:

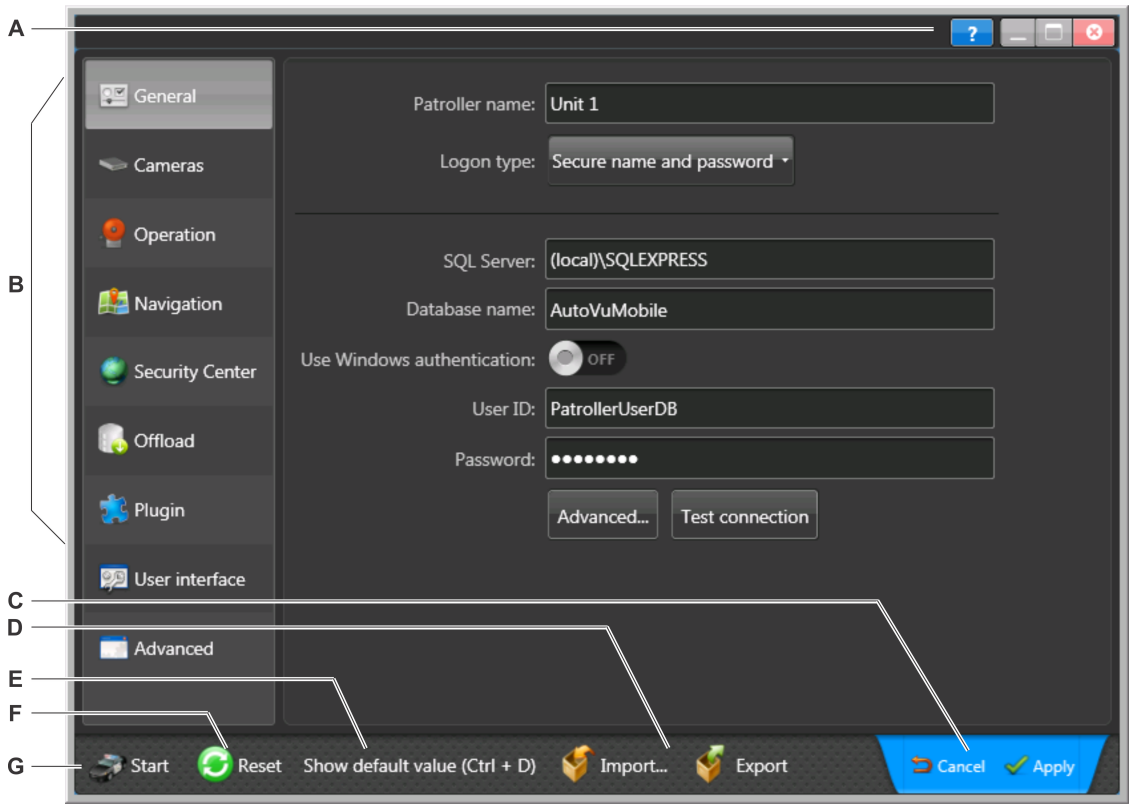
1 On the in-vehicle computer, navigate to *C:\Program Files\Genetec AutoVu x.y\MobileClient*.

2 Double-click *PatrollerConfigTool.exe*.

Patroller Config Tool opens.

Interface overview of the Patroller Config Tool

This section takes you on a tour of the main areas in the Patroller Config Tool user interface.



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

Related Topics

Restoring default settings in Patroller on page 5
Importing and exporting Patroller settings on page 6

Restoring default settings in Patroller

You can restore a default Patroller setting at any time.

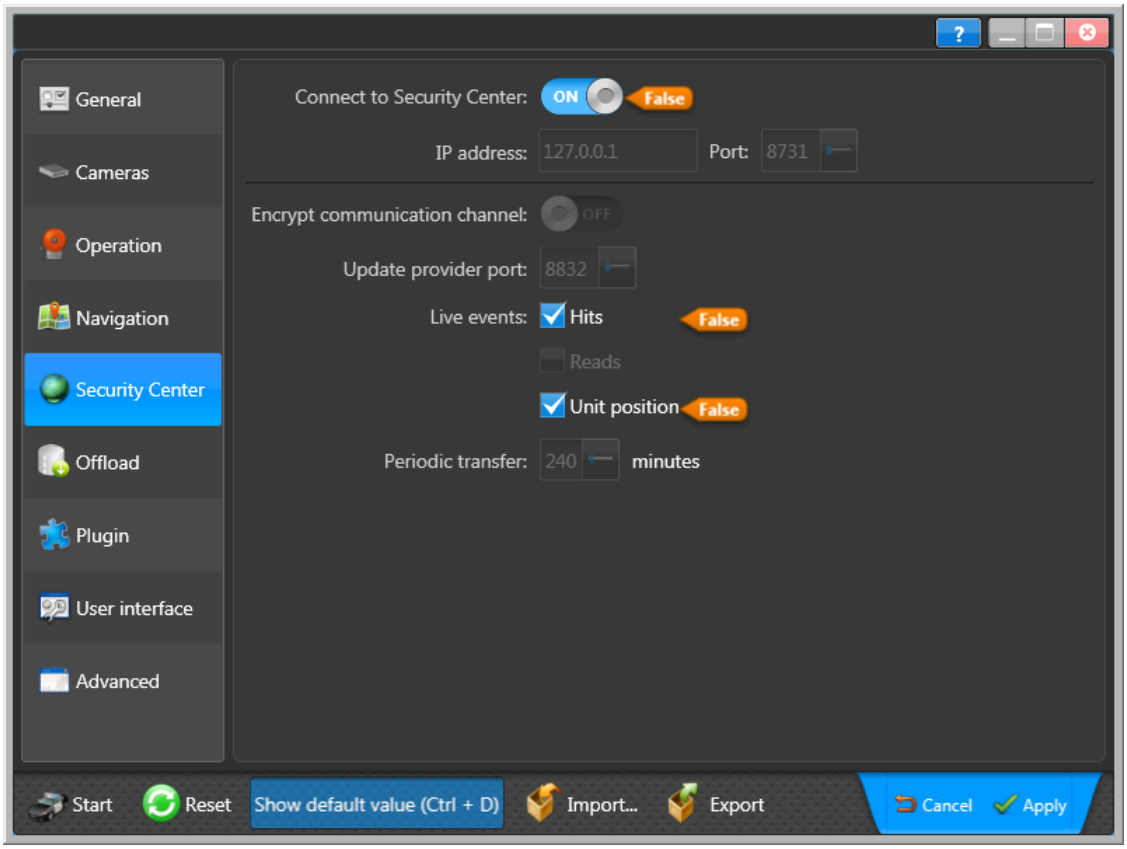
What you should know

The Default values appear as an orange tag next to the option. Click the orange tag to reset the option to the default value.

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.



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

3 Tap **Apply**.

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

Importing and exporting Patroller settings

You can import or export the configuration settings from one Patroller to another, simplifying the deployment of multiple Patroller vehicles.

What you should know

For example, if you have a fleet of Patroller vehicles, you can configure one and then export the settings to the others. You cannot import settings between different versions of Patroller. For example, you cannot import settings from a 5.2 version of Patroller to a 6.3 version of Patroller.

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

To export and import settings:

1 Open Patroller Config Tool on the Patroller computer that is ready to export settings.
2 Click **Export**.

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

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

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

4 Open Patroller Config Tool on the Patroller computer you want to configure.
5 Click **Import**.
6 Browse to the zip file with the Patroller settings you want to import.
7 Follow the on-screen instructions to proceed.

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

2

Installing Patroller

This section includes the following topics:

Preparing to install Patroller

Install AutoVu™ Patroller components in the following order:

Before you install Patroller:

1 Read the *Patroller Release Notes* for any known issues and other information about the release. The latest version of the release notes is available from the Technical Information Site.

2 Check the Patroller system requirements. For more information, see the *Patroller System Requirements*.

3 Check the SQL Express database requirements.

Patroller setup installs SQL Express 2014 which supports up to 10 GB (that is, approximately 160,000 reads) of data for hotlists, permit applications, and overtime applications with wheel imaging.

BEST PRACTICE: If you're upgrading Patroller, and you're still using SQL Express 2008 R2, you should let the Patroller setup program install SQL Express 2014.

4 (Windows 7 and later) Disable the Windows User Account Control security option.

NOTE: Not applicable to Patroller standalone.

5 (Windows 8) Enable Patroller clock synchronization with Security Center.

NOTE: Not applicable to Patroller standalone.

After you finish

Install Patroller.

Related Topics

Configuring SQL server memory in Patroller on page 9

Configuring SQL server memory in Patroller

Patroller Install Shield configures the memory correctly. For older systems, if you are using the Sharp with both context and wheel images in high-definition, then you'll need to configure the SQL server memory on the mobile data computer running the Patroller application.

Before you begin

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

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

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

To change the SQL server memory at the command prompt:

1 Depending on the version of SQL running, do one of the following:
   - For SQL 2005, type:
     ```
     cd C:\Program Files\Microsoft SQL Server\90\Tools\Binn
     ```
   - For SQL 2008, type:
     ```
     cd "C:\Program Files\Microsoft SQL Server\100\Tools\Binn"
     ```
2 Type the following:
   ```
   Sqlcmd -S (local)\<name of DB server, ex: sqlexpress2005>
   sp_configure 'show advanced options', 1
   RECONFIGURE WITH OVERRIDE
   GO
   sp_configure 'max server memory', 1024
   RECONFIGURE WITH OVERRIDE
   GO
   ```

Default Patroller ports

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

Computer	Inbound	Outbound	Port usage
Patroller in-vehicle computer	HTTP 8001		Communication with Simple Host.
	TCP 4545	TCP 4545	Communication from the mobile Sharp units.
	TCP 4546		Time synchonization service for Sharp units.
	TCP 8899		Used by the Patroller's Updater Service to communicate with the mobile Sharp units (mobile Sharps are updated through Patroller).
	TCP 8666	TCP 8666	Used by Patroller and the Plate Reader Server (Sharp software) to communicate with their Updater Service.
	TCP 8787		Used by Patroller to communicate with Pay-by-Plate plugin.
		HTTP 2323	Used by the Patroller and the Sharp to determine which Extension to load.
		UDP 5000	Used to discover connected mobile Sharp units.
		TCP 8731	Communication to the LPR Manager role.
		TCP 8889	Used to notify the mobile Sharp's Updater Service to connect to the Patroller's Updater Service on a specific address and port (Updater Service discovery).
		TCP 8832	Used to communicate with the LPR Manager role for updates (used by Patroller's and fixed Sharps).

Disabling User Account Control in Patroller (Windows 7 and later)

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

What you should know

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

To disable Windows User Account Control:

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

Enabling Patroller clock synchronization with Security Center (Windows 8)

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

What you should know

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

To grant permission to a Patroller user to change the system time:

1 Log on to Windows as an administrator.

2 Run `secpol.msc`.

The **Local Security Policy** section of the Microsoft Management Console appears.

3 Go to **Local Policies** > **User Rights Assignment** > **Change the system time**.

4 Click **Add user or group**.

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

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

6 Restart the computer.

Installing AutoVu™ Patroller

This section explains how to install Patroller.

Before you begin

Prepare to install Patroller.

To install AutoVu™Patroller

1 Insert the AutoVu™ installation DVD in your computer's DVD drive, or double-click *Setup.exe* in the root folder of the Patroller installation package.

2 Select the installation language (English or French), and click **OK**.

3 If you are prompted to install any missing prerequisites, click **Install**. A reboot may be required.

4 Once the prerequisite software is installed, In the InstallShield Wizard *Welcome* window, click **Next**.

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

6 In the *Language Selection* page, select the user interface language for AutoVu™Patroller applications, and click **Next**.

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

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

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

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

11 In the *Patroller Connectivity* page, select whether you want Patroller to connect to Security Center or run in stand-alone mode.

12 If you chose to have Patroller connect to Security Center, select the Patroller configuration you want to install.

13 In the *Maps Configuration Selection* window, select whether to install maps or not.

NOTE: Maps are mandatory for City and University parking enforcement.

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

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

  This option will install Microsoft SQL Server 2014 Express Edition and create a database instance called SQLEXPRESS.

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

15 Click **Next**.

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

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

16 Click **Next.**

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

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

17 Click **Next**.

18 Click **Install**.

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

After you finish

- If you did not allow the setup program to automatically create firewall rules, then open the default ports to ensure that all AutoVu™ components can communicate with each other.
- If you have anti-virus software, it is recommended to add the following paths and files to the exception list of your anti-virus software. Failure to do so may result in slower performance from Patroller and extended software load times.
  - C:\Program Files (x86)\Genetec AutoVu X.X
  - C:\Offload
  - C:\Users\<username>\AppData
  - C:\Program Files (x86)\Microsoft SQL Server
  - C:\ProgramData\Genetec

AutoVu™ Patroller installation in silent mode

AutoVu™Patroller can be installed without any prompts or visual feedback using a command line.

Silent install command for Security Center

When performing a silent installation, specific program options are required to run the Security Center Installer.

The syntax for running the setup in silent mode is:

```
<setup_exe> <setup_options> <msi_options>
```

where:

- `<setup_exe>`: This is the setup program for the Security Center Installer. You can either use the standalone version (`"Security Center Setup.exe"` found in the *SC Packages* folder) or the web version (`SecurityCenterWebSetup.exe`).

  Do not use *setup.exe* found in the root folder of the installation package. It is an AutoRun-enabled version of the standalone installer, and as such, it does not accept command line arguments.
- `<setup_options>`: These are the setup options. They all start with a forward slash (/).
- `<msi_options>`: These are the Installer (MSI) options. They are all written in capital letters.

The following table lists the setup options.

Setup option	Description
`/ISInstallDir`	Specifies the path where the software will be installed. **EXAMPLES**: • `/ISInstallDir=C:\MyFolder` • `/ISInstallDir="D:\Program Files\MyFolder"` **NOTE:** In the second example, the (") are required because the value contains spaces. If not specified, the default is `<ProgramFiles>\Genetec Security Center 6.3`, where `<ProgramFiles>` is either %PROGRAMFILES% or %PROGRAMFILES(X86)%, depending on the version of your operating system.
`/ISFeatureInstall`	Specifies the features to be installed. The possible values are: • `Server` (Genetec™ Server with or without Directory, depends on the SERVER_TYPE installer option) • `Client` (Security Desk and Config Tool) • `SecurityDesk` (only Security Desk) • `ConfigTool` (only Config Tool) • `CompPacks,CompPack4x[,CompPack4x]` (Omnicast compatibility packs, you must specify at least one pack) **EXAMPLES**: • `/ISFeatureInstall=Server,Client` (DEFAULT) • `/ISFeatureInstall=Client,CompPacks,CompPack48`

Setup option	Description
`/silent`	Sets the Security Center setup.exe program to run in silent mode with no user interaction.
`/debuglog<FilePath>`	Enables the creation of the debug log file and specifies the file path. **NOTE:** The folder path specified in `<FilePath>` must exist. The setup program will not create it. **EXAMPLE**: `/debuglog"C:\DebugLog.log"`
`/log<FolderPath>`	Enables the creation of log files and specifies the folder path. **NOTE:** The `<FolderPath>` must exist. The setup program will not create it. **EXAMPLE**: `/log"C:\AllMyLogFiles\"`
`/language:`	Sets the language used by the installation program. Immediately precedes the four-digit language code. No space is allowed. **EXAMPLES** • `/language:1033` for English (DEFAULT) • `/language:3084` for French
`<msi_options>`	Sets the Security Center Installer (MSI) option list. Each option in the list uses the following syntax: `<option>=<value_list>` where `<option>` is an option name, and `<value_list>` is a list of comma seperated values. No space is allowed on either side of the equal sign (=). If the value list must contain spaces, the entire value list must be included between a pair of double quotes preceded by a backslash (\").

Installer options in Patroller

The following table lists the installer options:

Option	Description
`INSTALLDIR`	Specifies the path where the software will be installed. • `INSTALLDIR=C:\MyChoiceOfFolder` • `INSTALLDIR=\"D:\Program Files\Genetec AutoVu X.Y\"` Note that in the second example, (`\"`) is required because the value contains spaces. If do you not specify a path, it will be installed at *C:\Program Files\Genetec AutoVu X.Y*.
`ADDLOCAL`	Specifies the features to be installed. • ALL (installs Patroller files and documentation) • Documentation (installs only AutoVu™Patroller documentation) If the ADDLOCAL option is omitted, Patroller files are installed without documentation.

Option	Description
DATABASE_SERVER	Database server name. When omitted the default is “(local)\SQLEXPRESS”.
SQLSERVER_AUTHENTICATION	Specifies the authentication method used to connect to SQL server. Possible values are 0 or 1. When omitted the default value is 1. • 0 = Windows Authentication • 1 = SQL Server and Windows Authentication. If 1 is specified, you also need to specify SQLSERVER_PASSWORD for the password. **Example**: `SQLSERVER_AUTHENTICATION=0`
LANGUAGECHOSEN	Language used by Patroller. The possible code values are: • Arabic - 1025 • Chinese (Simplified) - 2052 • Chinese (Traditional) - 1028 • Czech - 1029 • Dutch - 1043 • English - 1033 • French - 3084 • German - 1031 • Hebrew - 1037 • Hungarian - 1038 • Italian - 1040 • Japanese - 1041 • Korean - 1042 • Norwegian - 1044 • Persian - 1065 • Polish - 1045 • Brazilian Portuguese - 2070 • Spanish - 1034 • Thai - 1054 • Turkish - 1055 **Example**: `LANGUAGECHOSEN=1033` If the code is invalid, English will be used. If this option is omitted, the installation language (specified with the `/L` option) will be used.
PATROLLER_CONNECTIVITY	Specifies whether or not to connect to Security Center. Accepted values are: • Security Center • Standalone When omitted the default is Security Center.

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

Sample installation commands in AutoVu™

The following are sample AutoVu™ installation commands.

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Uninstalling AutoVu™ Patroller in silent mode

AutoVu™ Patroller can be uninstalled in silent mode.

To uninstall AutoVu™ Patroller in silent mode:

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

Installing BeNomad files on the in-vehicle computer

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

Before you begin

- (Law Enforcement only) Make sure that you installed the “Maps Engine” during Patroller installation in the *Map Configuration Selection* page.
- When your AutoVu™ license is created, you receive an auto-generated email with a zip file containing the *BeNomad* maps for your geographic location, and a unique *.glic* file that contains your license information. You'll need both these files to install *BeNomad*.

To install *BeNomad*:

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

A folder called *BeNomad* is created.

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

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

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

4 Go to **Navigation** > **Maps**.

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

6 Click **Apply**.

NOTE: The Windows user account accessing the mobile client folder should have read and write permissions, other wise the map will always load zoomed out.

BeNomad maps are enabled when you start Patroller.

3

Updating and Upgrading Patroller

This section includes the following topics:

Installing AutoVu™ updates wirelessly

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

Before you begin

- Download the update from GTAP.
- In a wireless system setup, connect to the components you want to upgrade. For example, if you want to upgrade Patroller or mobile Sharp units, Patroller must be connected to Security Center.

What you should know

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

To install AutoVu™ updates wirelessly:

1 Turn on the updater service and specify the listening port in Security Center Config Tool, as follows:
   a) Log on to Security Center Config Tool.
   b) From the Security Center Config Tool *Home* page, go to **LPR** > **Roles and units**, select the LPR Manager that controls the units you want to update, and then click **Properties**.
   c) Turn on the **Update provider** and specify the listening port.

      This port number must match the **Update provider port** specified for Patroller in Patroller Config Tool.

2 Make the updates available, as follows:
   a) From the Security Center Config Tool home page, go to **LPR** > **General settings** > **Updates** to display all the Patroller and Sharp units on your system.
   b) Click the tab that corresponds to what you want to update:
      - Patroller and Sharp units
      - Update services
      - Firmware upgrade
   c) Click on the folder button under the *Path* column corresponding to the entity you want to update then navigate to the .zip file that contains the updates.

      An **Authorize** button appears under the *State* column. This button appears for all entities that have the same version as the one you want to update. This way you do not need to specify the path of the .zip file again if you decide to update the other entities.

      Example: For instance, if you specify the .zip file path for a Sharp camera version x.y, all Sharps with version x.y under the same LPR manager will have the **Authorize** button under the *State* column.

3 Push the updates to AutoVu™ components, as follows:
   a) From the Security Center Config Tool home page, go to **LPR** > **General settings** > **Updates**.

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

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

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

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

   If you have a fixed installation, you're finished. The update is automatically installed on the associated Sharps. For a mobile installation you need to manually accept the updates for Patroller and the associated Sharps.
4 (Mobile installations only) Manually accept Patroller and mobile Sharp updates, as follows:
   a) Start Patroller, and log on if required.
   b) In the Patroller notification bar, tap **Update** ( ).

      The **Update** dialog box appears, listing all the updates that are ready to install.
   c) Tap the **Patroller** icon to start the update.

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

   d) Tap **Update** ( ).

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

   e) Tap the **Sharp** icon to start the update.
      The Sharp update is installed on all Sharps connected to Patroller, and the SharpOS software restarts.

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

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

Updating Patroller by copying files to the in-vehicle computer

If your AutoVu™ components are not connected through a network or wireless link, you must manually copy the updates to Patroller.

To update Patroller:

1 On the in-vehicle computer, close Patroller and Patroller Config Tool.
2 Download and unzip the *Patroller.<update number>.zip* file, and then copy the contents to the Patroller's *MobileClient* folder.
   The default location of the folder on the in-vehicle computer is *C:\Program Files\Genetec AutoVu X.Y \MobileClient*.
3 Start Patroller for the update to take effect.
   Patroller is updated with the hotfix or service pack.

Upgrading Patroller to the latest version

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

Before you begin

- Read the following Release Notes (see the Technical Information Site) for any known issues and other information about the release:
  - *AutoVu SharpOS Release Notes*
  - *AutoVu Patroller Release Notes*
  - *Security Center Release Notes*
- Offload any remaining data in the Patroller database.
- Close Patroller and Patroller Config Tool.

What you should know

Your configuration settings are carried over from the previous version.

To upgrade Patroller:

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

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

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

2 Click **OK**.

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

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

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

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

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

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

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

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

  This option will install Microsoft® SQL Server 2014 Express Edition and create a database instance called SQLEXPRESS.

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

10 Click **Next**.

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

- **Windows Authentication:** Only users with Windows administrator privileges on the Patroller computer will be able to access the Patroller database.

- **SQL Server and Windows Authentication (mixed mode):** This is the recommended authentication method. It allows users without Windows administrator privileges to access thePatroller database. Choose a **Password** for Patroller to access the database.

  NOTE: The password you choose, along with the username "PatrollerUserDB," will be embedded in the Patroller Config Tool *Connection string*.

11 Click **Next.**

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

13 Click **Next**.

14 Click **Install**.

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

16 Upgrade the Patroller database:

a) Start Patroller.

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

The *Drop Database* window appears.

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

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

The Patroller upgrade procedure is complete.

After you finish

- If you did not allow the setup program to create firewall rules, open the default Patroller ports.
- Upgrade Plate Reader on the mobile Sharp units (described in a separate document). For more information, contact your Genetec representative.
- The following Patroller settings are reset to their factory defaults after upgrading:
  - **Patroller window behavior:** The Patroller window's initial size, position, and state (normal, minimized, maximized) are reset. You re-size and re-position the window manually, and you configure the window's state from the User interface section in Patroller Config Tool.
  - **Map rotation behavior:** The option to have the Patroller icon or the map rotate with vehicle movement is reset. You can configure this setting from Patroller's **Options** tab.
  - **Main window display:** The option to display the map or the vehicle's context image in the Patroller main window is reset. You can configure this setting by clicking the thumbnail map or image in the Patroller information panel.
  - **Initial GPS position:** The Patroller's initial GPS position is reset. This will automatically be adjusted as the Patroller vehicle starts moving.
  - **MLPI Selection type:** (Mobile License Plate Inventory only) The way you patrol a parking facility in MLPI is reset. You can choose between **Route** or **Configuration** when selecting a parking facility in Patroller.
  - **Patroller location display:** How Patroller displays the vehicle's current location is reset. You can tap the address in the notification bar at the top of the Patroller window to toggle between displaying the reverse-geocoded address or GPS coordinates.
- You can refer to your old Patroller configuration files to update the current Patroller settings. The files are located on the in-vehicle computer at the default location *C:\Program Files\Genetec AutoVu X.Y \MobileClient\OldConfigFiles*. The configuration files from the earlier versions remain in their original directory.
- If you're using maps, you'll need to install and configure BeNomad maps because *MapInfo* is no longer supported.

Default Patroller sound files

There are four default sound files that Patroller uses for LPR events, which are located on the in-vehicle computer in *C:\Program Files\Genetec AutoVu X.Y\MobileClient\Config\Sounds* (default location).

The default sound files are the following:

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

You must know the following about the default sound files:

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

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

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

  BEST PRACTICE: New hotlist sound files can be stored anywhere on the in-vehicle computer, but you should keep them in the same *Sounds* folder as the default sound files. This makes it easier to update them later.

Changing sound files for LPR events using the updater service

You can send different sound files to the Patroller's *MobileClient* folder using the Security Center updater service.

What you should know

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

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

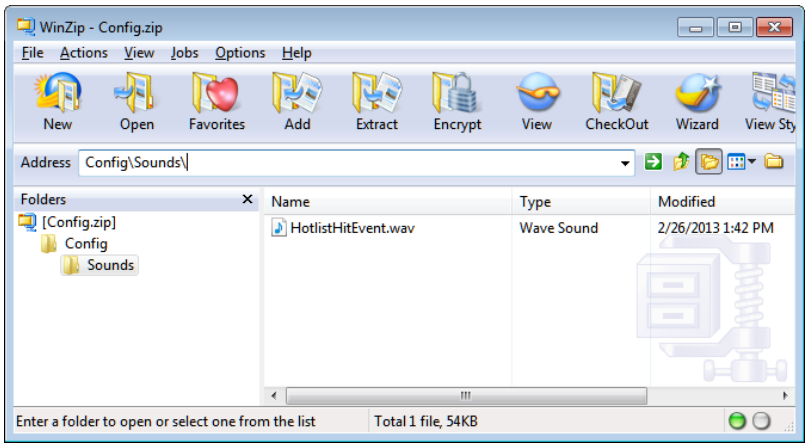
To change the sound files for LPR events using the updater service:

1 (Optional) If you want to overwrite a default sound file, rename your new sound file to match the name of the default file you want to replace (for example, *HotlistHitEvent.wav*).

2 On the Security Center computer, create the same Windows Explorer file structure found on the Patroller in-vehicle computer (for example, *C:\Program Files\Genetec AutoVu X.Y\MobileClient\Config\Sounds*).

3 Copy your new sound file to the *Sounds* folder you created.

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



The file extracts to the destination defined in the zip file path (*Sounds* folder).

5 (Optional for hotlist sounds) If the file has a different filename than the default *HotlistHitEvent*, you must specify the full path to the file, including the new filename:

a) From the Config Tool home page, open the **LPR** task.
b) Select the hotlist to configure, and click the **Advanced** tab.
c) In the **Sound file** field, specify the path and filename to the sound file on the in-vehicle computer.
d) Repeat the steps for as many hotlists as you want.

6 Send the sound file to Patroller as if you were installing an update wirelessly.

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

Related Topics

Default Patroller sound files on page 26

Changing sound files for LPR events

You can add new sound files to Patroller to use for LPR events, by manually copying the sounds to the Patroller in-vehicle computer.

What you should know

The sound files must be *.wav* format.

To change the sound files for LPR events:

1 Log on to the Patroller in-vehicle computer.

2 To overwrite the default sound files, do the following:
   a) Open the folder *C:\Program Files\Genetec AutoVu X.Y\MobileClient\Config\Sounds*.
   b) Rename your sound file to match the default file you want to overwrite.
   c) Copy your new sound file to the *Sounds* folder so that it overwrites the default file.

3 (Optional) To use a sound file with a different filename for hotlists, do the following:
   a) Copy your new sound file to any location on the in-vehicle computer.
   b) Open Config Tool.
   c) From the home page, open the **LPR** task.
   d) Select the hotlist to configure, and click the **Advanced** tab.
   e) In the **Sound file** field, specify the path and filename to the sound file on the in-vehicle computer.
   f) Repeat Step d and e for as many hotlists as you want.

4 Restart Patroller for your changes to take effect.

Patroller uses the new sound file for the LPR event.

4

Configuring Patroller

This section includes the following topics:

Naming a Patroller unit

The Patroller unit name is the name of the Patroller unit or vehicle as it will appear in Security CenterConfig Tool and Security Desk.

What you should know

The Patroller unit name is **not** the Patroller user's username. The username is set in Security Center Config Tool when you create a user. For more information on creating users and user groups, see the Security Center Config Tool product help.

To name a Patroller unit:

1 Open Patroller Config Tool.
2 Go to the *General* page.
3 In the **Patroller name** field, enter the name of the Patroller unit as you want it to be seen in Security Center and Security Desk.
4 Click **Apply**.

The Patroller unit name is detected automatically when you connect Patroller to Security Center. It will appear as a Patroller entity under the LPR Manager.

Configuring Patroller logon options

How a user logs on to Patroller is configured on the *General* page of Patroller Config Tool.

To configure Patroller logon options:

1 Open Patroller Config Tool.

2 Go to the *General* page.

3 From the **Logon type** drop-down menu, select how you want to log on to Patroller:

- **No logon:** No username or password required.
- **Windows logon:** If the username logged on to Windows matches a username contained in the *Users* file downloaded to Patroller, you won't be asked for a username or password; Patroller will simply open.
- **Secure name:** Only the Patroller user's Security Center username is required.
- **Secure name and password:** The Patroller user's Security Center username and password are required.

  NOTE: You create usernames and passwords in Security CenterConfig Tool when configuring users and user groups.

4 Click **Apply**.

Configuring Patroller database options

The Patroller database options are configured on the *General* page of Patroller Config Tool.

To configure Patroller database options:

1 Open Patroller Config Tool.
2 Go to the *General* page.
3 Beside **SQL server,** select the address and name of the SQL server.
4 In the **Database name** field, you can leave the default database name, or change it if desired.

   You can change this name at any time to create a new database.

5 Beside **Use Windows authentication**, do one of the following:

   - Turn this setting on to use your Windows credentials to connect to the database.
   - Turn this setting off to use the specific User ID and Password you specified during Patroller installation to connect to the database.

   NOTE: Your username and password are part of the database Connection String.

6 In the **User id** field, enter the User ID to connect to the Patroller database. This User ID was entered during Patroller installation.
7 In the **Password** field, enter the password to connect to the Patroller database. This password was entered during Patroller installation.
8 Click **Advanced** to configure the following:

   - **Max logout:** Set the amount of time (in hours) that a user can be logged out and still resume their shift when logging back on. When this period has elapsed, or if a different user logs on, the system sees this as the start of a new shift and the data presented to the user reflects that. A value of 0 deactivates this feature, meaning that a new shift begins any time a user logs in. The default logout time is 4 hours.
   - **Store reads for:** Set the amount of time that reads are stored in the Patroller database. Reads older than this value are deleted from the database at the start of the next shift. The default storage time is 96 hours.
   - **Store hits for:** Set the amount of time that hits are stored in the database. Hits older than this value are deleted from the database at the start of the next shift. The default storage time is 120 hours.
   - **Record search:** Set the amount of time that records (reads or hits) are searchable by the Patroller user. Records older than this value will no longer be searchable at the start of the next shift. The default search time is 48 hours.
   - **Record display:** Set the amount of time that a record can be displayed. The default time is 12 hours.
   - **Folder path:** Type the folder path where the database files are created and replicated.
   - **Offload query timeout:** Define the timeout duration for the offload queries. The default timeout is 1800 seconds.
   - **Connection string:** The string to connect to the Patroller database.

   You shouldn't need to configure this option since SQL is installed automatically, or an existing SQL instance is used when you install Patroller.

   If you selected *SQL Server and Windows Authentication (mixed mode)* when you installed Patroller, you can see the *User ID* and *Password* you selected in this string.

9 Click **Test connection**, to test the connection to the Patroller database with the options selected.
10 Click **Apply**.

Connecting Patroller to Security Center

You need to configure Patroller and Security Center so the LPR Manager can discover and communicate with the Patroller units it controls.

To connect a Patroller to Security Center:

1 From the home page in Security Center Config Tool, click **System** > **Roles**, and then select the LPR Manager you want to configure.
2 Click the **Properties** tab, and then click **Live**.
3 In the **Listening port** option, select the port to listen for connection requests coming from Patrollers.
4 To encrypt the communication between Security Center and Patroller Config Tool, select the **Encrypt communication channel** option.

   IMPORTANT: This setting also needs to be applied in Patroller Config Tool.

5 To allow Security Center to still accept incoming connections from Patrollers that do not have the encryption option enabled, select the **Access non encrypted messages** option.
6 Click **Apply**.
7 Open Patroller Config Tool.
8 Go to Security Center, and turn on the **Connect to Security Center** option.
9 Enter the IP address of the Security Center machine hosting the LPR Manager role.
10 Enter the Port number Patroller should use to connect to the LPR Manager role.
11 If you chose the Encrypt communication channel option in Security Center Config Tool, turn the on the Encrypt communication channel option.
12 Enter the Update provider port that Security Center uses to send updates to Patroller and connected Sharp units.

   NOTE: Enter the same Update provider **Listening port** that is configured in Security Center Config Tool. For more information, see the *Security Center Administrator Guide*.

13 Select which **Live events** you want to send to Security Center.
14 Beside **Periodic transfer**, specify how often hotlist and permit list changes are downloaded to Patroller (if you have a live connection). The default transfer period is every 240 minutes. You can disable Periodic transfer on specific hotlists (not permit lists) in Security Center Config Tool on the hotlist's Advanced page. For more information, see the *Security Center Administrator Guide*.

Copying the *MatcherSettings.xml* from the Patroller in-vehicle computer to Security Center

If shared permits are enabled and Patroller is connecting to a Security Center 5.2 server, you must copy the *MatcherSettings.xml* file from the Patroller in-vehicle computer to the Security Center server and then apply the new LPR matcher settings using Server Admin.

To copy the MatcherSettings.XML from the Patroller in-vehicle computer to the Security Center server:

1 On the Patroller in-vehicle computer, navigate to *C:\Program Files (x86)\Genetec AutoVu 6.3\MobileClient* and copy the *MatcherSettings.xml* file.
2 On the Security Center server, navigate to *C:\Program Files\Genetec\Security Center 5.2* and replace the *MatcherSettings.xml* with the one you copied from the Patroller in-vehicle computer.
3 From a web browser, open the Server Admin console by typing *http://<server>/genetec/console#/Commands*.
4 From the **All commands** page, click **UpdateAutoVuGlobalSettings** then close Server Admin console.
5 Restart the Security Center Directory.
   a) From a web browser, open Server Admin by typing *http://<server>/genetec*.
   b) Click the Directory tab and under **Directory status**, click **Restart**.

c) After the Directory restarts, close Server Admin.

LPR matcher settings are now configured and applied to all the LPR Manager roles on your system. Patroller units are updated the next time they connect to Security Center.

Configuring Patroller offload settings

Offloading allows you to transfer reads, hits, and other Patroller data to Security Center or to a local file that can be copied to a USB key.

What you should know

Other than selecting the offload method, you can also select which events from the Patroller are transferred. You can select if you want to include the images and you also determine what happens with the data once the offload is completed.

To configure Patroller offload settings:

1 Open Patroller Config Tool.

2 Go to **Offload**.

3 From the **Offload method** drop-down list, choose your offload method:

- **None:** Does not offload data.
- **Local file:** You can configure Patroller to offload data to a file on the in-vehicle computer. 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.
  - If you are connected to Security Center: After you have offloaded the data, you can then copy the data to a USB key, and transfer it to the Security Center computer.
  - If you are using Patroller Standalone: After you have offloaded the data, you can open the *Offload.Standalone* file in Internet Explorer to view the information or import the *.Standalone* file into your own reporting tool.
- **Live Transfer:** This offload method transfers all data from the Patroller vehicle to Security Center using a wireless connection. For example, you can offload your data at the end of a shift, when you're in range of the company's wireless network. You also use this option to offload data to a network drive rather than your local drive on the in-vehicle computer.

  NOTE: Please note the following about *Live transfer*:

  - This option automatically transfers the offload data into the *Offload* folder under the LPR Manager root folder. For more information about the LPR Manager root folder, see the *Security Center Administrator Guide*.
  - If you try to offload without being connected to Security Center, the offload is done on your local in-vehicle computer. You can then transfer the offload data to Security Center with a USB key.

4 Configure the following settings:

- **Local offload drive:** If using *Local file* as your offload method, specify where on your machine the data should be saved (e.g. C:\ if you want to offload to your C drive).
- **Use encryption:** Turn on to encrypt the offloaded data. You'll also need the Public key (not applicable to Patroller Standalone).
- **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 <your version>*, and copy the *OffloadPublicKey.xml* file to your clipboard.
  2 On the Patroller computer, go to *C:\Program Files\Genetec AutoVu X.Y\MobileClient*, and paste the *OffloadPublicKey.xml* in the folder.
  3 In the *Public key* field, enter the path to the public key you just pasted to the Patroller computer (*C:\Program Files\Genetec AutoVu X.Y\MobileClient\OffloadPublicKey.xml).*
- **Offload events:** This option allows you to choose which data you want to include in an offload. For example, you may only want to offload **Hits** to use less bandwidth when performing an offload.

- **Include all images:** Turn on to offload all images. If this option is turned off, only images associated with a hit will be included in the offloaded data.
- **Incremental offload:** By default, Patroller offloads data in increments, or segments. Turn this setting off if you want to offload the full data file each time.
- **Data segment size:** Specify the maximum file size of each data segment (MB) when using Incremental offload. Once the offload file reaches the size limit, a new offload file is created and the offload process continues. The default maximum file size is 1 MB.
- **Force offload before exit:** Turn on to make Patroller exit commands unavailable. The only way to close the application is to perform an offload.

  NOTE: This option won't work if you set **Offload method** and **Action after offload** to **None**.
- **Action after offload:** Select the exit procedure that occurs after you have performed an offload:
  - *None* **:** Return to the application.
  - *Exit* **:** MobileServer, MobileClient, and IO.Services are exited.
  - *Shutdown* **:** If the *PowerManagement.UsePowerManagement* option is selected, the OffloadExit setting is automatically set to *Shutdown*. This option does not work with laptops; choose *Exit* instead.
- **Delete after offload:** Turn on to delete all records of user logins, images, hotlist hits, vehicles, unit states, street blocks, tire images, cameras, and attributes after a successful offload.

Connecting mobile Sharp units to Patroller

Sharp camera units are added to the in-vehicle network so they can capture license plates and send the data 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).

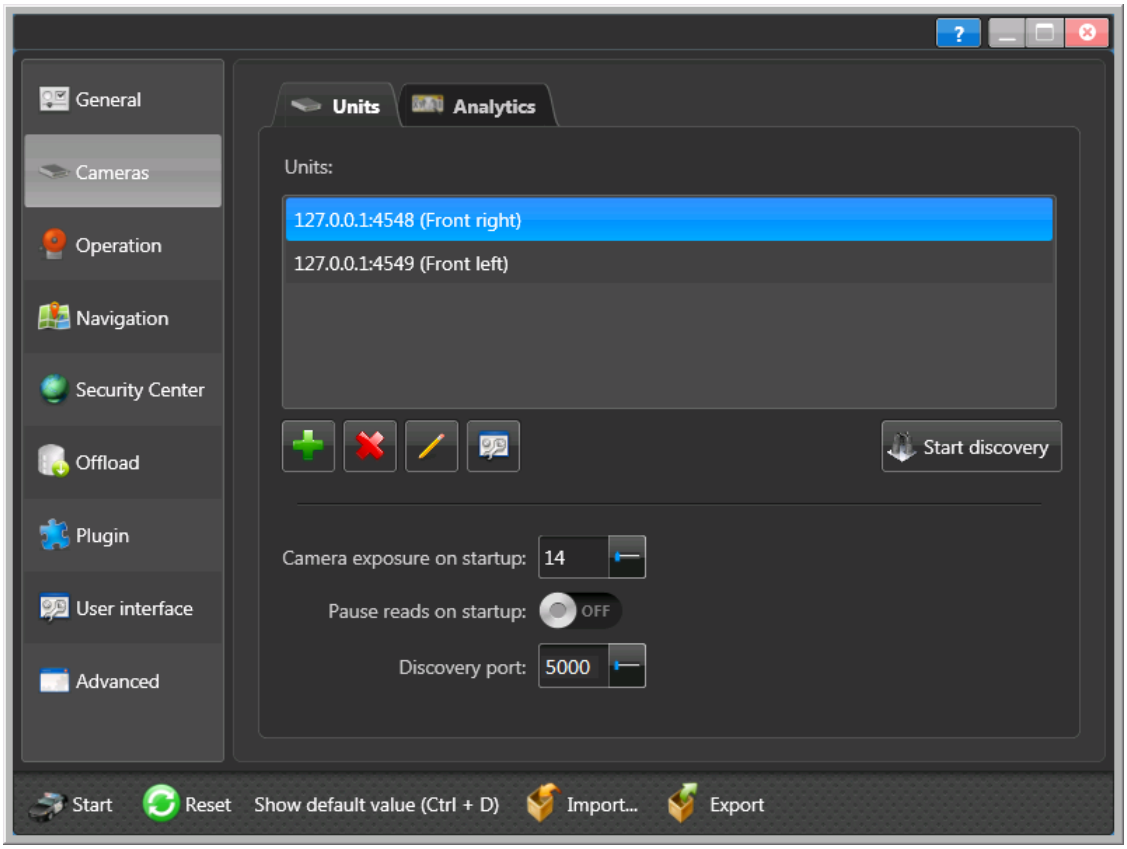
Before you begin

Your Sharp units must be configured for a mobile AutoVu system. For information about configuring Sharp units, see the *Sharp Administrator Guide*.

To connect a Sharp unit to Patroller:

1 Open Patroller Config Tool.

2 Go to the *Cameras* page.



3 To auto-detect all Sharps connected to the LPR Processing Unit, do the following:

a) Make sure the **Discovery port** matches the discovery port you set for the Sharp in the Sharp Portal. For more information, see the *Sharp Administrator Guide*.

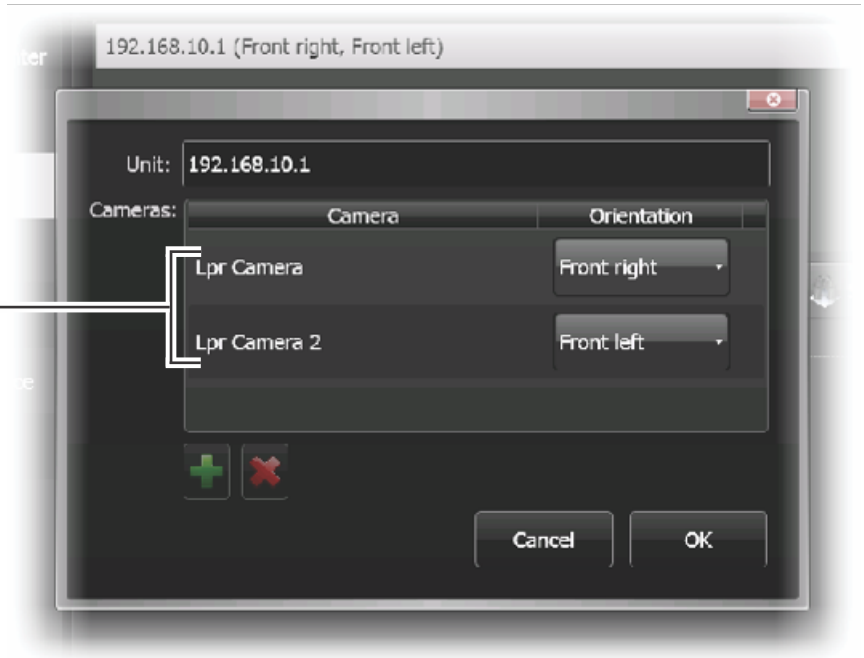
NOTE: The default discovery port for all Sharps is 5000, therefore you shouldn't need to change the port number.

b) Click **Start discovery**.

Patroller detects the connected Sharps and adds them to the **Units** list.

c) Make sure each Sharp in the **Units** list has a different orientation. To do this, click on a Sharp, click the **Edit** button (), and then change the orientation of the Sharp to match where the Sharp is located on the vehicle.

For SharpX systems, you may see up to four LPR cameras controlled by a single unit (Single Board Computers or SBC). Make sure that all LPR cameras have different orientations.



Spell the camera names exactly as shown. They must be “**L**pr **C**amera ”, “**L**pr **C**amera **2**” etc. (case-sensitive).

4 (Optional) If you want to manually add a Sharp camera instead of using the automatic discovery feature, click the **Create** button (), and do the following:

a) Under **Unit**, enter the Sharp’s IP address (e.g. 192.168.10.1), or the Sharp name as it appears on the Sharp camera unit’s label (e.g. Sharp1234).

If you're using a SharpX system, the LPR Processing Unit will have either one (X1S) or two (X2S) processors (Single Board Computers or SBCs). Each SBC will correspond to one "unit" and can be connected to up to four SharpX cameras. In this case, go to Step b to add the required cameras. If you don't have a SharpX system with multiple cameras, go to Step c.

b) (For SharpX systems) When more than one camera is connected to an SBC, click the **Create** () button to add additional cameras.

**IMPORTANT: ** Enter camera names as “Lpr Camera” and “Lpr Camera 2” (case-sensitive).

c) Choose the camera’s orientation from the drop-down list.

5 (Optional) Select the Sharp camera’s initial exposure settings. In general, higher exposure is for darker environments, and lower exposure is for brighter environments.

NOTE: The Sharp has auto-exposure capability that compensates for different plate reflectivity, as well as exterior ambient light. You shouldn’t need to change the default value for this setting.

6 (Optional) Click **Start suspended mode** to start Patroller with plate reading turned off.

7 Click **Apply**.

The Sharp cameras are now connected to Patroller, and you should be able to see the live feed from the Patroller application.

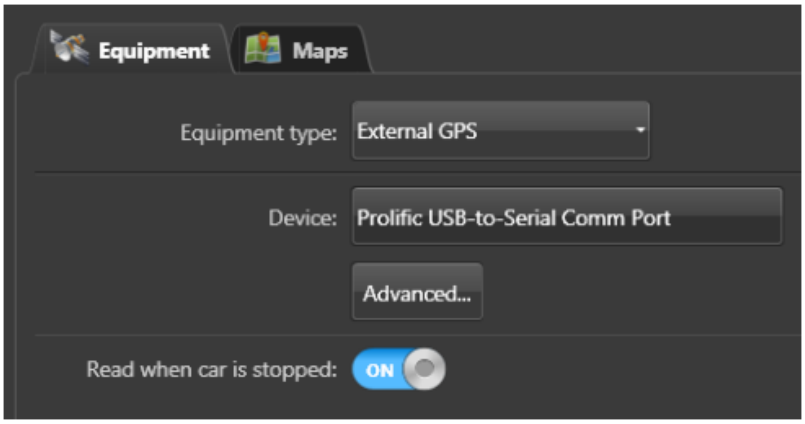
Enabling Patroller GPS settings

If you are using Patroller with GPS, you need to configure the related settings in Patroller Config Tool. These settings apply to the USB GPS that connects directly to the in-vehicle computer.

To enable External GPS settings for Patroller:

1 Open Patroller Config Tool.

2 Go to **Navigation** > **Equipment**.



3 From the **Equipment type** list select **External GPS**, and then configure the following:

- **Device:** Click in the field to open the **Select device** dialog box. Choose the appropriate USB device and click **OK** > **Apply**.

4 Click **Advanced** and configure the following:

- **Baud rate:** The speed of the GPS communications channel (serial port). The default value is 9600, but some USB GPS devices require a reduced speed of 4800. This value should not be modified for the External Navigator box, but for example, if you are using the USB GPS antenna that connects to the in-vehicle computer (model number BU-353), the baud rate value is automatically set to 4800.
- **(Optional) Force port:** Turn this option on when you want to make sure that Patroller uses the port configured in Patroller Config Tool. This is useful when you are using two USB GPS devices and you want to prevent Patroller from automatically switching to the other GPS port if it cannot detect the GPS port specified in Patroller Config Tool.
- **Port:** When the GPS is configured the port is automatically detected by Patroller during startup.
- **GPS initialization string:** Displays the initialization commands to be sent to the GPS device when you log on to the application.

  IMPORTANT: Do not modify. This is the default firmware setting.
- **Consecutive invalid strings before restart:** Specify the number of consecutive invalid GPS strings allowed before the device is restarted. Invalid GPS strings happen when the GPS signal can't be detected. The default number is 10.

  IMPORTANT: You should not need to change this setting.
- **Noise:** Specify the noise value. If the distance from 0,0 to the GPS position is less than the value you define, no GPS event is generated. The default noise value is 5.

  IMPORTANT: You should not need to change this setting.

5 Turn **Read when car is stopped** on if you want to continue reading plates when the Patroller vehicle is stopped.

When doing parking enforcement, Patroller vehicles may stop and reverse frequently.

6 Click **Apply**.

The GPS settings for Patroller are configured.

After you finish

Install the GPS driver on the Patroller computer.

Enabling Patroller Navigator box GPS settings

If you are using Patroller with the AutoVu™ External Navigator box, you need to configure the settings that apply to the GPS antenna connected to the Navigator box in Patroller Config Tool.

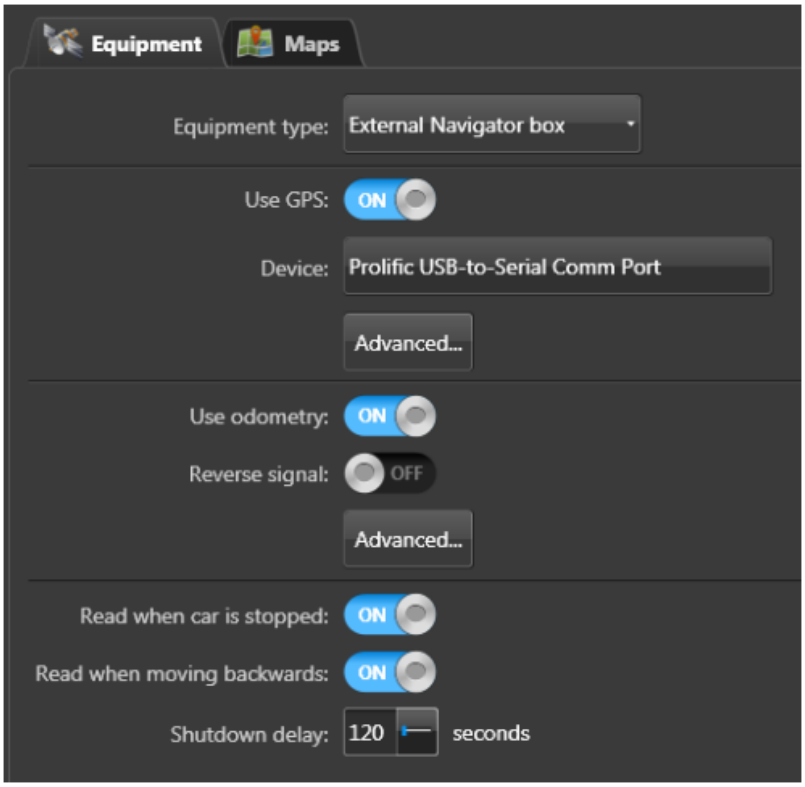
Before you begin

Install the GPS driver on the Patroller computer.

To enable GPS settings for Patroller:

1 Open Patroller Config Tool.

2 Go to **Navigation** > **Equipment**.



3 From the **Equipment type** list, select **External Navigator box**.

4 Turn **Use GPS** to **ON**, then configure the following:

- **Device:** Click in the field to open the **Select device** dialog box. Choose the appropriate USB device and click **OK** > **Apply**.

5 Click **Advanced** and configure the following:

- **Baud rate:** The speed of the GPS communications channel (serial port). The default value is 9600, but some USB GPS devices require a reduced speed of 4800. For example, if you are using Genetec's USB GPS antenna that connects to the in-vehicle computer model number BU-353, the baud rate value is automatically set to 4800.

  IMPORTANT: You should not need to change this setting for the External Navigator Box.

- **(Optional) Force Port:** Turn this option on when you want to make sure that Patroller uses the port configured in the Patroller Config Tool. This is useful when you are using two USB GPS devices and you want to prevent Patroller from automatically switching to the other GPS port if it cannot detect the GPS port specified in Patroller Config Tool.

- **Port:** Specify the COM port number of the GPS device as seen in Windows Device Manager. The name of the device is *u-blox 5 GPS and GALILEO Receiver*.
- **GPS initialization string:** Displays the initialization commands to be sent to the GPS device when you log on to the application.

  IMPORTANT: Do not modify. This is a default firmware setting.
- **Consecutive invalid strings before restart:** Specify the number of consecutive invalid GPS strings allowed before the device is restarted. Invalid GPS strings happen when the GPS signal can't be detected. The default number is 10.

  IMPORTANT: You should not need to change this setting.
- **Noise:** Specify the noise value. If the distance from 0,0 to the GPS position is less than the value you define, no GPS event is generated. The default noise value is 5.

  IMPORTANT: You should not need to change this setting.

6 Turn **Use odometry** to **ON** if you want to use the car's odometry system then configure the following:

- **Reverse signal active when:** This option confgures if the reverse signal is active HIGH or LOW while using the Navigator box. When the option is ON, the signal is active HIGH.

7 Click **Advanced** then configure the following:

- **Scale:** Value specified during system calibration.
- **Sensitivity:** Navigator box's sensitivity as measured during calibration using the Oscilloscope tool.
- **GPS distance tolerance:** Maximum GPS distance correction allowed (in meters) when using odometry.
- **GPS odometry calibration tolerance:** Acceptable odometry calibration error (in meters).

For more information about Navigator box calibration, see *AutoVu Hardware Guide for SharpX Installation*.

8 If you want to continue reading plates when the Patroller vehicle is stopped, turn **Read when car is stopped** to **ON**.

9 If you want to continue reading plates when the Patroller vehicle moves in reverse, turn **Read when moving backwards** to **ON**.

NOTE: When doing parking enforcement, Patroller vehicles may stop and reverse frequently.

10 Specify the **Shutdown delay**. This delay is the number of seconds to wait after the vehicle’s ignition is turned off before shutting down the in-vehicle computer. To disable this feature, enter “0”.

11 Click **Apply**.

The GPS settings of the Navigator box are configured.

Process Overview: AutoVu™ Navigation

If the LPR Processing Unit in your Patroller vehicle includes the AutoVu™ Navigation option, you must configure and calibrate the system to ensure that accurate location information is associated with LPR reads and hits.

To configure and calibrate the AutoVu Navigation system:

1 Enable the AutoVu™ Navigation settings in Patroller Config Tool. This is where you select your navigation hardware and configure system settings.

2 Specify the position of the GNSS antenna and the navigation module relative to the center of the rear axle of the Patroller vehicle to get accurate navigation values.

3 Calibrate the AutoVu™ Navigation hardware. This is where you drive the vehicle while following on-screen instructions to calibrate the system.

Enabling AutoVu Navigation settings

If you are using Patroller with the AutoVu™ Navigation hardware, you need to configure the related settings in Patroller Config Tool. These settings allow you to calibrate and monitor the positioning hardware, as well as configure the GNSS antenna.

Before you begin

Connect your Sharp mobile units to Patroller.

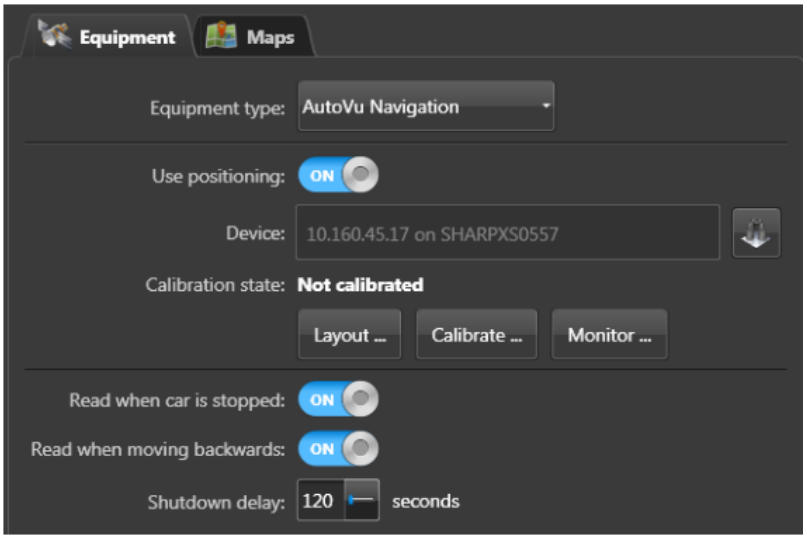
What you should know

To use AutoVu™ Navigation, your LPR Processing Unit must include the AutoVu Navigation option and must be running SharpOS 11.4 or higher.

To configure settings for AutoVu™ navigation:

1 Open Patroller Config Tool.

2 Go to **Navigation** > **Equipment**.



3 From the **Equipment type** list, select **AutoVu Navigation**.

4 Turn **Use positioning** to **ON**, then configure the following:

- **Device:** The navigation hardware auto discovery starts automatically when a SharpX camera is accessible. Click the discovery button to restart the auto discovery if necessary. When a navigation device is discovered, the **Layout...**, **Calibrate...** and **Monitor...** buttons as well as the **Calibration state** field appear.
- **Layout:** This button allows you to enter the GNSS antenna and port positions. This operation is necessary to calibrate the navigation hardware. For details, see Configuring the AutoVu navigation equipment layout.
- **Calibrate:** This button allows you to perform step-by-step odometry and GNSS calibration. For details, see Calibrating Patroller Navigation.
- **Monitor:** Click this button to get information about navigation position, malfunctions, and vehicle status. For details, see the Navigation Page - Equipment - Monitor reference page.

5 If you want to read plates when the Patroller vehicle is stopped, turn **Read when car is stopped** to **ON**.

6 If you want to read plates when the Patroller vehicle moves in reverse, turn **Read when moving backwards** to **ON**.

NOTE: When doing parking enforcement, Patroller vehicles may stop and reverse frequently.

7 Specify the **Shutdown delay**. This delay is the number of seconds to wait after the vehicle's ignition is turned off before shutting down the in-vehicle computer. To disable this feature, enter "0".

8 Click **Apply**.

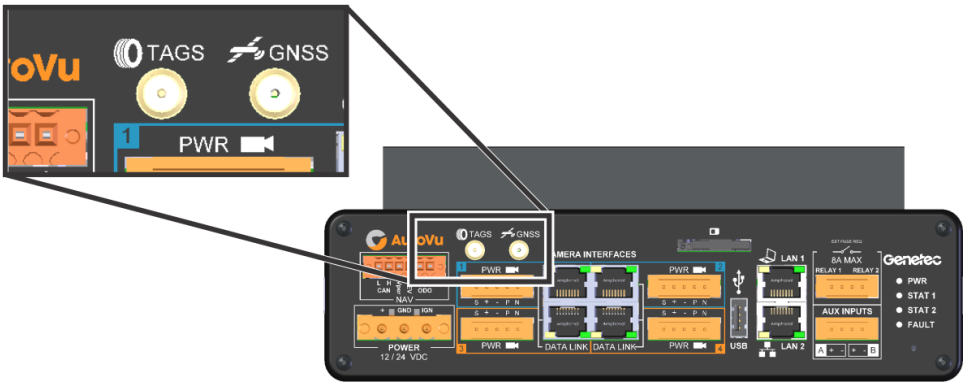
The settings for AutoVu navigation are configured.

Configuring the AutoVu navigation equipment layout

If you are using the AutoVu™ navigation system, you need to specify the position of the GNSS antenna and the navigation module relative to the center of the rear axle of the patrolling vehicle to get accurate navigation values.

Before you begin

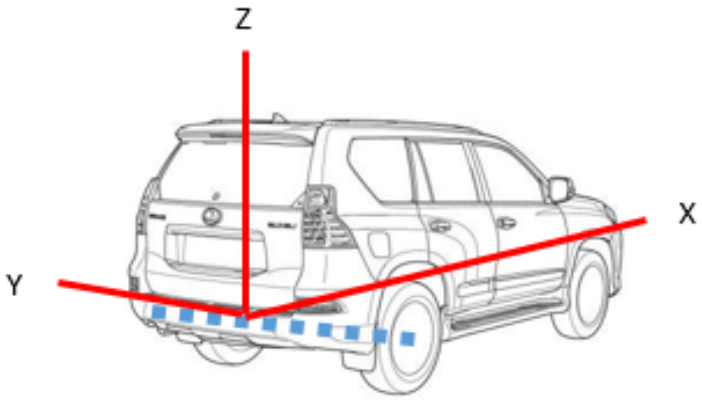
- You need to measure the x, y, and z distances (see vehicle image below) between the vehicle's rear axle and both the GNSS antenna and the GNSS connector. You will need a measuring tape, and other tools to help you. You need to measure from the antenna to the rear axle in all three directions, and from the GNSS connector to the rear axle in all three directions. The GNSS connector is located on the LPR processing unit face plate. See the following diagram:

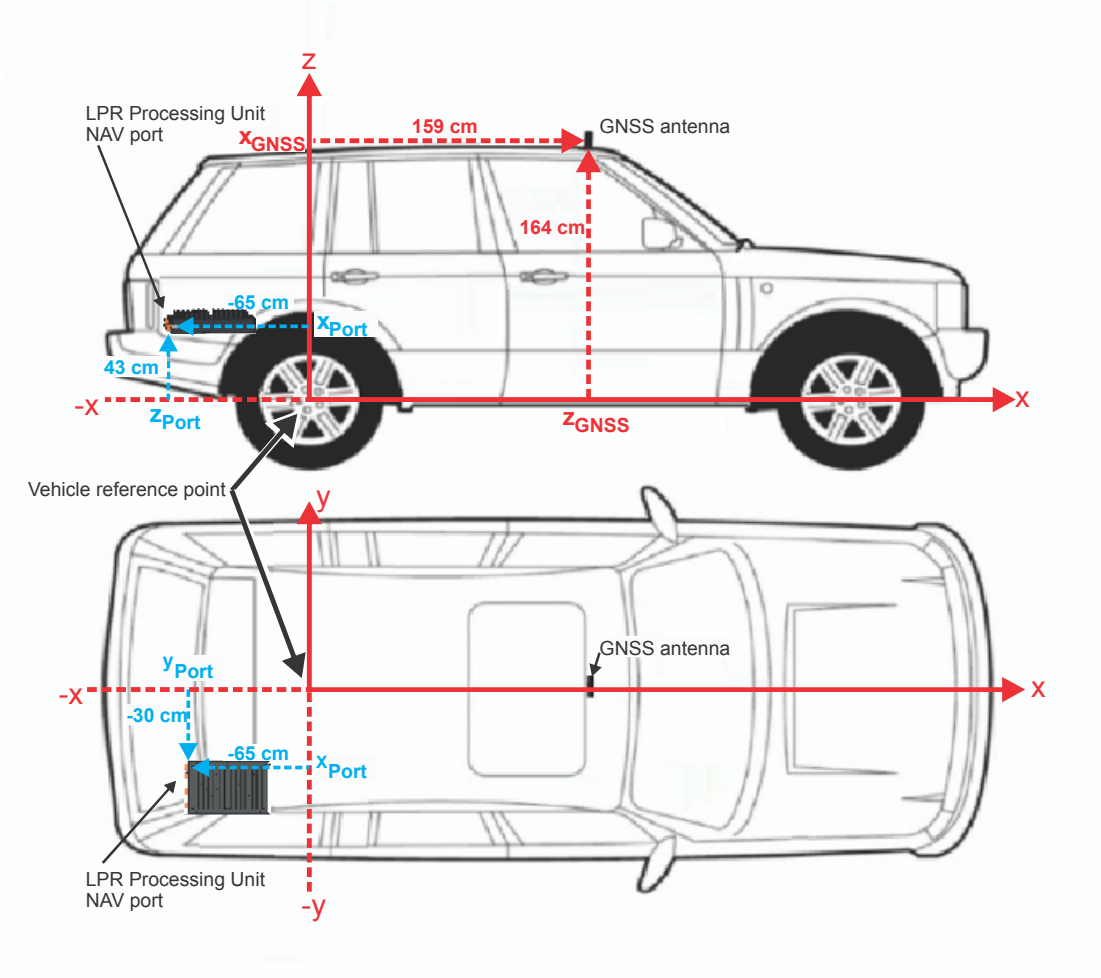


  Measurement precision must be within 10 cm (4 in.).

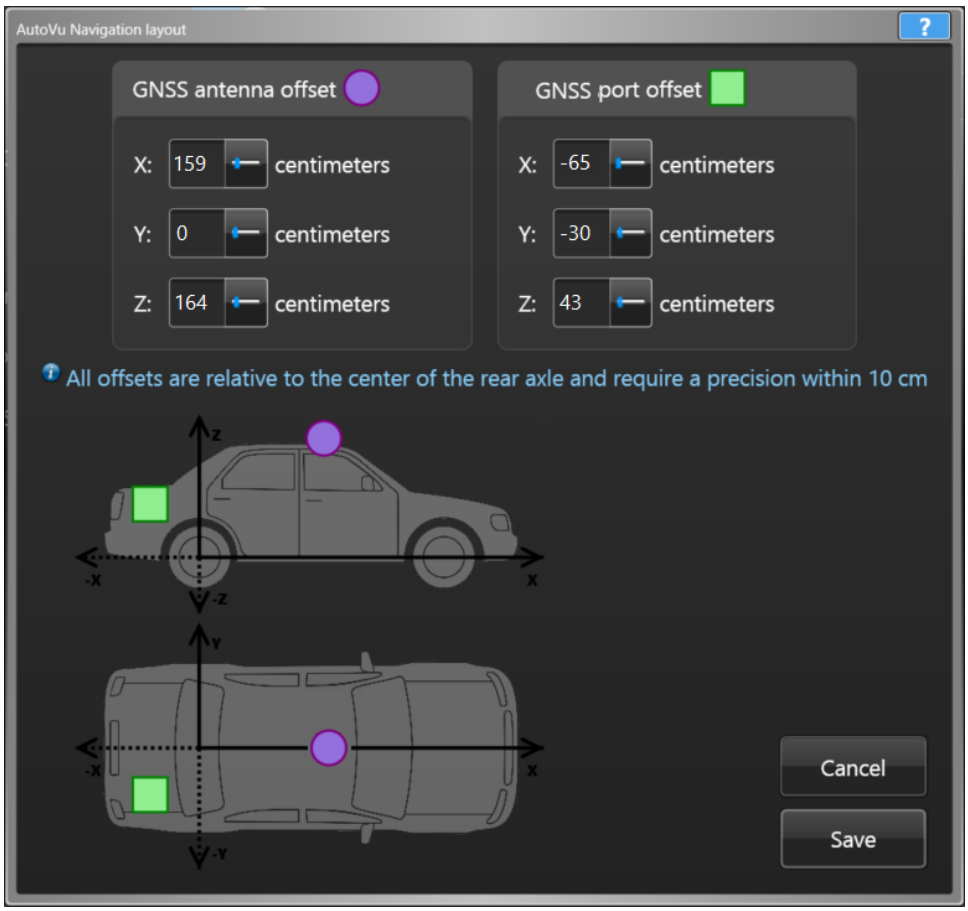
- Enable AutoVu™ navigation.

What you should know





- The x axis represents the position of the equipment relative to the length of the car (rear and front). The zero position being the rear axle, a negative value is behind the rear axle and a positive value is in front of the rear axle.
- The y axis represents the position of the equipment relative to the width of the car (left or the right) when standing behind the vehicle and looking towards it. The zero position being the center of the car, a positive value is towards the left and a negative value is towards the right.
- The z axis represents the height of the equipment relative to the rear axle. A positive value is positioned above the axle.
- The diagrams provided on the configuration page are for illustrative purpose only as vehicle models may vary. The symbols will be displayed within the diagram boundaries even if large numbers are entered in the measurements input fields.



To configure navigation equipment layout for AutoVu™ navigation:

1 Enter the GNSS antenna x, y, and z measurements in centimeters.

The purple dot shows the antenna's position on the car diagram, both on the top and side views. The axis being modified is highlighted on the diagram.

NOTE: You can configure Patroller to use Imperial or Metric units in the **User interface** configuration page.

2 Enter the GNSS port (or connector) x, y, and z measurements in centimeters.

The green square shows the processing unit's position on the car's diagram. The axis being modified is highlighted in blue.

3 Click **Save**.

The position values are saved on the LPR Processing unit. When starting calibration, Patroller will first try to load values that have been saved on the navigation module. If the module has been programmed with values, they will be used by default, which is good if the on-board computer has to be changed. The measurements do not need to be taken again. If an LPR Processing unit has never been initialized, all zeros are shown. If the values can't be read or written correctly, a warning message appears.

The AutoVu™ navigation equipment layout is now configured.

Calibrating the AutoVu™ Navigation system

If you are using Patroller with the AutoVu™ Navigation hardware, you need to calibrate the hardware in order to get accurate readings.

Before you begin

- Enable AutoVu™ Navigation.
- Configure the navigation system layout.

What you should know

- The calibration time (approximately 10-15 minutes) can vary based on geographical location, environment, driving style, vehicle repositioning time, proper execution of requested maneuvers, and driver experience with the procedure.
- The procedure requires that you drive straight, backwards, and that you execute several turns. You will also be asked to drive over hills. You need to locate a suitable road, parking lot or large area where you can complete the procedure in a safe way.
- No feedback is given when a maneuver is performed.
- You can perform the maneuvers in any order.
- There is no time limit to complete the maneuvers.
- If required, you can reposition the vehicle prior to each maneuver.

WARNING: For safety reasons, you must carry out calibration of AutoVu navigation away from any area with motor vehicle traffic, with the assistance of another individual to identify and avoid any hazards in the selected area. GENETEC WILL IN NO EVENT BE LIABLE FOR ANY DIRECT OR INDIRECT, CONSEQUENTIAL, INCIDENTAL DAMAGES OF ANY KIND, INCLUDING ANY TRAFFIC ACCIDENT, ARISING OUT OF YOUR FAILURE TO FOLLOW THE FOREGOING INSTRUCTIONS

To calibrate the AutoVu™ navigation hardware:

1. From the **Calibration** window, select if the odometry signal comes from the tire tags or from the vehicle pulse (VSS or magneto kit). Read the warning that appears and click **I accept these terms** to be able to start the calibration process.
2. Click **Start calibration**.

   This procedure is designed to be performed with minimal need to touch the screen. The instructions are read out loud and a sound signal indicates when to switch to the next step. It is recommended that you perform this operation with a co-driver and ensure that all necessary safety precautions are taken. The following conditions must be met for the calibration to start:

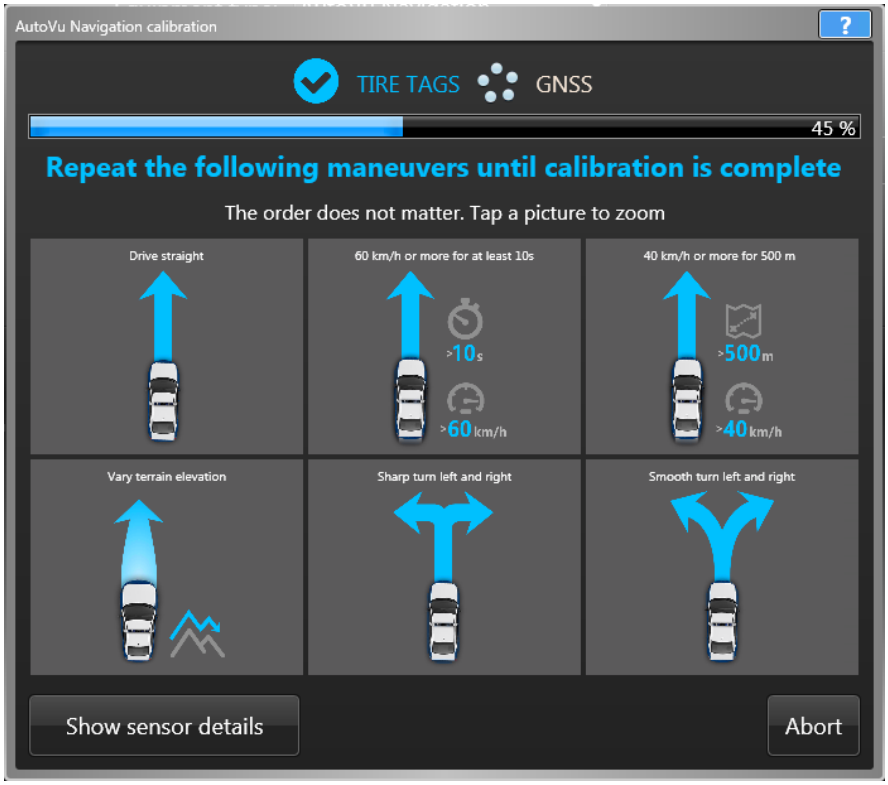
   - The antenna can receive the GNSS signal. If the vehicle is inside a garage, move it to a clear sky area before starting the calibration process.
   - The vehicle engine is running and the transmission is in Park.
   - The LPR Processing Unit is powered up.

3. Follow the instructions on the screen for a step-by-step description of the calibration maneuvers. Execute the maneuvers until the window changes to the next step or until the *Calibration completed* screen appears. You can abort the procedure and start over at any time.

   The following instructions will appear for a tire tags calibration:

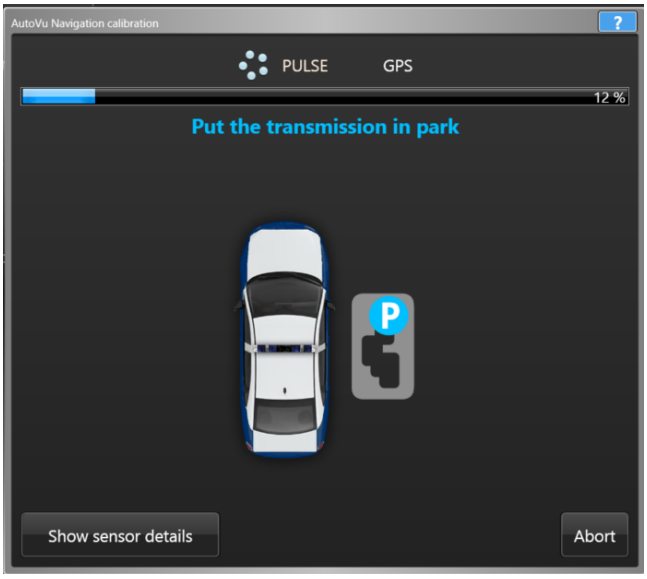
   - **Drive forward at low speed:** Drive slowly forward until you hear the sound signal and the next screen appear. Make sure that you do not go faster than the indicated speed.

- **Drive forward at 50 km/h:** Drive forward at a speed of 50 km/h (30 mph) until you hear the sound signal and the next screen appears. This step can take time. It is important to continue until the step is completed.
- **Miscellaneous maneuvers:** Execute the six maneuvers on the screen in any order. There will be no prompt to go to the next one and no sound signal. You can tap an image to zoom in and see it better. Tap again to restore the view. If you have completed the six maneuvers and the sensors are still not calibrated, do all the six maneuvers again, in any order. To save time, you can combine maneuvers. For example, you can drive straight on a small slope, combining two maneuvers into one. Drive until the *Calibration completed* screen appears.



The following instructions will appear for a pulse calibration:

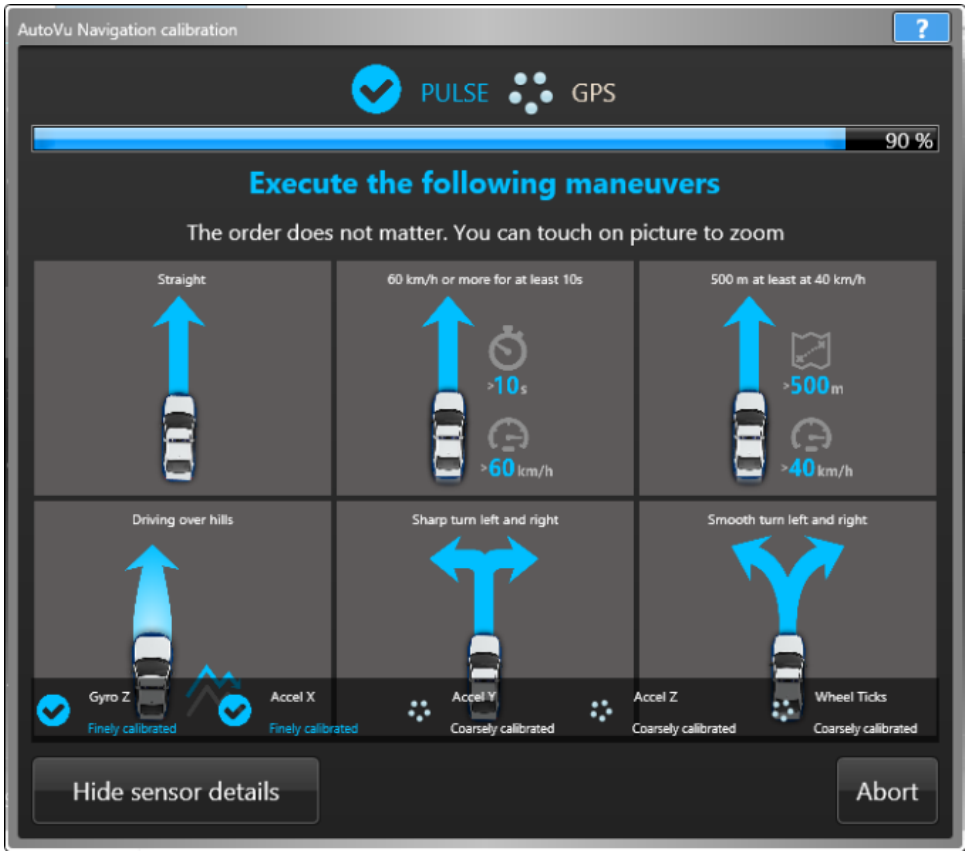
- **Put the vehicle to park:** Stop the vehicle and put the transmission in Park until you hear the sound signal and the next screen appears.
- **Put the transmission in reverse:** No need to drive backward. Put the transmission gear in reverse until you hear the sound signal and the next screen appears.
- **Put the vehicle to park:** Stop the vehicle and put the transmission in Park until you hear the sound signal and the next screen appears.



- **Drive forward at low speed:** Drive slowly forward until you hear the sound signal and the next screen appear. Make sure that you do not go faster than the indicated speed.
- **Drive forward at 50 km/h:** Drive forward at a speed of 50 km/h (30 mph) until you hear the sound signal and the next screen appears. This step can take time. It is important to continue until the step is completed.
- **Miscellaneous maneuvers:** Execute the six maneuvers on the screen in any order. There will be no prompt to go to the next one and no sound signal. You can tap an image to zoom in and see it better. Tap again to restore the view. If you have completed the six maneuvers and the sensors are still not calibrated, do all the six maneuvers again, in any order. To save time, you can combine maneuvers. For example, you can drive straight on a small slope, combining two maneuvers into one. Drive until the *Calibration completed* screen appears.

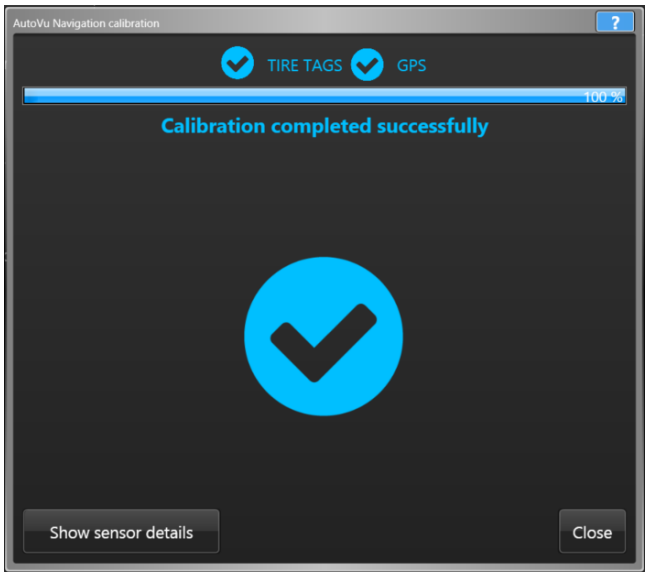
The calibration procedure may take time as a large number of samples are required for the wheel sensors to function correctly. Keep driving the vehicle until the calibration completed screen appears.

4 Click **Show sensor details** anytime during calibration to view the status of individual sensors:



- **Gyro Z:** Measures the angular rotational velocity, or rotation speed, that determines the orientation of the vehicle.
- **Accel X:** Measures the acceleration in the direction of travel (forward, backward)
- **Accel Y:** Measures the acceleration perpendicular to the direction of travel (sideways).
- **Accel Z:** Measures the acceleration up and down.
- **Wheel ticks:** Measures the wheel rotation speed.

5 Click **Close** in the *Calibration completed* screen to conclude calibration.



NOTE: If a problem occurs with the navigation system, you can enable verbose logs to help Technical Support understand the situation. Go to the *Advanced* page in the *Traces* section and put the **Navigation diagnostic logs** to **verbose**. Do not forget to turn it back off as it can take a lot of hard disk space. You can click **Abort** at any time to cancel the calibration procedure.

The AutoVu navigation is calibrated.

After you finish

If you change the position of the GNSS antenna or the LPR Processing Unit, you must modify the layout accordingly and recalibrate the system.

Enabling Patroller Map settings

If you're using Patroller with maps, you must select the Patroller mapping option to use, and configure the related settings.

Before you begin

If you're using maps, you must install the BeNomad files, Patroller's mapping solution.

To enable Patroller Map settings:

1 Open Patroller Config Tool.
2 Go to **Navigation** > **Maps**.
3 From **Mapping type**, select **BeNomad**.
The default map type for AutoVu™.
4 Configure the following settings:
- **Show vehicle route:** Displays a trail behind the Patroller icon that allows you to see the route Patroller has taken. Turn this setting off to show only the Patroller's current position.
- **Show parking lots overlay:** Turn on to display configured parking lots on the map in the Patroller main viewer.
- **Snap to road threshold:** Specify the maximum distance error (in meters). If the distance between the vehicle and the closest map item is greater than this value, no snapping will occur.

5 Click **Apply**.

Patroller mapping settings are configured.

Installing the GPS driver on the Patroller computer

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.

To install the GPS driver:

1 On the in-vehicle computer, open Windows Device Manager.
   a) Right-click **My Computer**.
   b) Select **Manage**.
   c) Select **Device Manager**.
2 Expand the **Ports** menu.
3 Right-click the u-blox 5 GPS Receiver port and select **Update Driver**.
4 In the Hardware Update Wizard, select **Install from a list or specific location (Advanced)**.
5 In the following window, select the **Don't search. I will choose the driver to install** option and click Next.
6 Click **Have Disk** in the next window.
7 Retrieve the new driver on the installation CD, and click **OK.**

8 Click **Finish** to complete the installation of the new GPS driver.

After you finish

If you're using the USB GPS receiver provided by Genetec, you also need to change the baud rate of the device to 4800.

Configuring New Wanted Patroller options

After you have created the *New wanted* attributes and categories, and they have been pushed to Patroller, you need to configure them in Patroller Config Tool.

To configure New Wanted Patroller options:

1 Open Patroller Config Tool.

2 Go to **Operation** > **Hotlists**, turn on **Enable new wanted**, and then configure the following settings as needed:

- **Enable new wanted management:** Turn on to allow Patroller users to edit and delete *New wanted* entries from the database.
- **Enable comments for new wanted:** Turn on to activate a text box where you can enter a comment when entering a *New wanted* hotlist item.
- **New wanted expiry options (in days):** Select one or more expiration options for New Wanted entries.

3 Click **Apply**.

Patroller users can now add and manage (if enabled) *New wanted* entries.

Turning on Simplematcher in Patroller

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

Before you begin

You'll also need to configure the LPR matcher to turn off OCR equivalence. This will ensure that you don't get too many false positive hits.

What you should know

When **Use Simple Matcher** is not enabled in the Patroller Config Tool, the Patroller will automatically use the simple matcher by default if the number of entries in the plate list exceeds two million entries. When this is the case, common and contiguous characters "fuzzy matching" is not available.

To turn on Simplematcher:

1 Open Patroller Config Tool.

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

3 Click **Apply**.

After you finish

Turn off OCR equivalence in the LPR matcher. For more information about configuring LPR matcher settings, see the *Security Center Administrator Guide*

Configuring hotlist settings

The hotlist settings in Patroller Config Tool determine how the hotlists are used and what is the Patroller behavior with different hotlist options.

To configure hotlist settings:

1 Open Patroller Config Tool.

2 Go to **Operation** > **Hotlists**.

3 Configure the following options:

- **Allow consecutive hits:** Turn on to allow sequential hits for the same plate. For example, if you capture a plate that raises a hit, and then capture the same plate again, it will raise another hit.

  NOTE: If you turn this setting off, Patroller would need to capture a new plate before allowing a hit for the same plate.

- **Enable new wanted:** Turn on to allow Patroller users to add New wanted hotlist entries.
- **Enable new wanted management:** Turn on to allow Patroller users to edit and delete New wanted entries from the database.
- **Enable comments for new wanted:** Turn on to activate a text box in Patroller where you can enter a comment when entering a New wanted hotlist item.
- **New wanted expiry options (days):** Create the expiry options available to the Patroller user when adding a New wanted entry.

  For example, let's say you create the options 1, 5, and 10. When you add a New wanted entry, you'll be able to choose for that entry to expire in 1, 5, or 10 days. If you don't provide an expiration option, New wanted entries will remain in the Patroller database indefinitely.

- **Add expiration option ( ):** Enter an expiration option (in days). Maximum value is 100.
- **Delete expiration option ( ):** Delete an existing expiration option.
- **Enable Selectable hotlist:** Turn on to allow Patroller users to select which hotlists among those available on the Patroller are used to generate Hits.
- **Enable past read matching:** Turn on to compare reads from the past with a new hotlist, or new wanted plates that have been manually added.
- **Past read matching look back:** Enter how long in hours you would like Patroller to look back in the database for reads that match a new hotlist, or new wanted entry.
- **Bypass hit enforcement:** Turn on to bypass the additional step of enforcing a hit after accepting it. When turned on, Patroller assumes you enforced the hit, and will not display the Enforced/Not enforced prompt.
- **Auto-enforce hotlist hits:** Turn on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction.

  NOTE: If you have configured "Hit accept" or "Hit reject reasons", they are ignored when this setting is on.

- **Display hits by priority:** Turn on to display hits in Patroller by the priority you specified in Security CenterConfig Tool.

  For example, if you have set "Hotlist A" to a higher priority than "Hotlist B", hits generated from Hotlist A will be displayed first (on the right of the Patroller scrollbar).

- **Use simple matcher:** Turn on Simplematcher when using very large hotlists with millions of entries. You'll also need to turn off OCR equivalence in the LPR matcher. For more information about configuring LPR matcher settings, see the *Security Center Administrator Guide*.

4 Click **Apply**.

Permits and shared permits are now enabled and configured in Patroller.

Configuring overtime settings in Patroller

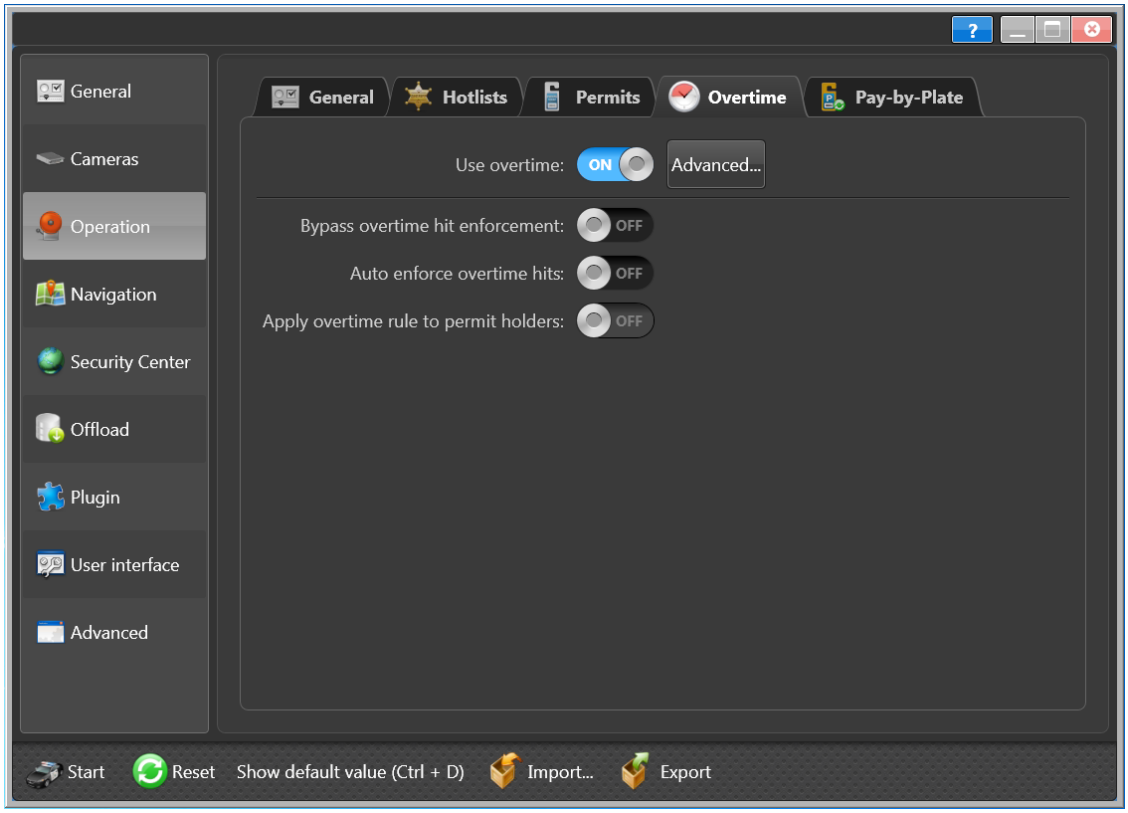
To use overtime rules in City and University parking enforcement, you need to enable overtime and configure the overtime settings in Patroller Config Tool.

To configure overtime settings:

1 Open Patroller Config Tool.

2 Go to **Operation** > **Overtime**.

NOTE: The *Overtime* page is for a City Parking Enforcement system. It includes all the possible overtime configuration options.

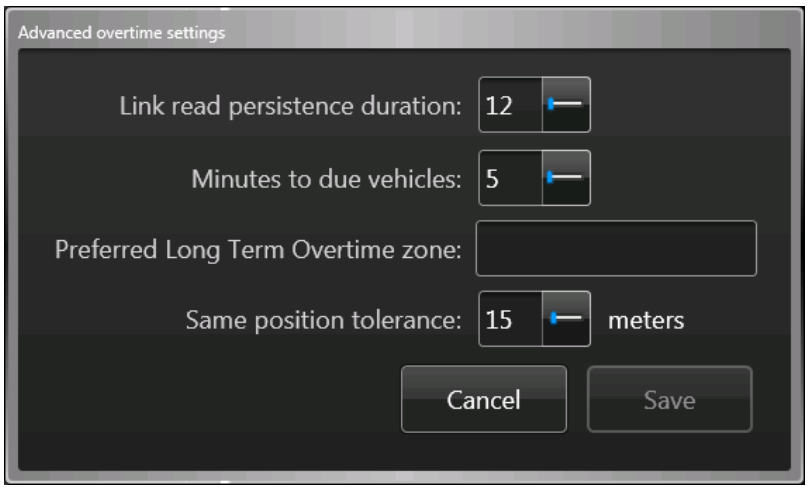


3 Turn on **Use overtime**, then configure the following:

- **Bypass hit enforcement:** Turn this off if you want Patroller users to indicate whether or not they enforced the hit after accepting it. Turn it on to bypass enforcement. When turned on, Patroller automatically enforces hits after they are accepted.
- **Auto enforce overtime hits:** Turn this on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction. Hit accept and hit reject surveys are ignored when this option is enabled.
- **Apply overtime rule to permit holders:** Turn this on for locations where parking access can be bought for a limited period. In this configuration, if a plate is read once and is not on the selected permit list, a Hit will be generated. However, if it is on the list, no Hit will be generated on the first read. The second Read will determine if the time limit is exceeded and if a Hit is generated. If this option is disabled, permit holders do not generate violations.

4 Click **Advanced**.

The *Advanced overtime settings* window appears.



5 From the *Advanced overtime settings* window, configure the following:

- **Link read persistence duration:** Enter the amount of time that a plate read stored in the Patroller database is considered to be a “time 1” read for a particular overtime rule.

  NOTE: When using Overtime Rule Regulation with time range and a link persistence over 24hours, overtime hit will not raise on different days.
- **Minutes to due vehicles:** Enter the amount of time before the vehicles are due for enforcement. This value determines the **Show Due** functionality in Patroller. The default value is 5 minutes.
- **Preferred Long Term Overtime zone:** If you have more than one Long Term Overtime zone configured in Security Center, you must type the name of the zone you want Patroller to display, because you can only enforce one zone at a time. This value is not case sensitive.
- **Same position tolerance:** This is a buffer used for “Same position” overtime rules. It is the distance that Patroller considers to be a single position or parking space.

6 Click **Save**.

7 Click **Apply**.

Overtime rules are now enabled and configured in Patroller.

After you finish

If you are using tire images, configure the wheel imaging settings.

Configuring Pay-by-Plate settings

To use Pay-by-Plate in City and University parking enforcement, you need to enable it and configure the settings in Patroller Config Tool.

What you should know

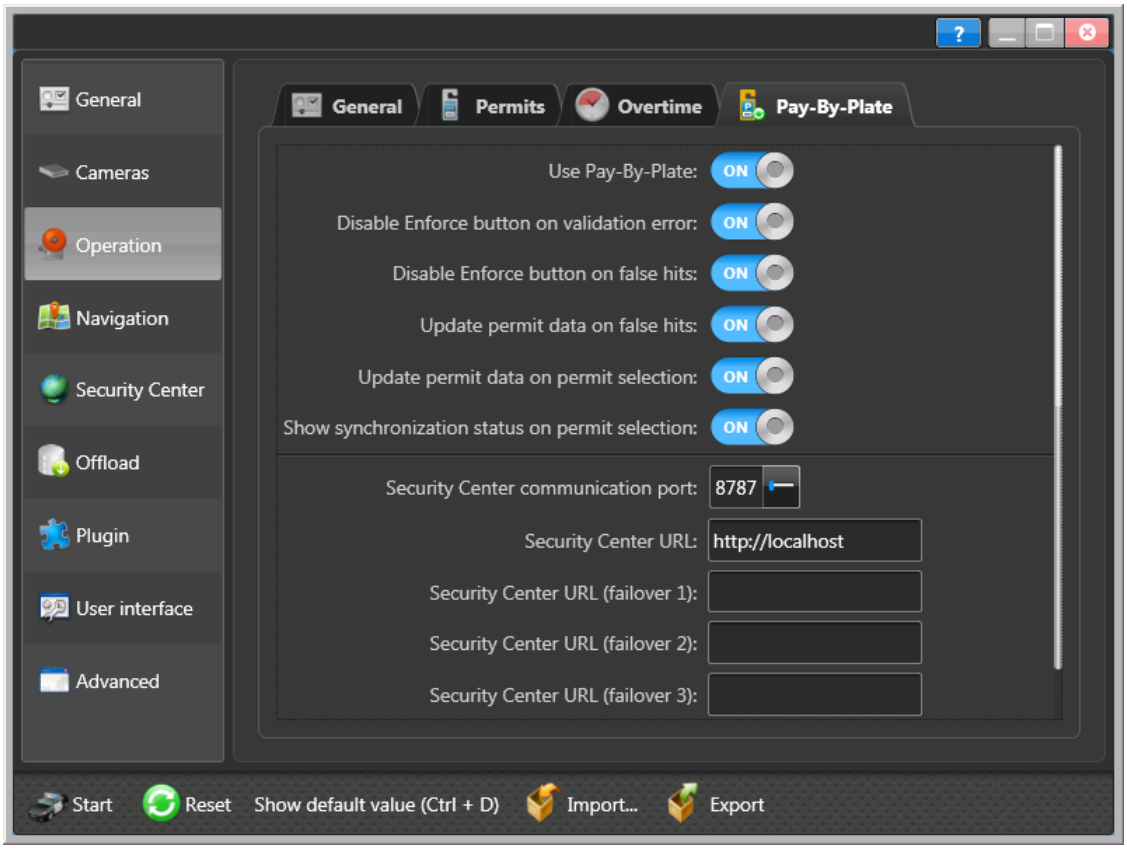
For complete details about installing the Pay-by-Plate plugin, licensing information, and how to configure it in Security Center, please see the *Pay-by-Plate Sync Plugin Guide*.

Prior to Patroller 6.1, Pay-by-Plate was installed as a plugin for Patroller. If the Pay-by-Plate plugin was previously installed and enabled prior to upgrading to Patroller 6.1 or later, Pay-by-Plate is automatically enabled on the Pay-by-Plate tab of the Operations page. Your configured settings are preserved, and the *Plate copy* and *Hit export* plugins are are activated by default on the Plugin page.

To configure Pay-by-Plate settings:

1 Open Patroller Config Tool.

2 Go to **Operation** > **Pay-by-Plate**.



3 Configure the following options:

- **Use Pay-by-Plate:** Turn ON to enable Pay-by-Plate plugin.
- **Disable Enforce button on validation error:**
  - **ON:** Disables Patroller's Enforce button if there is a communication error that prevents Live Infraction Validation from validating the hit.
  - **OFF:** Does not disable enforcement if there is a validation error.

  The option **Disable Enforce button on false hits** supersedes this option. If you allow enforcement of false hits, this option has no effect.

- **Disable Enforce button on false hits:**
  - **ON:** Disables Patroller's *Enforce* button if Live Infraction Validation confirms the captured plate is valid and is in the provider's system (false hit).
  - **OFF:** You will receive a message informing you that the hit is invalid, but you will be allowed to enforce it if you choose.
- **Update permit data on false hits:**
  - **ON:** Updates your selected permit list if the Live Infraction Validation confirms the captured plate is valid and is in the provider's system (false hit).
  - **OFF:** You will need to update your permits manually by re-selecting your permits in Patroller.
- **Update permit data on permit selections:**
  - **ON:** When you select a permit to enforce in Patroller, the permit is automatically updated with the latest information from the parking provider's system.
  - **OFF:** Permits are only updated when Security Center gets new information from the parking provider, and then updates Patroller using Periodic Transfer (which should be set to one minute). **NOTE:** If you turn this setting off, you cannot have permit updates set to "0" in Security Center Config Tool. Doing so would disable automatic updating of permits.
- **Show synchronization status on permit selection:**
  - **ON:** Displays a popup window after you select a permit that shows the synchronization status between Patroller and Security Center.
  - **OFF:** The popup window is not displayed.
    IMPORTANT: If you turn this setting off, synchronization will still occur if the Update permit data on permit selections option is enabled. However, you will not know when synchronization is complete, or if there were any errors. It is recommended that you leave this setting on at all times.
- **Security Center communication port:** Enter the port number to use for connecting to the Security Center Pay-by-Plate plugin role (8787 is the default). This must match the port entered in Security Center Config Tool for the setting: **Patroller communication port**.
- **Security Center URL:** Type the IP address (in the form of a URL) to connect to the Security Center Pay-by-Plate Sync plugin role. For example, if you want to connect to IP address 123.456.78.9, you must type the full address as http://123.456.78.9.

  IMPORTANT: Do not include a trailing slash after the IP address.
- **Security Center URL (failover 1):** If you have failover configured for the Pay-by-Plate sync plugin role, enter the IP address (in the form of a URL) of the first failover server.
- **Security Center URL (failover 2):** If you have failover configured for the Pay-by-Plate sync plugin role, enter the IP address (in the form of a URL) of the second failover server.
- **Security Center URL (failover 3):** If you have failover configured for the Pay-by-Plate Sync plugin role, enter the IP address (in the form of a URL) of the third failover server.
- **Communication timeout (seconds):** Enter how long (in seconds) before a communication request between Patroller and Security Center times out.

4 Click **Apply**.

Permits and shared permits are now enabled and configured in Patroller.

Measuring the Tire cam-to-plate distance in Patroller

To determine when Patroller should start grabbing wheel images from the wheel imaging camera, you must measure the distance between the tire camera and the license plate. You need to be in the Patroller vehicle and parked next to a “target” vehicle to perform this procedure.

Before you begin

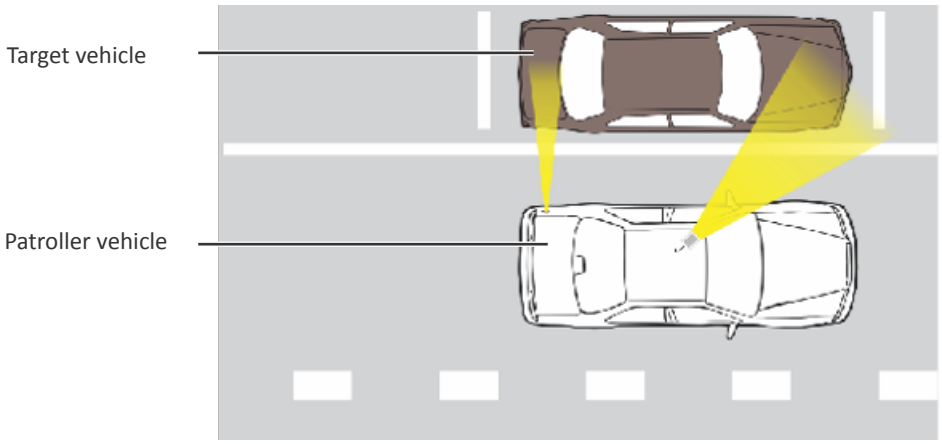
Patroller must be installed on the in-vehicle computer, and you must have a tape measure available.

What you should know

This procedure is the same for parallel or 45-degree parking, but the distance is less for 45- degree parking because of the parked vehicle’s angle.

To measure Tire cam-to-plate distance:

1 Park the Patroller vehicle next to the target vehicle. Keep the engine running.



2 Start Patroller, then tap **Video**.

The video window appears showing the available Sharps and tire cameras.

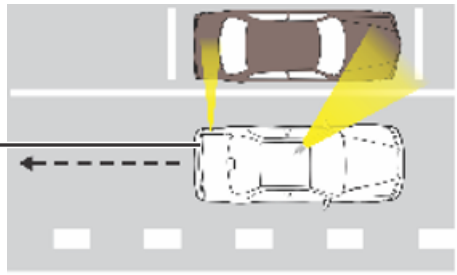
3 Select the camera (if you have more than one) aimed at the target vehicle, then tap LPR to see the LPR camera’s feed

The LPR camera’s video feed appears.

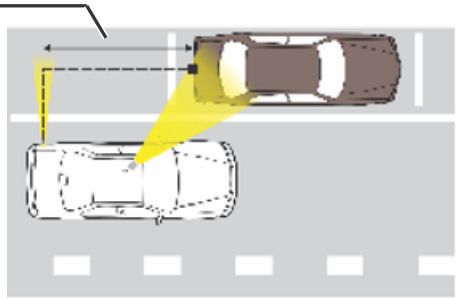
4 Put the Patroller vehicle in reverse, then slowly back up until you see the target vehicle’s entire plate in the LPR video feed. Stop the vehicle.

5 Using your tape measure, measure the **parallel** distance (in meters) from the wheel imaging camera’s field of view to the target vehicle’s license plate.

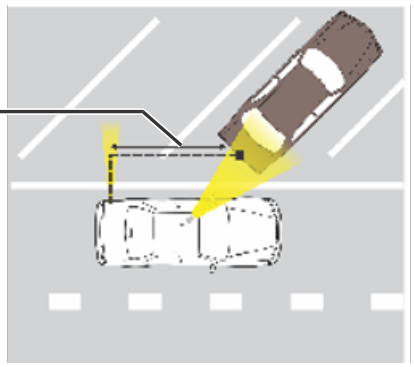
Slowly back up the Patroller vehicle.



When the entire plate is visible, measure the parallel distance to the tire camera.



For 45-degree angled parking, the distance is less because of the parked vehicle's angle.



6 Write down the distance you measured.

After you finish

You will need to enter the distance in Patroller Config Tool. The distance is used by Patroller to know when to start grabbing tire images after a plate read.

Related Topics

Configuring wheel imaging settings in Patroller on page 65

Configuring wheel imaging settings in Patroller

You can enter the required settings for Patroller to know when to grab wheel images from the tire cameras.

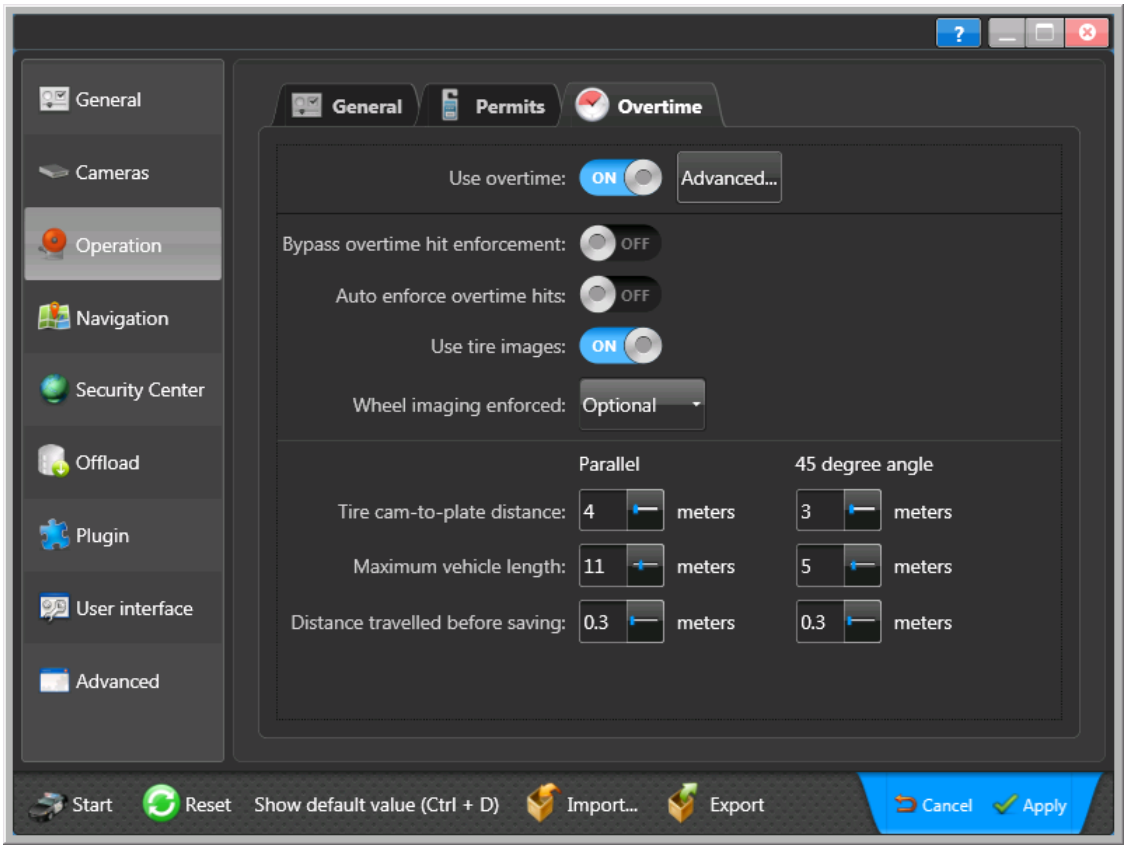
Before you begin

Measure the Tire cam-to-plate distance because this measurement is requirement for this procedure.

To configure wheel imaging settings:

1 Open Patroller Config Tool .

2 Go to **Operation** > **Overtime**, turn on **Use overtime**, then turn on **Use tire images**.



The *Overtime* page appears with the wheel imaging settings displayed.

3 Configure the following:

NOTE: You should only need to modify the *Tire cam-to-plate distance* parameter. The other settings should be adequate for any parking enforcement scenario.

- **Wheel imaging enforced:** Select **Mandatory** or **Optional** from the drop-down list. If you select optional, Patroller users can enforce a hit without confirming wheel images.
- **Tire cam-to-plate distance:** This distance tells Patroller how far to travel (after the initial plate read) before it starts grabbing wheel images.
- **Maximum vehicle length:** Patroller will stop grabbing wheel images after it has travelled the Tire cam-to-plate distance + Maximum vehicle length.

  TIP: The distance you enter should be based on the general size of the vehicles in your patrol area. For example, vehicles in Europe tend to be smaller than in the United States.

- **Distance travelled before saving:** When grabbing wheel images, this distance tells Patroller how often to grab an image. For example, the default 0.3 meters means that an image is grabbed every 30 centimeters.

4 Click **Apply**.
Wheel imaging calibration is now complete.

Example

Here is an example of how all these settings work together:

1 The Sharp reads a parked vehicle's plate.
2 After the Patroller vehicle travels 4 meters (if **Tire cam-to-plate distance** = 4), Patroller starts grabbing wheel images from the tire camera.
3 Patroller grabs an image every 0.3 meters (if Distance travelled before saving = 0.3).
4 Patroller keeps grabbing images until it travels 11 meters (if Maximum vehicle length = 11) past the initial read.

After you finish

Perform a road test to ensure that the wheel imaging configuration provides the expected results.

Related Topics
Measuring the Tire cam-to-plate distance in Patroller on page 63

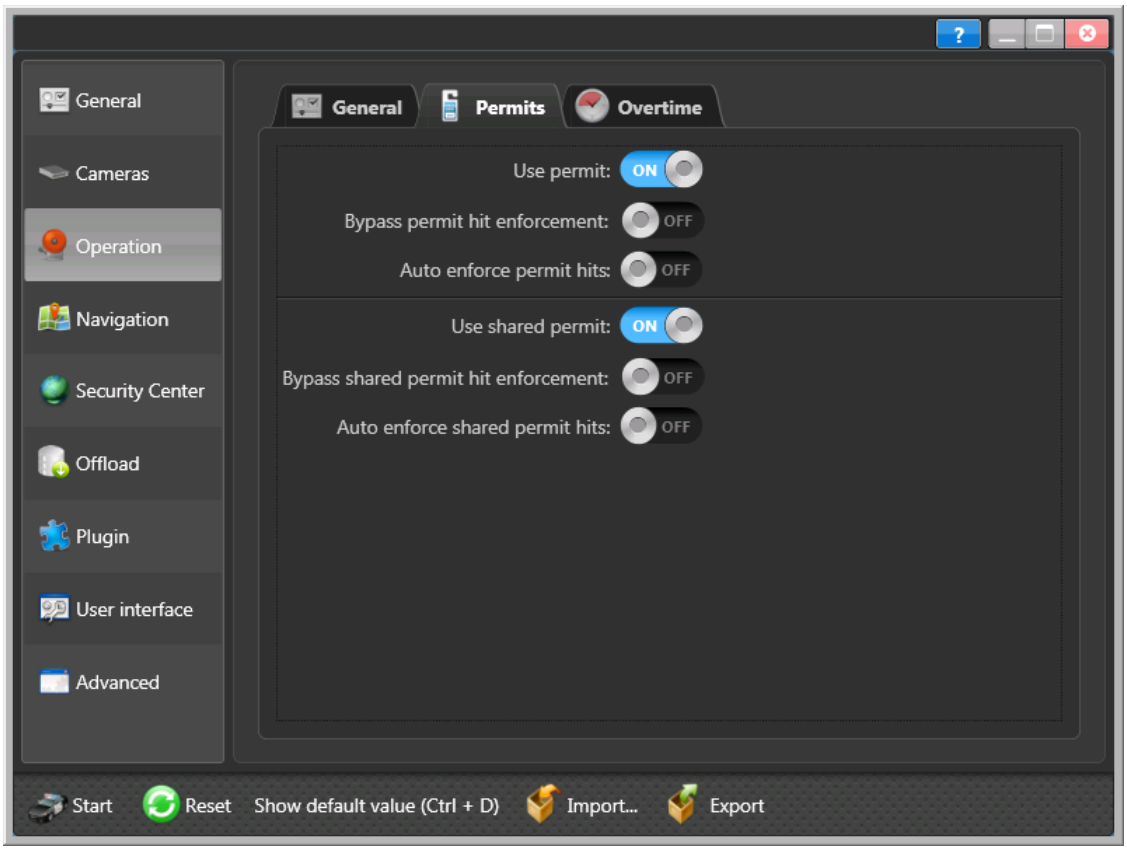
Configuring permit settings in Patroller

To use permits and shared permits for City and University parking enforcement, permits need to be enabled and configured in Patroller Config Tool.

To configure permit settings:

1 Open Patroller Config Tool.

2 Go to **Operation** > **Permits**.



3 Turn on **Use permit**, then configure the following:

- **Bypass permit hit enforcement:** Turn this off if you want Patroller users to indicate whether or not they enforced the hit after accepting it. Turn it on to bypass enforcement. When turned on, Patroller automatically enforces hits after they are accepted.
- **Auto enforce permit hits:** Turn this on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction. If you've configured a hit accept or hit reject survey, it is ignored when this option is enabled.

4 Turn on **Use shared permit** (if you're using them), then configure the following:

- **Bypass shared permit hit enforcement:** Turn this off if you want Patroller users to indicate whether or not they enforced the hit after accepting it. Turn it on to bypass enforcement. When turned on, Patroller automatically enforces hits after they are accepted.
- **Auto enforce shared permit hits:** Turn this on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction. If you've configured a hit accept or hit reject survey, it is ignored when this option is enabled.

5 Click **Apply**.

Permits and shared permits are now enabled and configured in Patroller.

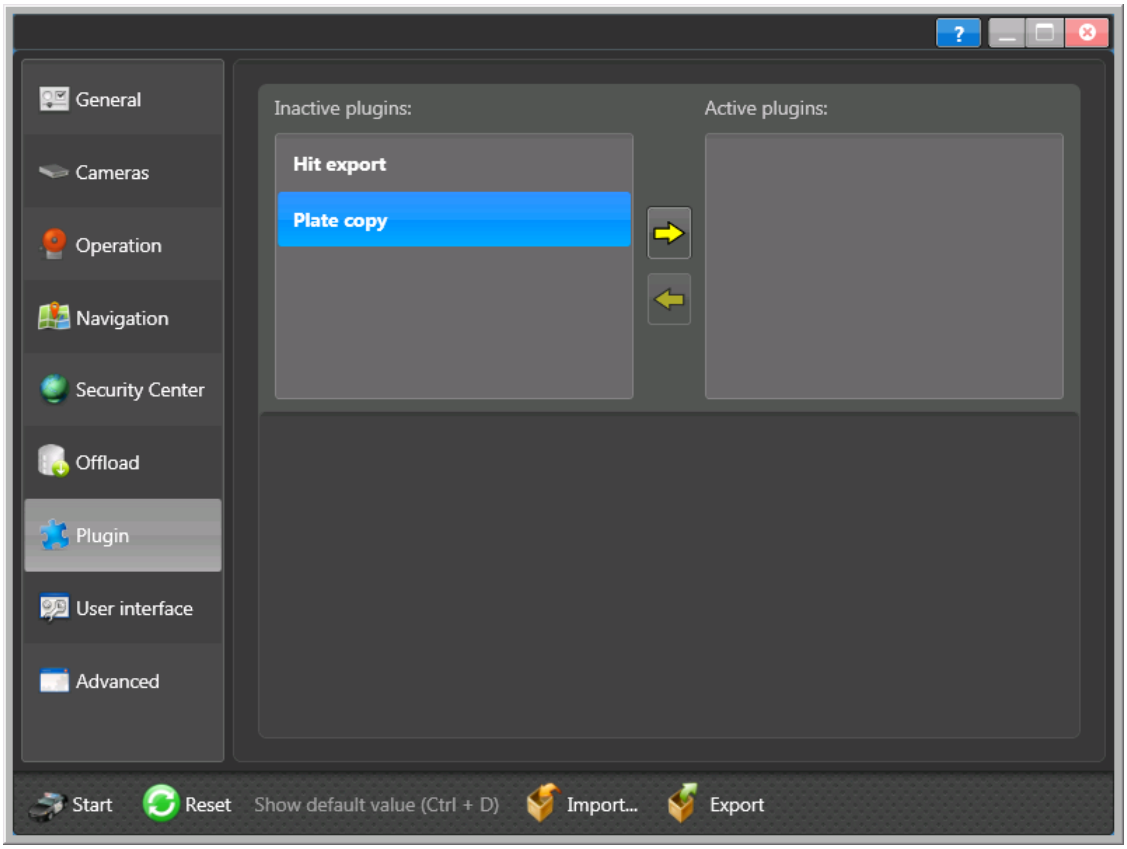
Activating plugins in Patroller

To use AutoVu plugins such as *Hit export* and *Plate copy*, you need to activate them in Patroller Config Tool.

To activate a plugin:

1 Open Patroller Config Tool.

2 Click **Plugin**.



3 Under **Inactive plugins**, select the plugins you want to activate then click the **Activate Selected plugins** icon. You can activate multiple plugins at the same time.

The selected plugins will move to the **Active plugins** list. You can deactivate a plugin at any time by selecting it from the **Active plugins** list and clicking the **Deactivate selected plugins** icon.

IMPORTANT: The *Hit export* and the *Plate copy* plugin can be activated at the same time. The other plugins were not designed to be used with certain plugins, and may cause unwanted behavior.

4 Click **Apply**.

After you finish

Configure the plugin settings.

About the Hit export XML template in Patroller

The Hit export plugin can be configured to create an XML file when you accept or enforce a permit hit in Patroller. This section enables you to view an example of the default XML template, learn what the fields in the template mean, and to view an example of what your final output should look like.

What you should know

- When data is not available from a hit, the field information is replaced by an empty string in the output file. For example, on a regular hit (no overtime) all the overtime fields are removed and no values are output.
- Date and time formats can be added between curly brackets ({}) to the following time fields:
  - TimeStamp
  - TimeStampUTC
  - OvertimeTimeStamp
  - OvertimeTimeStampUTC

  For example, if you want the **TimeStamp** field to output the date (Month, Day, Year) and a 24 hour time format, you would enter **%TimeStamp%{MM/dd/yyyy HH:mm:ss}**. For more information about supported date and time format strings, click here.

Hit export XML template example

Following is an example of the default *HitExportTemplate.XML* located at:

C:\Program Files (x86)\Genetec AutoVu 6.3\MobileClient\TemplateFiles.

IMPORTANT: The default template provides a sample of the available tags and is subject to change. Do not use it as is. Create instead your own template by renaming or creating a copy of the default file.

```
<?xml version="1.0" encoding="utf-8" ?>
<!--
      !!!!!!!!!!!!!!!!!!!!!!!!!!!! IMPORTANT !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
      This file is a sample of the available tags that you can use when creating a
      template. Do not create a dependency on this file for it is subject to change.

      Instead, you must create a copy of this sample and use it for your own purposes.
      !!!!!!!!!!!!!!!!!!!!!!!!!!!! IMPORTANT !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  -->

<Enforce>

  <!--
    ***************************************************************************
    NEW

    The following section describes the supported tags using the new format.

    ***************************************************************************
  -->
  <IsPlateExpired>#ISPLATEEXPIRED#</IsPlateExpired>
  <IsPayZone>#ISPAYZONE#</IsPayZone>
  <PlateStatus>#PLATESTATUS#</PlateStatus>

  <HitId>#HIT_ID#</HitId>
  <HitType>#HIT_TYPE#</HitType>
  <UserAction>#USER_ACTION#</UserAction>

  <ReadId>#READ_ID#</ReadId>
  <PlateRead>#PLATE_READ#</PlateRead>
  <PlateState>#PLATE_STATE#</PlateState>
  <ReadType>#READTYPE#</ReadType>
  <PermitName>#PERMIT_NAME#</PermitName>
  <RuleId>#RULE_ID#</RuleId>
  <RuleName>#RULE_NAME#</RuleName>
  <UnitName>#UNIT_NAME#</UnitName>
  <UnitId>#UNIT_ID#</UnitId>
  <UserName>#USER_NAME#</UserName>
  <UserLogin>#USER_LOGIN#</UserLogin>
  <UserId>#USERId#</UserId>
  <PermitId>#PERMIT_ID#</PermitId>
  <ParkingPermitId>#PARKING_PERMIT_ID#</ParkingPermitId>
  <Longitude>#LONGITUDE#</Longitude>
  <Latitude>#LATITUDE#</Latitude>
  <LprImagePath>#PLATE_IMAGE#</LprImagePath>
  <ContextImagePath>#CONTEXT_IMAGE#</ContextImagePath>
  <TireImagePath>#TIRE_IMAGE#</TireImagePath>
  <TimeStamp>#DATE_LOCAL#{yyyy-MM-dd} #TIME_LOCAL#{HH:mm:ss}</TimeStamp>
  <TimeStampUTC>#DATE_UTC#{yyyy-MM-dd} #TIME_UTC#{HH:mm:ss}</TimeStampUTC>

  <OvertimeVehicleId>#OVERTIME_READ_ID#</OvertimeVehicleId>
  <OvertimePlateRead>#OVERTIME_PLATE_READ#</OvertimePlateRead>
  <OvertimePlateState>#OVERTIME_PLATE_State#</OvertimePlateState>
  <OvertimeReadType>#OVERTIME_READTYPE#</OvertimeReadType>
  <OvertimePermitName>#OVERTIME_PERMIT_NAME#</OvertimePermitName>
```

```
<OvertimeRuleId>#OVERTIME_RULE_ID#</OvertimeRuleId>
<OvertimeRuleName>#OVERTIME_RULE_NAME#</OvertimeRuleName>
<OvertimeUnitName>#OVERTIME_UNIT_NAME#</OvertimeUnitName>
<OvertimeUnitId>#OVERTIME_UNIT_ID#</OvertimeUnitId>
<OvertimeUserName>#OVERTIME_USER_NAME#</OvertimeUserName>
<OvertimeUserLogin>#OVERTIME_USER_LOGIN#</OvertimeUserLogin>
<OvertimeUserId>#OVERTIME_USER_ID#</OvertimeUserId>
<OvertimePermitId>#OVERTIME_PERMIT_ID#</OvertimePermitId>
<OvertimeLongitude>#OVERTIME_LONGITUDE#</OvertimeLongitude>
<OvertimeLatitude>#OVERTIME_LATITUDE#</OvertimeLatitude>
<OvertimeLprImagePath>#OVERTIME_PLATE_IMAGE#</OvertimeLprImagePath>
<OvertimeContextImagePath>#OVERTIME_CONTEXT_IMAGE#</OvertimeContextImagePath>
<OvertimeTireImagePath>#OVERTIME_TIRE_IMAGE#</OvertimeTireImagePath>
<OvertimeTimeStamp>#OVERTIME_DATE_LOCAL#{yyyy-MM-dd} #OVERTIME_TIME_LOCAL#{HH:mm:ss}</OvertimeTimeStamp>
<OvertimeTimeStampUTC>#OVERTIME_DATE_UTC#{yyyy-MM-dd} #OVERTIME_TIME_UTC#{HH:mm:ss}</OvertimeTimeStampUTC>

<OvertimeElapseMinutes>#OVERTIME_ELAPSEMINUTES#</OvertimeElapseMinutes>
<OvertimeElapseSeconds>#OVERTIME_ELAPSESECONDS#</OvertimeElapseSeconds>
<OvertimeElapseHours>#OVERTIME_ELAPSEHOURS#</OvertimeElapseHours>

<!--
  ************************************************************************
  LEGACY

  The following section describes the supported tags using the legacy format.
  It can still be used but they have been deprecated since Patroller 6.2.

  ************************************************************************
-->
<IsPlateExpired>%IsPlateExpired%</IsPlateExpired>
<IsPayZone>%IsPayZone%</IsPayZone>
<PlateStatus>%PlateStatus%</PlateStatus>

<HitId>%HitId%</HitId>
<HitType>%HitType%</HitType>
<UserAction>%UserAction%</UserAction>

<VehicleId>%VehicleId%</VehicleId>
<Plate>%Plate%</Plate>
<State>%State%</State>
<ReadType>%ReadType%</ReadType>
<PermitName>%PermitName%</PermitName>
<ZoneName>%ZoneName%</ZoneName>
<UnitName>%UnitName%</UnitName>
<UnitId>%UnitId%</UnitId>
<UserName>%UserName%</UserName>
<UserLogin>%UserLogin%</UserLogin>
<UserId>%UserId%</UserId>
<PermitId>%PermitId%</PermitId>
<ParkingPermitId>%ParkingPermitId%</ParkingPermitId>
<ZoneId>%ZoneId%</ZoneId>
<GpsX>%GpsX%</GpsX>
<GpsY>%GpsY%</GpsY>
<LprImagePath>%LprImagePath%</LprImagePath>
```

```
  <ContextImagePath>%ContextImagePath%</ContextImagePath>
  <TireImagePath>%TireImagePath%</TireImagePath>
  <TimeStamp>%TimeStamp%</TimeStamp>
  <TimeStampUTC>%TimeStampUTC%</TimeStampUTC>

  <OvertimeVehicleId>%OvertimeVehicleId%</OvertimeVehicleId>
  <OvertimePlate>%OvertimePlate%</OvertimePlate>
  <OvertimeState>%OvertimeState%</OvertimeState>
  <OvertimeReadType>%OvertimeReadType%</OvertimeReadType>
  <OvertimePermitName>%OvertimePermitName%</OvertimePermitName>
  <OvertimeZoneName>%OvertimeZoneName%</OvertimeZoneName>
  <OvertimeUnitName>%OvertimeUnitName%</OvertimeUnitName>
  <OvertimeUnitId>%OvertimeUnitId%</OvertimeUnitId>
  <OvertimeUserName>%OvertimeUserName%</OvertimeUserName>
  <OvertimeUserLogin>%OvertimeUserLogin%</OvertimeUserLogin>
  <OvertimeUserId>%OvertimeUserId%</OvertimeUserId>
  <OvertimePermitId>%OvertimePermitId%</OvertimePermitId>
  <OvertimeZoneId>%OvertimeZoneId%</OvertimeZoneId>
  <OvertimeGpsX>%OvertimeGpsX%</OvertimeGpsX>
  <OvertimeGpsY>%OvertimeGpsY%</OvertimeGpsY>
  <OvertimeLprImagePath>%OvertimeLprImagePath%</OvertimeLprImagePath>
  <OvertimeContextImagePath>%OvertimeContextImagePath%</OvertimeContextImagePath>
  <OvertimeTireImagePath>%OvertimeTireImagePath%</OvertimeTireImagePath>
  <OvertimeTimeStamp>%OvertimeTimeStamp%</OvertimeTimeStamp>
  <OvertimeTimeStampUTC>%OvertimeTimeStampUTC%</OvertimeTimeStampUTC>

  <OvertimeElapseMinutes>%OvertimeElapseMinutes%</OvertimeElapseMinutes>
  <OvertimeElapseSeconds>%OvertimeElapseSeconds%</OvertimeElapseSeconds>
  <OvertimeElapseHours>%OvertimeElapseHours%</OvertimeElapseHours>

</Enforce>
```

XML template fields

The following tables define the fields and the type of data output from the *HitExportTemplate.xml* file.

Field Patroller 6.1 and earlier	Field Patroller 6.2 and later	Description
IsPlateExpired	IsPlateExpired	"True" or "False" boolean value that indicates if the license plate is expired or not.
IsPayZone	IsPayZone	"True" or "False" boolean value indicating if the selected zone is a “pay by zone” parking area.
PlateStatus	PlateStatus	Specifies the status of the plate. The possible values are: Expired, Valid, and NotChecked.
HitId	Hit_Id	The hit ID output as a GUID. For example: 000000000-0000-0000-000000000000.
HitType	Hit_Type	The type of hit. Possible values are: Hotlist, Overtime, Permit, and SharedPermit.
UserAction	User_Action	The action taken by the Patroller operator. The possible values are: None, Enforced, NotEnforced, Reject, Accepted.

Field Patroller 6.1 and earlier	Field Patroller 6.2 and later	Description
VehicleId	Read_Id	The vehicle's ID output as a GUID. For example: 000000000-0000-0000-000000000000.
Plate	Plate_Read	The license plate number. For example, ABC123.
State	Plate_State	The license plate's issuing state or province. For example: QC.
ReadType	ReadType	The type of read. Possible values are Standard, Permit, Overtime, SharedPermit.
PermitName	Permit_Name	Permit entity name.
ZoneName	Rule_Name	Permit zone name (parking lot, permit restriction, and so on). Used in University Parking Enforcement only.
UnitName	Unit_Name	The name given to the Patroller unit in Patroller Config Tool.
UnitId	Unit_Id	The Patroller unit's GUID ID. For example: 000000000-0000-0000-000000000000.
UserName	User_Name	The Patroller operator's Security Center username.
UserLogin	User_Login	The Patroller operator's login name.
UserId	UserId	The Patroller user's GUID ID. For example: 000000000-0000-0000-000000000000.
PermitId	Permit_Id	The selected permit's GUID ID. For example: 000000000-0000-0000-000000000000.
ParkingPermitId	Parking_Permit_Id	The selected shared permit's GUID ID. For example: 000000000-0000-0000-000000000000.
ZoneId	Rule_Id	The selected zone's GUID ID. For example: 000000000-0000-0000-000000000000.
GpsX	Longitude	The Patroller's longitude in decimal degrees for when the hit occurred. For example: -73.5878100.
GpsY	Latitude	The Patroller's latitude in decimal degrees for when the hit occurred. For example: 45.5088400.

Field Patroller 6.1 and earlier	Field Patroller 6.2 and later	Description
LprImagePath	Plate_Image	The location of the LPR image on the Patroller in-vehicle computer.
ContextImagePath	Context_Image	The location of the context image on the Patroller in-vehicle computer.
TireImagePath	Tire_Image	The location of the tire image on the Patroller in-vehicle computer.
TimeStamp	Date_Local Time_Local	The plate read timestamp. For example: 8/15/2014 12:04:07.
TimeStampUTC	Date_UTC Time_UTC	The plate time stamp in Coordinated Universal Time (UTC). For example: 8/15/2014 4:04:07.

Overtime fields

The remaining fields in the *HitExportTemplate.xml* are related to the first plate read captured during the *first* pass in an overtime enforcement scenario.

Field Patroller 6.1 and earlier	Field Patroller 6.2 and later	Description
OvertimeVehicleId	Overtime_Read_Id	The vehicle's ID output as a GUID. For example: 000000000-0000-0000-000000000000.
OvertimePlate	Overtime_Plate_Read	The license plate number. For example, ABC123.
OvertimeState	Overtime_Plate_State	The license plate's issuing state or province. For example: QC.
OvertimeReadType	Overtime_ReadType	The type of read. Possible values are Standard, Permit, Overtime, SharedPermit.
OvertimePermitName	Overtime_Permit_Name	Permit entity name.
OvertimeZoneName	Overtime_Rule_Name	Permit zone name. For example, parking lot or permit restriction name. Used in University Parking Enforcement only.
OvertimeUnitName	Overtime_Unit_Name	The name given to the Patroller unit in Patroller Config Tool.
OvertimeUnitId	Overtime_Unit_Id	The Patroller unit's GUID ID. For example: 000000000-0000-0000-000000000000.
OvertimeUserName	Overtime_User_Name	The Patroller operator's Security Center username.

Field Patroller 6.1 and earlier	Field Patroller 6.2 and later	Description
OvertimeUserLogin	Overtime_User_Login	The Patroller operator's login name.
OvertimeUserID	Overtime_User_ID	The Patroller user's GUID ID. For example: 000000000-0000-0000-000000000000.
OvertimePermitId	Overtime_Permit_Id	The selected permit's GUID ID. For example: 000000000-0000-0000-000000000000.
OvertimeZoneId	Overtime_Rule_Id	The selected zone's GUID ID. For example: 000000000-0000-0000-000000000000.
OvertimeGpsX	Overtime_Longitude	The Patroller's longitude (x-coordinate) in decimal degrees for when the hit occurred. For example: -73.5878100.
OvertimeGpsY	Overtime_Latitude	The Patroller's latitude (y-coordinate) in decimal degrees for when the hit occurred. For example: 45.5088400.
OvertimeLprImagePath	Overtime_Plate_Image	The location of the LPR image on the Patroller in-vehicle computer.
OvertimeContextImagePath	Overtime_Context_Image	The location of the context image on the Patroller in-vehicle computer.
OvertimeTireImagePath	Overtime_Tire_Image	The location of the tire image on the Patroller in-vehicle computer.
OvertimeTimeStamp	Overtime_Date_Local Overtime Time Local	The plate read timestamp. For example: 8/15/2014 12:04:07.
OvertimeTimeStampUTC	Overtime_Date_UTC Overtime_Time_UTC	The plate time stamp in Coordinated Universal Time (UTC). For example: 8/15/2014 4:04:07.
OvertimeElapseMinutes	Overtime_ElapseMinutes	The time (in minutes) between the first pass read plate read and second pass plate read.
OvertimeElapseSeconds	Overtime_ElapseSeconds	The time (in seconds) between the first pass read plate read and second pass plate read.
OvertimeElapseHours	Overtime_ElapseHours	The time (in hours) between the first pass read plate read and the second pass plate read.

Hit export XML output example (legacy system)

In the following example, since no permit zone was specified, the **ZoneName** and **OvertimeZoneName** fields are replaced by empty fields.


```
<?xml version="1.0" encoding="UTF-8"?>
<Enforce>
    <IsPlateExpired>True</IsPlateExpired>
    <IsPayZone>False</IsPayZone>
    <PlateStatus>NotChecked</PlateStatus>
    <HitId>786088dd-05e7-49af-a278-687b90878109</HitId>
    <HitType>SharedPermit</HitType>
    <UserAction>None</UserAction>
    <VehicleId>5a08f724-98d7-4510-8a20-01558d14fa56</VehicleId>
    <Plate>015WNJ</Plate>
    <State>QC</State>
    <ReadType>Standard, Permit</ReadType>
    <PermitName>Genetec</PermitName>
    <ZoneName/>
    <UnitName>Sample Patroller</UnitName>
    <UnitId>2d88a0af-63ee-4df7-a4e3-e83223873d33</UnitId>
    <UserName>PatrollerUser</UserName>
    <UserLogin>PATROLLERUSER</UserLogin>
    <UserId>ef6f85a7-4bf1-4c36-a6ac-a561035a4575</UserId>
    <PermitId>4e227340-bfb4-4c27-a04b-5dffde100f25</PermitId>
    <ParkingPermitId>101</ParkingPermitId>
    <ZoneId>00000000-0000-0000-0000-000000000000</ZoneId>
    <GpsX>-73.4140616187016</GpsX>
    <GpsY>45.5982875705029</GpsY>
    <LprImagePath>C:\PBP\5a08f72498d745108a2001558d14fa56lpr.jpg</LprImagePath>
    <ContextImagePath>C:\PBP\5a08f72498d745108a2001558d14fa56context.jpg</ContextImagePath>
    <TireImagePath>C:\PBP\5a08f72498d745108a2001558d14fa56tire.jpg</TireImagePath>
    <TimeStamp>8/15/2014 12:06:41 PM</TimeStamp>
    <TimeStampUTC>8/15/2014 4:06:41 PM</TimeStampUTC>
    <OvertimeVehicleId>a579afcb-35e0-4e08-8367-36ad04196901</OvertimeVehicleId>
    <OvertimePlate>005ZQB</OvertimePlate>
    <OvertimeState>QC</OvertimeState>
    <OvertimeReadType>Standard, Permit</OvertimeReadType>
    <OvertimePermitName>Genetec</OvertimePermitName>
    <OvertimeZoneName/>
    <OvertimeUnitName>Sample Patroller</OvertimeUnitName>
    <OvertimeUnitId>2d88a0af-63ee-4df7-a4e3-e83223873d33</OvertimeUnitId>
    <OvertimeUserName>PatrollerUser</OvertimeUserName>
    <OvertimeUserLogin>PATROLLERUSER</OvertimeUserLogin>
    <OvertimeUserId>ef6f85a7-4bf1-4c36-a6ac-a561035a4575</OvertimeUserId>
    <OvertimePermitId>4e227340-bfb4-4c27-a04b-5dffde100f25</OvertimePermitId>
    <OvertimeZoneId>00000000-0000-0000-0000-000000000000</OvertimeZoneId>
    <OvertimeGpsX>-73.4143994826998</OvertimeGpsX>
    <OvertimeGpsY>45.598502570503</OvertimeGpsY>
    <OvertimeLprImagePath>C:\PBP\Overtime5a08f72498d745108a2001558d14fa56lpr.jpg</OvertimeLprImagePath>
    <OvertimeContextImagePath>C:\PBP\Overtime5a08f72498d745108a2001558d14fa56context.jpg</OvertimeContextImagePath>
    <OvertimeTireImagePath>C:\PBP\Overtime5a08f72498d745108a2001558d14fa56tire.jpg</OvertimeTireImagePath>
    <OvertimeTimeStamp>8/15/2014 12:06:33 PM</OvertimeTimeStamp>
    <OvertimeTimeStampUTC>8/15/2014 4:06:33 PM</OvertimeTimeStampUTC>
    <OvertimeElapseMinutes>0.125975558333333</OvertimeElapseMinutes>
    <OvertimeElapseSeconds>7.5585335</OvertimeElapseSeconds>
    <OvertimeElapseHours>0.00209959263888889</OvertimeElapseHours>
</Enforce>
```

Modifying the font size in Patroller

To accommodate varying screen sizes and resolutions, you can adjust the font size in Patroller through a configuration file.

What you should know

The font size modifications of Patroller applies only to the Information Panel section of the screen. This sections displays Reads and Hits information. The font size value can vary from 100% (default size) to 140%.

To modify Patroller information panel font size:

1 Open the following file:
<Patroller 6.3 installation folder> \MobileClient\Genetec.AutoVu.Configuration.config

2 Add the following line: *<add key="Mobile.Patroller.Display" value="100" />*
The number in the "value" element can vary from 100 to 140 and represents the increase percentage of the default font size.

3 Save the file and restart Patroller.

The information Panel font size on the Patroller is now modified according to the configured value.

5

Patroller Config Tool Reference

This section includes the following topics:

General page in Patroller Config Tool

The *General* settings page allows you to configure basic Patroller options such as the Patroller unit's name, how users should log on, etc.

Patroller Standalone is not connected to Security Center, therefore for some settings it's indicated that they are not applicable for Patroller Standalone. These settings do not appear in Patroller Config Tool.

- **Patroller name:** Enter the name of the Patroller unit as you want it to be seen in Security Center and Security Desk.
- **Logon type (not applicable to Patroller Standalone):** Select how to log on to Patroller.
- **SQL Server:** The address and name of the SQL Server.
- **Database name:** You can leave the default database name, or change it to whatever you want. You can change this name at any time to create a new database.
- **Use Windows authentication:** Turn the setting on or off.
- **User ID:** The User ID to connect to the Patroller database. This User ID was entered during Patroller installation.
- **Password:** The password to connect to the Patroller database. This password was entered during Patroller installation.
- **Advanced:** Configure Advanced settings for the Patroller database.
- **Test connection:** Test the connection to the Patroller database with the options selected.

Related Topics

Naming a Patroller unit on page 30
Configuring Patroller logon options on page 31
Configuring Patroller database options on page 32

Cameras page in Patroller Config Tool

The *Cameras* page allows you to add Sharp camera units to your network, and configure basic settings related to Patroller's interaction with the Sharp cameras. You can also enable Sharp analytics, which provide information on vehicle speed, relative motion, and more.

Related Topics

Connecting mobile Sharp units to Patroller on page 37

Cameras - Units tab in Patroller Config Tool

The **Units** tab allows you to add a Sharp unit to your network, and configure its settings.

- **Units:** These are the Sharp units connected to your in-vehicle LAN.
  - **Add a Sharp ( ):**
    Manually add a Sharp camera unit to the network. Do the following:
    - You'll need to enter the Sharp unit name. This is the IP address of the Sharp (for example, 192.168.10.1 for a SharpX).
    - You also need to specify the camera's orientation, meaning where it's installed on the vehicle (front right, front left, and so on).

    If you're using a *SharpX* system with an X2S LPR Processing Unit, the "unit" corresponds to one of the LPR Processing Unit's Single Board Computers (SBCs). You may see up to two (X2S) or four (X1S) LPR cameras controlled by a single unit. Cameras must be named "Lpr Camera ", "Lpr Camera 2" etc. (case sensitive).
  - **Remove a Sharp ( ):** Remove a Sharp camera from the network.
  - **Edit a Sharp ( ):** Edit the Sharp's connection settings to Patroller.
  - **Configure the Sharp ( ):** Opens the Sharp Portal in a web browser so you can configure the Sharp's properties.
  - **Start discovery:**
    Automatically detect installed Sharp cameras and add them to the network. You will still need to specify each camera's orientation (front right, front left, and so on). This is the preferred method of adding Sharps to the network.
- **Camera exposure on startup:** Use the slider to set the initial value for the camera exposure control when you first login to the application.
- **Pause reads on startup:** Turn on to have plate reading paused when you log on to Patroller.
- **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. For more information, see the *Sharp Administrator Guide*.

Cameras - Analytics tab in Patroller Config Tool

Sharp cameras can provide analytical information based on the license plate and context images they capture.

- **Confidence score:** The Sharp assigns a numerical value (from 0 to 100) to each license plate read. This value tells you how confident the Sharp is in the accuracy of the read.
- **Relative Motion:** The Sharp can detect if the vehicle is getting closer or moving away.
- **Speed:** Sharp cameras are able to estimate a vehicle's approximate speed. For a mobile AutoVu™ installation, the Patroller vehicle must be stopped for this feature to work.
- **Vehicle Make:** Sharp cameras can recognize the make of certain vehicles. Vehicle make recognition is performed on a best-effort basis and is continually being updated.

  NOTE: The Sharp must see the vehicle's logo for this feature to work.
- **Vehicle Type:** Certain license plates include character symbols that identify specific vehicle types (for example, taxi, transport, and so on). The Sharp can read these symbols, and display the vehicle type along with the other read/hit information.
- **Prefix:** Certain license plates have sections that contain numbers or text that have a specific meaning. For example, a number that represents a city or a borough. The Sharp with the corresponding LPR contexts can read these sections and display the result in the "Prefix" value.

Operation page in Patroller Config Tool

The *Operation* page allows you to configure options related to Patroller operation and enforcement.

Operation - General tab in Patroller Config Tool

Configure the general options that apply to all types of hits.

- **Pause reads while enforcing:** Turn on to pause Patroller plate reading while you're in the process of accepting or enforcing a hit.
- **Allow popup hit:** Turn on for Patroller to display hits on screen as they occur. Turn off for hits to accumulate in the background.
- **First hit on top:** Choose the order that hits are displayed. Turn on to display the oldest hit first (right side of the Patroller scrollbar). Turn off to display the latest hit first.
- **Enable plate editing:** Turn on to allow editing of license plate characters when you receive a hit. From the hit screen, click or tap the plate text string to open the editor.
- **Text-to-speech voice (not applicable to Patroller Standalone):** Select the voice you want to use for notifications, such as when the Patroller vehicle is entering and exiting a zone and the name of the zone. Select None to disable the option.

NOTE: The voices that are available depend on your Windows operating system.

Operation - Hotlists tab in Patroller Config Tool

Configure hotlist-related options.

NOTE: You set New wanted attributes and categories in Security Center Config Tool.

- **Allow consecutive hits:** Turn on to allow sequential hits for the same plate. For example, if you capture a plate that raises a hit, and then capture the same plate again, it will raise another hit.

  NOTE: If you turn this setting off, Patroller would need to capture a new plate before allowing a hit for the same plate.
- **Enable new wanted:** Turn on to allow Patroller users to add New wanted hotlist entries.
- **Enable new wanted management:** Turn on to allow Patroller users to edit and delete New wanted entries from the database.
- **Enable comments for new wanted:** Turn on to activate a text box in Patroller where you can enter a comment when entering a New wanted hotlist item.
- **New wanted expiry options (days):** Create the expiry options available to the Patroller user when adding a New wanted entry.

  For example, let's say you create the options 1, 5, and 10. When you add a New wanted entry, you'll be able to choose for that entry to expire in 1, 5, or 10 days. If you don't provide an expiration option, New wanted entries will remain in the Patroller database indefinitely.
- **Add expiration option ():** Enter an expiration option (in days). Maximum value is 100.
- **Delete expiration option ():** Delete an existing expiration option.
- **Enable Selectable hotlist:** Turn on to allow Patroller users to select which hotlists among those available on the Patroller are used to generate Hits.
- **Enable past read matching:** Turn on to compare reads from the past with a new hotlist, or new wanted plates that have been manually added.

- **Past read matching look back:** Enter how long in hours you would like Patroller to look back in the database for reads that match a new hotlist, or new wanted entry.
- **Bypass hit enforcement:** Turn on to bypass the additional step of enforcing a hit after accepting it. When turned on, Patroller assumes you enforced the hit, and will not display the Enforced/Not enforced prompt.
- **Auto-enforce hotlist hits:** Turn on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction.

  NOTE: If you have configured “Hit accept” or “Hit reject reasons”, they are ignored when this setting is on.
- **Display hits by priority:** Turn on to display hits in Patroller by the priority you specified in Security CenterConfig Tool.

  For example, if you have set “Hotlist A” to a higher priority than “Hotlist B”, hits generated from Hotlist A will be displayed first (on the right of the Patroller scrollbar).
- **Use simple matcher:** Turn on Simplematcher when using very large hotlists with millions of entries. You’ll also need to turn off OCR equivalence in the LPR matcher. For more information about configuring LPR matcher settings, see the *Security Center Administrator Guide*.

Operation - Permits tab in Patroller Config Tool

Enable and configure permits, shared permits (if applicable), and related options.

- **Use permit:** Turn on to enable the use of permits.
- **Bypass permit hit enforcement:** Turn on to bypass the additional step of enforcing a hit after accepting it. When turned on, Patroller assumes you enforced the hit, and will not display the Enforced/Not enforced prompt.
- **Auto enforce permit hits:** Turn on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction.

  NOTE: If you’ve configured Hit reject reasons, they are ignored when you turn this setting on.
- **Use shared permit:** (University Parking Enforcement only). Turn on to enable the use of shared permits.
- **Bypass shared permit hit enforcement:** (University Parking Enforcement only). Turn on to bypass the additional step of enforcing a hit after accepting it. When turned on, Patroller assumes you enforced the hit, and will not display the Enforced/Not enforced prompt.
- **Auto enforce shared permit hits:** (University Parking Enforcement only). Turn on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction.

  NOTE: If you’ve configured Hit reject reasons, they are ignored when you turn this setting on.

Operation - Overtime tab in Patroller Config Tool

Enable and configure overtime enforcement, wheel imaging (if applicable), and related settings.

NOTE: This tab is not available in Patroller Standalone.

- **Use overtime:** Turn on to enable the use of overtime rules.
- **Advanced:** Click to configure the *Advanced overtime settings*:
  - **Link read persistence duration:** Enter the amount of time that a plate read stored in the Patroller database is considered to be a “time 1” read for a particular overtime rule.
    Let’s say you enter 8 hours, which is a typical Patroller’s shift. You start your shift and select *OT_Rule1*. You do your first pass and read plate *ABC123* at 9:00 a.m. This is now “time 1” for the rest

of the day (until 5:01 P.M.). Even if you close and restart Patroller, the “time 1” for plate *ABC123* for *OT_Rule1* will be 9:00 a.m. If you start Patroller after the duration (8 hours in this example), the 9:00 a.m. read is no longer considered to be a “time 1” read.

- **Minutes to due vehicles:** Enter the amount of time before the vehicles are due for enforcement. This value determines the *Show Due* functionality in Patroller. The default is 5 minutes.
- **Preferred Long Term Overtime zone:** If you have more than one Long Term Overtime zone configured in Security Center, you must type the name of the zone you want Patroller to display, since you can only enforce one zone at a time. This value is not case-sensitive.
- **Enable logs:** Turn on to enable logs related to overtime enforcement. This option should only be used for troubleshooting and technical support, if required.
- **Same position tolerance:** This is a buffer used for “Same position” overtime rules. It is the distance that Patroller considers to be a single postion or parking space.

- **Bypass hit enforcement:** Turn on to bypass the additional step of enforcing a hit after accepting it. When turned on, Patroller assumes you enforced the hit, and will not display the Enforced/Not enforced prompt.
- **Auto enforce overtime hits:** Turn on for Patroller to run in unattended mode. Hits are automatically accepted and enforced without requiring user interaction.

  NOTE: If you’ve configured Hit reject reasons, they are ignored when you turn this setting on.
- **Apply overtime rule to permit holders:** Turn this on for locations where parking access can be bought for a limited period. In this configuration, if a plate is read once and is not on the selected permit list, a Hit will be generated. However, if it is on the list, no Hit will be generated on the first read. The second Read will determine if the time limit is exceeded and if a Hit is generated. If this option is disabled, permit holders do not generate violations.
- **Use tire images:** Turn on to use wheel imaging. Wheel images are saved to the in-vehicle computer.
- **Wheel imaging enforced:** Select whether wheel imaging is enforced or not from the drop-down list:
  - *Mandatory* **:** The user is required to verify wheel images for both passes in order to enforce a hit.
  - *Optional* **:** The user can enforce a hit without verifying wheel images.
- **Tire cam-to-plate distance:** Specify the distance (in meters) from the tire camera to the vehicle license plate when the car is parked. The default parallel distance is 4 meters, and the default 45 degree angle distance is 3 meters.
- **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.

Operation - MLPI tab in Patroller Config Tool

Enable and configure options related to Mobile License Plate Inventory.

NOTE: This tab is only available in MLPI mode.

- **Enable read deletion:** Allows you to delete the plate read from the information panel of the Patroller main window. This is useful to correct any mistakes before the plate data is offloaded.

  For example, if you have misreads, or did a sweep but specified the wrong location before you started, you can delete those reads before they are offloaded to Security Center.

  NOTE: This only applies to plates that are read when an MLPI zone is selected.

- **Enable read modification:** Allows you to modify plate numbers from the information panel of the Patroller main window. This is useful if a plate is misread and you want to correct it before offloading the data.
- **Enable too many reads popup:** Patroller will trigger an alarm (sound or warning message) if the reads collected during your sweep of a row exceed the number of spaces specified in the “Space count” for that row.

  NOTE: You specify the “Space count” in the Parking facility rule in Security CenterConfig Tool.

Operation - Pay-by-Plate tab in Patroller Config Tool

Enable and configure options related to the Pay-by-Plate plugin.

NOTE: This tab is only available in City and University mode.

- **Use Pay-by-Plate:** Turn ON to enable Pay-by-Plate plugin.
- **Disable Enforce button on validation error:**
  - **ON:** Disables Patroller’s Enforce button if there is a communication error that prevents Live Infraction Validation from validating the hit.
  - **OFF:** Does not disable enforcement if there is a validation error.

  The option **Disable Enforce button on false hits** supersedes this option. If you allow enforcement of false hits, this option has no effect.
- **Disable Enforce button on false hits:**
  - **ON:** Disables Patroller’s *Enforce* button if Live Infraction Validation confirms the captured plate is valid and is in the provider’s system (false hit).
  - **OFF:** You will receive a message informing you that the hit is invalid, but you will be allowed to enforce it if you choose.
- **Update permit data on false hits:**
  - **ON:** Updates your selected permit list if the Live Infraction Validation confirms the captured plate is valid and is in the provider’s system (false hit).
  - **OFF:** You will need to update your permits manually by re-selecting your permits in Patroller.
- **Update permit data on permit selections:**
  - **ON:** When you select a permit to enforce in Patroller, the permit is automatically updated with the latest information from the parking provider’s system.
  - **OFF:** Permits are only updated when Security Center gets new information from the parking provider, and then updates Patroller using Periodic Transfer (which should be set to one minute).
    NOTE: If you turn this setting off, you cannot have permit updates set to “0” in Security Center Config Tool. Doing so would disable automatic updating of permits.
- **Show synchronization status on permit selection:**
  - **ON:** Displays a popup window after you select a permit that shows the synchronization status between Patroller and Security Center.
  - **OFF:** The popup window is not displayed.
    IMPORTANT: If you turn this setting off, synchronization will still occur if the Update permit data on permit selections option is enabled. However, you will not know when synchronization is complete, or if there were any errors. It is recommended that you leave this setting on at all times.
- **Security Center communication port:** Enter the port number to use for connecting to the Security Center Pay-by-Plate plugin role (8787 is the default). This must match the port entered in Security Center Config Tool for the setting: **Patroller communication port**.

- **Security Center URL:** Type the IP address (in the form of a URL) to connect to the Security Center Pay-by-Plate Sync plugin role. For example, if you want to connect to IP address 123.456.78.9, you must type the full address as http://123.456.78.9.

  IMPORTANT: Do not include a trailing slash after the IP address.
- **Security Center URL (failover 1):** If you have failover configured for the Pay-by-Plate sync plugin role, enter the IP address (in the form of a URL) of the first failover server.
- **Security Center URL (failover 2):** If you have failover configured for the Pay-by-Plate sync plugin role, enter the IP address (in the form of a URL) of the second failover server.
- **Security Center URL (failover 3):** If you have failover configured for the Pay-by-Plate Sync plugin role, enter the IP address (in the form of a URL) of the third failover server.
- **Communication timeout (seconds):** Enter how long (in seconds) before a communication request between Patroller and Security Center times out.

Navigation page in Patroller Config Tool

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

Navigation - Equipment tab in Patroller Config Tool

Enable and configure global navigation system options.

- **Equipment type:** Select one of the following options:
  - **None:** No Global navigation equipment is being used.
  - **AutoVu Navigation:** Select this to use the navigation equipment embedded in the LPR Processing Unit.
  - **External GPS :** Select this to use the USB GPS receiver that connects to the in-vehicle computer.
  - **External Navigator box (not applicable to Patroller standalone):** Select this to use the GPS antenna that connects to the AutoVu Navigator box.
- **Use positioning (AutoVu Navigation only):** Slide **ON** to use the global navigation and positioning equipment integrated in the LPR Processing Unit.
- **Use GPS (External Navigator box only):** Slide **ON** to use GPS with the AutoVu external Navigator box.
- **Device:** Displays the device name connected to the Patroller. Applies to external Navigator Box, external GPS, and AutoVu Navigation system.
  - Click in the field (external Navigator Box and external GPS) to open the **Select device** dialog box. Choose the appropriate USB device and click **OK** > **Apply**.
  - Click the discovery button (AutoVu navigation) to restart navigation equipment auto discovery when necessary.
- **Advanced:** Click to configure the advanced GPS settings (external GPS and external Navigator box).
  - **Baud rate:** The speed of the GPS communications channel (serial port). The default value is 9600, but some USB GPS devices require a reduced speed of 4800. For example, if you're using Genetec's USB GPS receiver that connects to the in-vehicle computer (model number BU-353S4), you need to change this value to 4800.
  - **(Optional) Force Port:** Turn this option on when you want to make sure that Patroller uses the port configured in the Patroller Config Tool. This is useful in the case where you are using two USB GPS devices and you want to prevent Patroller from automatically switching to the other GPS port if it cannot detect the GPS port specified in Patroller Config Tool.
  - **Port:** Specify the COM port number of the GPS device as seen in Windows Device Manager.
    - If you're using the USB GPS that connects directly to the in-vehicle computer, the name of the device in Device Manager is **Prolific USB-to-Serial Comm Port**.
    - If you're using the GPS antenna that connects to the Navigator box, the name of the device in Device Manager is **u-blox 5 GPS and GALILEO Receiver**.
  - **GPS initialization string:** Displays the initialization commands to be sent to the GPS device when you log on to the application.
    IMPORTANT: Do not modify. This is the default firmware setting.
  - **Consecutive invalid strings before restart:** Specify the number of consecutive invalid GPS strings allowed before the device is restarted. Invalid GPS strings happen when the GPS signal can't be detected. The default number is 10.

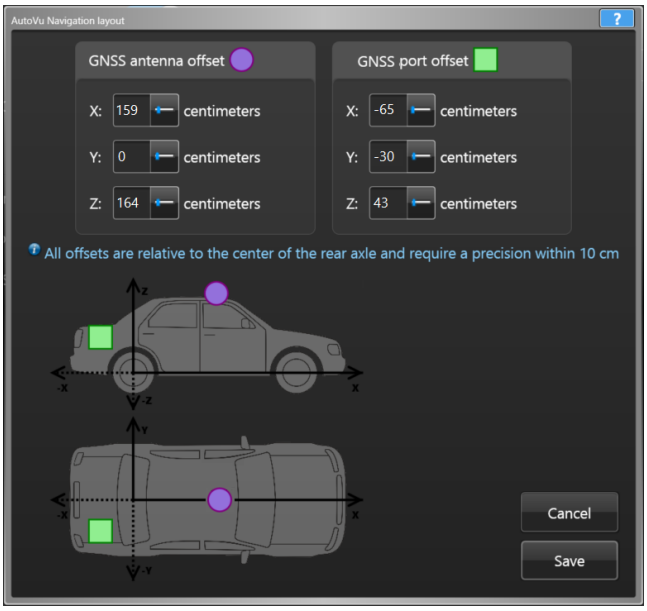
IMPORTANT: You should not need to change this setting.

- **Noise:** Specify the noise value. If the distance from 0,0 to the GPS position is less than the value you define, no GPS event is generated. The default noise value is 5.
  IMPORTANT: You should not need to change this setting.

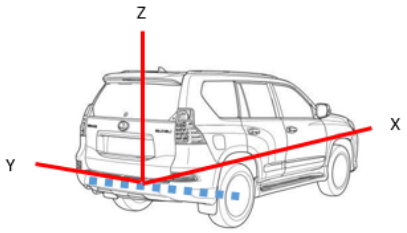
- **Layout... (AutoVu Navigation only):** Click to enter the GNSS antenna and port positions. This operation is necessary to calibrate the navigation hardware. For details, see the Layout page.
- **Calibrate...(AutoVu Navigation only):** Click to perform step-by-step odometry and GNSS calibration. For details, see the Calibration procedure.
- **Monitor...(AutoVu Navigation only):** Click this button to get information about navigation position, malfunctions, and vehicle status. For details, see the Monitor page.
- **Use odometry (External Navigator box only):** Slide **ON** to use the Navigator box for odometry as well as global positionning.
- **Reverse signal active when (External Navigator box only):** Slide **ON** to indicate that the transmission reverse signal is active when high. Leave it **OFF** to indicate active when low.
- **Advanced (External Navigator box only):** Allows you to configure the following Odometry settings:
  - **Scale:** Value specified during system calibration.
  - **Sensitivity:** Navigator box's sensitivity as measured during calibration using the Oscilloscope tool.
  - **GPS distance tolerance:** Maximum GPS distance correction allowed (in meters) when using odometry.
  - **GPS odometry calibration tolerance:** Acceptable odometry calibration error (in meters).
- **Read when car is stopped:** Specify whether or not to continue reading plates when the Patroller vehicle is stopped. When doing parking enforcement, Patroller vehicles may stop and reverse frequently.
- **Read when moving backwards:** Specify whether or not to continue reading plates when the Patroller vehicle moves in reverse. When doing parking enforcement, Patroller vehicles may stop and reverse frequently.
- **Shutdown delay (not applicable for Patroller Standalone):** Specify the number of seconds to wait after the vehicle's ignition is turned off before shutting down the in-vehicle computer. To disable this feature, enter "0".

Navigation - Equipment tab - Layout in Patroller Config Tool

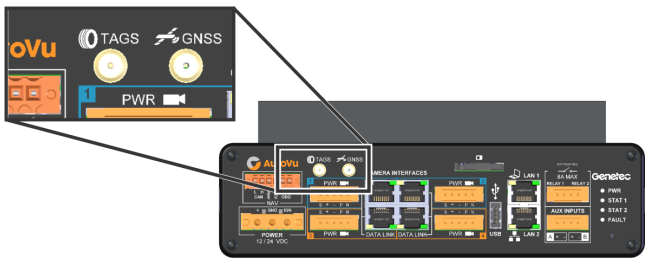
Configure GNSS equipment layout.



- **GNSS antenna offset:** The purple dot on the graphic represents the position of the GNSS antenna installed on the patrolling vehicle. Enter the following values (in centimeters) to configure the antenna layout:
  - **x:** The x value represents the position of the equipment relative to the length of the car (rear and front). The zero position being the rear axle, a negative value is behind the rear axle and a positive value is in front of the rear axle.
  - **y:** The y axis represents the position of the equipment relative to the width of the car (left or the right) when standing behind the vehicle and looking towards it. The zero position being the center of the car, a positive value is towards the left and a negative value is towards the right.
  - **z:** The z axis represents the height of the equipment relative to the rear axle. A positive value is positioned above the axle.



- **Tire tag port offset:** The green square on the graphic represents the position on the Patroller vehicle of the Tire tag connector on the LPR Processing Unit face plate.

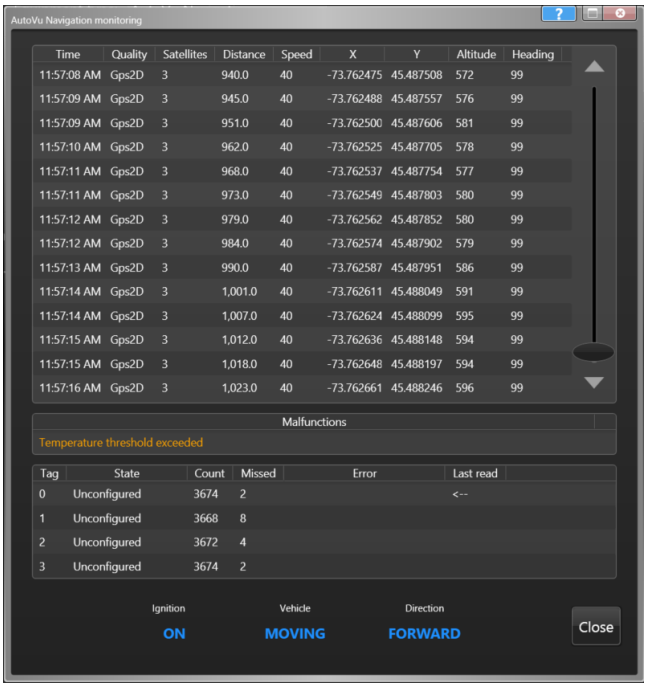


Enter the x, y, and z values as described for the antenna.

- **Diagram:** The diagrams provided on the configuration page are for illustrative purpose only as vehicle models may vary. The symbols will be displayed within the diagram boundaries even if large numbers are entered in the measurements input fields. The axis being modified is highlighted in blue on the diagram.

Navigation - Equipment tab - Monitor in Patroller Config Tool

Monitor AutoVu navigation hardware status.



- **GNSS navigation information:** The first table in the monitoring page shows the following information:
  - Signal quality
  - Longitude, latitude, and altitude
  - Odometry, heading, and speed
  - Number of satellites
  - Time

  The navigation information table scrolls down automatically to show the most recent data first. Use the scroll bar to go back and stop the automatic scrolling. To reactivate it, scroll completely down to display the most recent data.

- **Malfunctions:** The second table in the monitoring page shows different possible problems with the navigation hardware: high temperature, double information from tags, network connection lost with the navigation module, and others. It is hidden if no malfunction is detected.
- **Odometry tags status:** The third table in the monitoring window shows the odometry tire tags' statistics, and their configuration status. This table also shows the position of the tag that is next to the reader (last read). This information is useful if you need to locate a faulty tire tag.
- **Vehicle status:** Three status are available about the vehicle on which the navigation is installed:
  - **Ignition:** Indicates the engine ignition status: ON or OFF.
  - **Vehicle:** Indicates the vehicle mobility: still or moving
  - **Direction:** Indicates the direction the vehicle is moving: backward or forward.

Navigation - Maps tab in Patroller Config Tool

Enable and configure maps and related GPS options.

- **Mapping type:** Select the map type from the drop-down list:
  - **None:** Do not use maps.
  - **BeNomad:** The default map type for AutoVu™.
- **Show vehicle route:** Displays a trail behind the Patroller icon that allows you to see the route Patroller has taken. Turn this setting off to show only the Patroller's current position.
- **Show parking lots overlay:** Turn on to display configured parking lots on the map in the Patroller main viewer.
- **Snap to road threshold:** Specify the maximum distance error (in meters). If the distance between the vehicle and the closest map item is greater than this value, no snapping will occur.

Security Center page in Patroller Config Tool

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

NOTE: This tab is not applicable to Patroller Standalone.

Security Center - Live connection tab in Patroller Config Tool

Configure how Patroller connects to Security Center.

- **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.

  NOTE: After you properly configure this setting, leave it on indefinitely. Patroller will connect to Security Center whenever a wireless connection is available (e.g. you are in range of the company WiFi network), and download any modifications or updates required.
- **IP address:** Enter the IP address of the Security Center machine hosting the LPR Manager role.
- **Port:** Enter the port number Patroller should use to connect to the LPR Manager role.

  NOTE: You must *also* enter the same port number for the listening port in Security CenterConfig Tool. Go to the LPR Manager *Properties* page, and then under *Live*, enter the *Listening port*.
- **Encrypt communication channel:** Turn this setting on if you want to encrypt communication between Patroller and Security Center.

  NOTE: To use this feature, you must *also* encrypt communication in Security CenterConfig Tool. Go to the LPR Manager *Properties* page, and then under *Live*, select *Encrypt communication channel*.
- **Update provider port:** Enter the port that Security Center uses to send hotfixes and other updates to Patroller and connected Sharp units.

  NOTE: To use this feature, you must *also* enter the same port number for the listening port in Security CenterConfig Tool. Go to the LPR Manager *Properties* page, turn on *Update provider*, and then enter the *Listening port*.
- **Live events:**
  - **Hits:** Send hits live to Security Center
  - **Reads:** Send reads live to Security Center.
  - **Unit position:** Send the position of the Patroller unit live to Security Center.
- **Periodic transfer:** Specify how often hotlist and permit list changes are downloaded to Patroller (if you have a live connection). The default transfer period is every 240 minutes.

  NOTE: You can disable Periodic transfer on specific hotlists (not permit lists) in Security CenterConfig Tool on the hotlist's *Advanced* page. For more information, see the *Security Center Administrator Guide*.

Offload page in Patroller Config Tool

Offloading allows you to transfer reads, hits, and other Patroller data to Security Center. Please note that if you're running Patroller Standalone (no connection to Security Center) your data is offloaded to a local *.Standalone* file on the in-vehicle computer.

NOTE: Patroller Standalone is not connected to Security Center, therefore, it is indicated for some settings that they do not apply to Patroller Standalone. These settings do not appear in the Patroller Config Tool.

- **Offload method:** Select your offload method:
  - **None:** Does not offload data.
  - **Local file:** You can configure Patroller to offload data to a file on the in-vehicle computer. 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.
    - If you are connected to Security Center: After you have offloaded the data, you can then copy the data to a USB key, and transfer it to the Security Center computer.
    - If you are using Patroller Standalone: After you have offloaded the data, you can open the *Offload.Standalone* file in Internet Explorer to view the information or import the *.Standalone* file into your own reporting tool.
- **Live transfer (not applicable to Patroller Standalone):** This offload method transfers all data from the Patroller vehicle to Security Center using a wireless connection. For example, you can offload your data at the end of a shift, when you're in range of the company's wireless network. You also use this option to offload data to a network drive rather than your local drive on the in-vehicle computer.

  NOTE: Please note the following about *Live transfer*:

  - This option automatically transfers the offload data into the *Offload* folder under the LPR Manager root folder. For more information about the LPR Manager root folder, see the *Security Center Administrator Guide*.
  - If you try to offload without being connected to Security Center, the offload is done on your local in-vehicle computer. You can then transfer the offload data to Security Center with a USB key.
- **Local offload drive:** If using *Local file* as your offload method, specify where on your machine the data should be saved (e.g. C:\ if you want to offload to your C drive).

  IMPORTANT: Do **not** specify the folder. Patroller creates the *Offload* folder on the drive you specify.
- **Use encryption (not applicable to Patroller Standalone):** Turn on to encrypt the offloaded data. You'll also need the Public key (not applicable to Patroller Standalone).
- **Public key (not applicable to Patroller Standalone):** To encrypt offload data, Patroller needs the public key from the Security Center computer. Do the following:
  1. On the Security Center computer, go to *C:\Program Files\Genetec Security Center <your version>*, and copy the *OffloadPublicKey.xml* file to your clipboard.
  2. On the Patroller computer, go to *C:\Program Files\Genetec AutoVu X.Y\MobileClient*, and paste the *OffloadPublicKey.xml* in the folder.
  3. In the *Public key* field, enter the path to the public key you just pasted to the Patroller computer (*C:\Program Files\Genetec AutoVu X.Y\MobileClient\OffloadPublicKey.xml).*
- **Offload events:** This option allows you to choose which data you want to include in an offload. For example, you may only want to offload **Hits** to use less bandwidth when performing an offload.
- **Include all images:** Turn on to offload all images. If this option is turned off, only images associated with a hit will be included in the offloaded data.

- **Incremental offload:** By default, Patroller offloads data in increments, or segments. Turn this setting off if you want to offload the full data file each time.
- **Data segment size:** Specify the maximum file size of each data segment (MB) when using Incremental offload. Once the offload file reaches the size limit, a new offload file is created and the offload process continues. The default maximum file size is 1 MB.
- **Force offload before exit:** Turn on to make Patroller exit commands unavailable. The only way to close the application is to perform an offload.

  NOTE: This option won't work if you set **Offload method** and **Action after offload** to **None**.
- **Action after offload:** Select the exit procedure that occurs after you have performed an offload:
  - *None* **:** Return to the application.
  - *Exit* **:** MobileServer, MobileClient, and IO.Services are exited.
  - *Shutdown* **:** If the *PowerManagement.UsePowerManagement* option is selected, the OffloadExit setting is automatically set to *Shutdown*. This option does not work with laptops; choose *Exit* instead.
- **Delete after offload:** Turn on to delete all records of user logins, images, hotlist hits, vehicles, unit states, street blocks, tire images, cameras, and attributes after a successful offload.

Plugin page in Patroller Config Tool

The *Plugin* page is where you enable and configure AutoVu™ plugins. You can use the arrows to activate and deactivate a plugin. Multiple plugins can be active at the same time. Once you activate a plugin, you can configure its settings by selecting it in the **Active plugins** list.

NOTE: The *Street Sweeper* and *Scofflaw mdt* plugin are only used for specific deployments, and therefore may not be available on the **Plugin** page. For more information about the *Street Sweeper* and *Scofflaw mdt* plugins, contact your Genetec representative.

Plugin - Plate copy in Patroller Config Tool

The Plate copy XML plugin makes it easier to verify the plates you capture in Patroller with other applications installed on your in-vehicle computer. With your other application open, you can simply paste the plate number in and perform your search, saving you valuable seconds every time you want to search for a plate. You can also use the XML file created on your computer in any custom application you choose.

You can customize the Plate copy plugin by modifying the following settings:

- **Clear XML files on startup:** Turn on so that when you start Patroller, the XML data created by the Plate Copy plugin is deleted from the in-vehicle computer. When this option is off, the XML data created by the *Plate Copy* plugin is not deleted automatically on startup. You can delete the data manually if needed.
- **Allow Plate Copy for hits only:** Turn on to have the Plate Copy feature work for hits only. When this option is turned off, the Plate Copy feature works for reads and hits.
- **Create a different XML file each time:** Turn on to creates a different Plate Copy XML file with each use. For more information on how this affects the filename, see Name of the created XML file. When this option is turned off, the *Plate Copy* XML file is overwritten with each use.

  IMPORTANT: Third-party applications that use the *Plate Copy* XML file must turn this setting on.
- **Name of the created XML file:** Type the filename you want for the *Plate Copy* XML file.
- **Where to save the created XML file:** Enter the path on the in-vehicle computer where you want the *Plate Copy* XML files to be saved (for example, you could save the files to *C:\PlateCopyXMLfiles*). The plugin will create the folder for you the first time you tap a plate image in Patroller.
- **Name of the XML template file to use:** Type the filename of the XML template you want to use for the *Plate Copy* XML file
- **Copy plate number to Windows clipboard:** Turn on to automatically copy the plate number to the Windows clipboard when you tap the plate image in Patroller. This allows you to quickly paste the plate number to the third-party application (use Ctrl+V).
- **Minimize Patroller window:** Turn on to minimize Patroller when you when you tap the plate image in the main window.

  NOTE: When this option is turned off Patroller is not minimized but the third-party application is displayed Patroller on top of the Patroller window if the **Maximize external application window** and **Restore external application window** settings are turned ON.
- **Search external application by process name:** When turned on, Patroller searches for the name of the third-party application process as it appears in Windows Task Manager (for example, *Notepad*). When turned off, Patroller searches for the name of the minimized window (for example, *Test.txt - Notepad*).
- **External application name:** Enter the name of the third-party application to display when you tap the plate image in Patroller. The name you enter here depends on whether the Search external application by process name option is turned on or off. For example, if you want to open Windows Notepad, type one of the following in this field:

- If Search external application by process name is turned **ON**, type `Notepad`, the name of the notepad process as it appears in Windows Task Manager (without the *.exe*).
- If Search external application by process name is turned OFF, type the full name as shown in the title bar of the application's window. For example, the name of an unsaved minimized Notepad window is called *Untitled - Notepad*.

IMPORTANT: Only applications that are already running can be displayed. This feature cannot start an application for you.

- **Restore external application window:** When this option is on, the third-party application is restored to its former size when you tap the plate image in Patroller. When this option is turned off, the third-party application is not displayed unless you also turn on the option **Maximize external application window**.
- **Maximize external application window:** Turn on to maximizes the third-party application when you tap the plate image in Patroller. When turned off the third-party option is not displayed unless you also turn on the **Restore external application window** option.
- **Display all external application windows:** Turn on to display all the windows of the third-party application when you tap the plate image in Patroller. When you turn this option off, the first thrid-party window that is listed in Windows Task Manager will be displayed when you tap the plate image in Patroller.

Plugin - Hit export in Patroller Config Tool

The Hit export plugin creates an XML file that third-party ticketing systems can use to help automate the issuing of parking citations. When you enforce a permit hit in Patroller, an XML file with the permit hit data is saved to the in-vehicle computer. Third-party ticketing systems can then use this XML file to pre-populate the required fields in their parking ticket citations (license plate number, street location, time/date, and so on).

You can customize the Hit Enforce plugin by modifying the following settings:

- **Clear exported XML files on startup:** Turn on so that when you start Patroller, the XML data created by the Hit export plugin is deleted from the in-vehicle computer. When this option is turned off, the XML data created by the *Hit export* plugin is not deleted automatically on startup. You can delete the data manually if needed.
- **Export XML file after accepting a hit:** Turn on so that when you accept a hit, Patroller exports the XML file to the specified location on your in-vehicle computer. When this option is turned off, Patroller exports the XML file to the specified location on your invehicle computer when you enforce the hit.
- **Create a different XML file each time:** Turn on to create a different XML file with each use. For more information on how this affects the filename, see the **Name of the created XML file** option. When this option is turned off, the same XML is overwritten with each use.

  IMPORTANT: Third-party applications that use the XML file must turn this setting on.
- **Name of the created XML file:** Type the filename you want for the XML file. This option only works when the Create a different XML file each time option is turned OFF.
- **Where to save the created XML file:** Enter the path on the in-vehicle computer where you want the Hit export XML files to be saved (for example, you could save the files to C:\XMLHitExportfiles). The plugin will create the folder for you the first time this feature is used.
- **Name of the XML template file to use:** Type the filename of the XML template you want to use for the XML file.

Plugin - Street Sweeper in Patroller Config Tool

This section lists the options in the Street Sweeper tab of the Plugin page.

- **AddTimeStampOverlay:** Turn Time Stamp overlay ON or OFF.
- **CameraLogin:** Enter the camera login name.
- **CameraPassword:** Enter the camera password.
- **CameraServerName:** Enter the IP address of the camera.
- **ImageParameterString:** Enter the desired resolution and rotation of the time stamp.
- **OverviewImageDelay:** Enter the time delay between the plate read and the overview image.
- **TimeStampOverlayColor:** Select a color for the overlay.
- **TimeStampOverlayFormat:** Format for the time stamp.
- **TimeStampOverlayPosition:** Select the position of the overlay in the image.
- **TimeStampOverlaySize:** Use the slider to increase or decrease the size of the overlay.

Plugin - Scofflaw mdt in Patroller Config Tool

This section lists the options in the Scofflaw mdt tab of the Plugins page.

- **Plate type:** Displays the plate type with one letter. This is only for Philadelphia specifications.
- **Queries path:** Displays the path on the local machine for storing text files with accepted hits.

User interface page in Patroller Config Tool

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.

User interface - General tab in Patroller Config Tool

Configure the settings related to how Patroller is displayed.

- **System unit:** Displays speed and distance in metric or U.S. system (for example, km/h or mph).
- **Default plate state:** Displays the default state or province when you enter a plate manually.

  NOTE: You should enter the state's abbreviation (for example, NY, QC, and so on), not the full name.
- **Enable virtual keyboard:** Turn on for Patroller to display an onscreen keyboard when you need to enter text. The onscreen keyboard appears when you tap or click in a text field.
- **Circle plate:** Turn on for Patroller to circle license plates in the context images.
- **Show overview label:** Turn on to display the overview label if the overview image exists.
- **Enable reviews:** Turn on to allow users to review reads or hits in the Patroller user interface.
- **Show plate lists on startup:** Turn on to automatically display the list of downloaded files (hotlists and permit lists) when Patroller starts up.
- **Enable manual capture:** Turn on to enable Manual capture in Patroller. This allows users to manually enter a license plate, and select the camera that captured it.

User interface - System tab in Patroller Config Tool

Configure the settings related to how Patroller behaves.

- **Enable minimize button:** Turn on to allow the Patroller window to be minimized.
- **Enable system tray menu:** Turn on to enable the Patroller menu located in the Windows system tray (right-click the Patroller icon in the system tray for more options).
- **Start application minimized:** Turn on to start Patroller with the window minimized. This option is not recommended if you log with a username and/or password.
- **Silent mode:** Turn on to enable silent mode. In this mode, the Patroller window starts and stays minimized until a hit is generated. After acknowledging the hit, Patroller returns to a minimized state.
- **Enable main buttons:** Turn on to enable the *Disabled, Hit, Zone, ShowDue, Manual Capture*, and *Cameras* buttons.

  NOTE: For the Street Sweeper plugin, you need to disable this setting.
- **Show taskbar when fullscreen:** Turn on to show the Windows taskbar when Patroller is full screen.
- **Enable printing:** Turn on to enable printing of read/hit information from the Patroller window.
- **Show username in tray:** Turn on to show the Patroller user's Security Center username in the notification bar.

  NOTE: If you're using Patroller for parking enforcement, you can turn this option off to make room for long enforcement rule names.
- **Show Patroller name in tray:** Turn on to show the Patroller's unit name in the notification bar.

NOTE: If you're using Patroller for parking enforcement, you can turn this option off to make room for long enforcement rule names.

Advanced page in Patroller Config Tool

The *Advanced* page allows you to configure advanced Patroller options. Advanced settings in Patroller Config Tool are used mostly by Genetec for diagnostic, debugging, and testing purposes. Most AutoVu™ deployments do not require advanced options to be modified.

IMPORTANT: The only settings that you should modify are the logging settings under the *Traces* section. For all the other advanced settings, contact your Genetec representative before you attempt to modify them.

6

Patroller SimpleHost

This section includes the following topics:

About Patroller SimpleHost

SimpleHost is a WCF service in Genetec AutoVu Patroller that allows an external third party application to retrieve hits and reads, in an XML format, from the AutoVu Patroller. It also allows to push New Wanted entries to the Patroller.

What is the AutoVu SimpleHost service?

Communication to the service is done through an Ethernet connection, and the service connection is configured using Microsoft Visual Studio.

About the contract

The SimpleHost service uses .NET WCF to offer SOAP based access to the AutoVu Patroller database. A contract is defined to identify the data access available to client applications.

Example:

```
[ServiceContract(Name="SimpleHost", Namespace="http://autovu.com")]
public interface ISimpleHostContract
{
  [OperationContract]
  string GetLatestXGuidAndPlateNumber(int lastX);

  [OperationContract]
  string GetHitData(Guid hitGuid);

  [OperationContract]
  void AddNewWanted(string plateNumber, string plateState,
                    int expirationDuration);

  [OperationContract]
  List <Guid> GetReadIds(DateTime from, DateTime to);

  [OperationContract]
  string GetReadData(Guid readGuid);

  [OperationContract]
  void RaiseHit(Guid readGuid, string hitPlateNumber,
                string hitPlateState,
                string category, HitColorEnum hitColor,
                string attributeKeyValuePairs);
}
```

Granting administrator privileges to connect to the SimpleHost service

Before you can connect your application to the SimpleHost service, you'll need to explicitly grant the user administrator privileges to the Simplehost ports and addresses using Netsh.exe tool.

To grant administrator privileges to the user:

1 Make sure that the user has an administrator account on the computer.

2 Right-click the Command prompt, and then click **Run as administrator**.

3 At the command prompt, type:

netsh http add urlacl url=http://+:8001/SimpleHost/ user=<domain>| <user>

Replacing <domain> and <user> with the computer domain and user name respectively.

NOTE: To remove this permission, use the following command:

netsh http delete urlacl url=http://+:8001/SimpleHost/

4 Restart Patroller

You are now ready to connect to the SimpleHost service.

Connecting to Patroller SimpleHost service

To get or push read and hit data through the SimpleHost service, you need to connect to a WCF service using your Visual Studio project.

Before you begin

- Make sure the user can listen to the SimpleHost port and address.
- Open Patroller to activate the service.

What you should know

In this procedure, you will use Microsoft Visual Studio 2013 to automatically generate code to connect to a WCF service. There is no need to use an existing AutoVu DLL.

To connect your application to the SimpleHost service:

1 Open Visual Studio.

2 In the **Visual Studio Solution Explorer**, right-click on the project that references the SimpleHost service, then select **Add Service Reference**.

3 In the **Address** field, enter the URL of the SimpleHost service. Click **Go**.

If the SimpleHost service is running on the same computer, the address is:

http://localhost:8001/SimpleHost

If the SimpleHost service is running, the SimpleHost web service will appear in the Services box. You can expand it to see the functions it contains.

4 Enter a namespace for the auto-generated code that is more descriptive than its default *ServiceReference1*, then click **OK**.

In the following example, we use the name AutoVu.SimpleHost.Service.

New auto-generated code will be added to your project. The following example code shows how to use the service from within a class of your application:

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using System.Xml;
using System.IO;
namespace Test2008
{
  public partial class Form1 : Form
  {
      AutoVu.SimpleHost.Service.SimpleHostClient _simpleHost;
      public Form1()
      {
          InitializeComponent();
      }
      private void buttonGetHit_Click(object sender, EventArgs e)
      {
          string lXml;
          try
          {
             lXml = _simpleHost.GetHitData
               (new Guid("48E6B5C7-0347-470F-9A95-9650AA7EB568"));
          }
          catch (Exception e1)
```

```
          {
             Console.WriteLine(e1.Message);
             return;
          }
      }
      private void buttonInit_Click(object sender, EventArgs e)
      {
          _simpleHost =
            new AutoVu.SimpleHost.Service.SimpleHostClient
                              ("BasicHttpBinding_SimpleHost");
        // the string passed to the constructor is the name of
        // the configuration that was generated in the
        // App.config file.
      }
  }
}
```

5 In your project or the main project of the application, find the App.config file.

NOTE: The App.config file must be the one in the Startup project of the solution, otherwise the configuration will not apply.

The autogenerating code process should have added a system.serviceModel tag to the content of the file:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <system.serviceModel>
        <bindings>
            <basicHttpBinding>
                  <binding name="BasicHttpBinding_SimpleHost"
                        closeTimeout="00:01:00"
                        openTimeout="00:01:00"
                        receiveTimeout="00:10:00"
                        sendTimeout="00:01:00"
                        allowCookies="false"
                        bypassProxyOnLocal="false"
                        hostNameComparisonMode="StrongWildcard"
                        maxBufferSize="65536"
                        maxBufferPoolSize="524288"
                        maxReceivedMessageSize="65536"
                        messageEncoding="Text"
                        textEncoding="utf-8"
                        transfer Mode="Buffered"
                        useDefaultWebProxy="true">
                      <readerQuotas maxDepth="32"
                                  maxStringContentLength="8192"
                                  maxArrayLength="16384"
                                  maxBytesPerRead="4096"
                                  maxNameTableCharCount="16384" />
                      <security mode="None">
                          <transport clientCredentialType="None"
                                     proxyCredentialType="None"
                                     realm="" />
                          <message clientCredentialType="UserName"
                                     algorithmSuite="Default" />
                       </security>
                  </binding>
            </basicHttpBinding>
        </bindings>
        <client>
            <endpoint address="http://localhost:8001/SimpleHost/"
                 binding="basicHttpBinding"
                 bindingConfiguration="BasicHttpBinding_SimpleHost"
                 contract="AutoVu.SimpleHost.Service.SimpleHost"
                 name="BasicHttpBinding_SimpleHost" />
        </client>
   </system.serviceModel>
</configuration
```

6 Replace the *readerQuotas* tag with the following, and then save the project file.

The default configuration does not allow a large amount of data to be transferred in one message, which we need when we transfer the images.

```
<readerQuotas maxDepth="2147483647"
              maxStringContentLength="2147483647"
              maxArrayLength="2147483647"
              maxBytesPerRead="2147483647"
              maxNameTableCharCount="2147483647" />
```

7 Compile and run the project

The string received from the SimpleHost is XML compliant and can be analysed using the .NET XmlDocument class. Also the images need to be re-encoded as a byte[] to create a bitmap object. See the following code:

```
private void ButtonGetHit_Click(object sender, EventArgs e)
{
   string lXml;
   XmlDocument lDoc = new XmlDocument();
   lXml = _simpleHost.GetHitData
          (new Guid("4E6B5C7-0347-470F-9A95-9650AA7EB568"));
   lDoc.LoadXml(lXml);
   XmlNodeList listXmlImages =
          lDoc.SelectNodes(string.Format("{0}/{1}/{2}/{3}",
                     "AutoVuReturn","Hit", "Vehicle","Image"));
   foreach (XmlNode node in listXmlImages)
   {
      XmlNode purposeNode = node.SelectSingleNode("Purpose");
      XmlNode dataNode = node.SelectSingleNode("Data");
      byte[] imageData = Covert.FromBase64String(dataNode.InnerXml);
      MemoryStream lMemoryStream = new MemoryStream(imageData);
      Bitmap image = new Bitmap(lMemoryStream);
      switch (purposeNode.InnerXml)
      {
          case "LPR":
          image.Save("Image_LPR.jpg");
          break;
          case "Context":
          image.Save("Image_Context.jpg");
          break;
      }
      image.Dispose();
   }
}
```

Getting data from Patroller SimpleHost service

You can retrieve read and hit data from the Patroller SimpleHost service using predefined functions. You can also push New Wanted entries and raise hits.

Six functions defined in the SimpleHost contract are available to get data from, or push data to, the Patroller:

- GetReadData
- GetReadIds
- GetLatestXGuidAndPlateNumber
- GetHitData
- AddNewWanted
- RaiseHit

The definition of each XML tags returned by the function calls is explained in XML tag descriptions for Patroller SimpleHost on page 111.

SimpleHost functions description

- **GetReadData:** The method *GetReadData* will return all relevant information required about a plate read. The following is an example of the XML returned by a call to this function.

```
<AutoVuReturn>
    <Vehicle>
        <PlateNumber>ABC123</PlateNumber>
        <TimeStamp>12/3/2013 8:15:08 AM</TimeStamp>
        <UnitName>Unit 1</UnitName>
        <UserName>Default user</UserName>
        <Attributes
            State="QC" CameraOrientation="3" ReadType="1" />
    </Vehicle>
</AutoVuReturn>
```

- **GetReadIds:** The method *GetReadIds* will return the unique identifiers (GUID) of all reads between the 'from' and 'to' parameters.
- **GetLatestXGuidAndPlateNumber:** The method GetLatestXGuidAndPlateNumber will return an XML string listing the last number of hits that were raised. The following is an example of the XML returned by a call to this function.

```
<AutoVuReturn>
    <Hit>
        <HitID>B117F607-8367-40BD-BB18-99230A4F0569</HitID>
        <Vehicle>
            <PlateNumber>YUI765</PlateNumber>
        </Vehicle>
    </Hit>
    <Hit>
        <HitID>BB5B4B67-5080-4E0A-AB0B-0159CF646459</HitID>
        <Vehicle>
            <PlateNumber>420RFA</PlateNumber>
        </Vehicle>
    </Hit>
    <Hit>
        <HitID>E86DFD41-BA15-446A-B902-83A51EF872E6</HitID>
        <Vehicle>
            <PlateNumber>9476073</PlateNumber>
        </Vehicle>
```

```
    </Hit>
    <Hit>
        <HitID>FE8B1F23-B8D6-4025-A9CE-6030F34FE097</HitID>
        <Vehicle>
            <PlateNumber>6549330</PlateNumber>
        </Vehicle>
    </Hit>
</AutoVuReturn>
```

- **GetHitData:** The function *GetHitData* returns all the data related to a hit, including the 64-bit encoded images that are associated to the hit. The function needs the GUID of the hit to retrieve the hit data. The GUID is retrieved using the function GetLatestXGuidAndPlateNumber. The following examples show the XML returned by this function.

  XML example for a hotlist hit

```
<AutoVuReturn>
    <Hit>
        <HitID>7A17CA80-79CC-46FF-8480-AEE4C71E0F2F</HitID>
        <HitCategory>Scofflaw</HitCategory>
        <HotlistPlateState>QC</HotlistPlateState>
        <UserAction>Enforced</UserAction>
        <Vehicle>
            <PlateNumber>QAZWSX</PlateNumber>
            <TimeStamp>9/9/2008 3:13:28 PM</TimeStamp>
            <UnitName>Unit 1</UnitName>
            <UserName>Default user</UserName>
            <Location>
                <Latitude>-73.6065188673537</Latitude>
                <Longitude>45.5278538806699</Longitude>
                <Heading>18.3796565908587</Heading>
                <Address>Av Viaduc Rosemont-Van Horne</Address>
                <ToStreet>Rue St-Urbain</ToStreet>
                <FromStreet>Rue Viaduc Rosemont-Van Horne</FromStreet>
            </Location>
            <Image>
                <Purpose>LPR</Purpose>
                <CameraName>Left LPR</CameraName>
                <Data>*</Data>
            </Image>
            <Image>
                <Purpose>Context</Purpose>
                <CameraName>Left context</CameraName>
                <Data>*</Data>
            </Image>
            <Attributes ReadType="1" />
        </Vehicle>
        <Attributes HitType="Hotlist" />
    </Hit>
</AutoVuReturn>
```

  XML example for an overtime hit.

  An overtime hit contains a second vehicle since we need two LPR reads to initiate an overtime hit.

```
<AutoVuReturn>
    <Hit>
        <HitID>E20AB636-C516-4CAD-BD91-72FFF07582B4</HitID>
        <UserAction>Enforced</UserAction>
        <Vehicle>
            <PlateNumber>123456</PlateNumber>
            <TimeStamp>9/9/2008 3:07:52 PM</TimeStamp>
            <UnitName>Unit 1</UnitName>
            <UserName>Default user</UserName>
            <Location>
                <Latitude>-73.6189690674709</Latitude>
                <Longitude>45.5159273241462</Longitude>
```

```
                <Heading>57.7012353085265</Heading>
                <Address>1726, Av Van Horne</Address>
                <ToStreet>Av Hartland</ToStreet>
                <FromStreet>Av Antonine Maillet</FromStreet>
            </Location>
            <Image>
                <Purpose>LPR</Purpose>
                <CameraName>Left LPR</CameraName>
                <Data>*</Data>
            </Image>
            <Image>
                <Purpose>Context</Purpose>
                <CameraName>Left context</CameraName>
                <Data>*</Data>
            </Image>
            <Attributes ReadType="5"
                           ZoneName="Zone A BF always 2 mins"
                           ZoneColor="-32640" NumberOfViolation="1" />
        </Vehicle>
        <Vehicle2>
            <PlateNumber>123456</PlateNumber>
            <TimeStamp>9/9/2008 3:03:08 PM</TimeStamp>
            <UnitName>Unit 1</UnitName>
            <UserName>Default user</UserName>
            <Location>
                <Latitude>-73.6189097563445</Latitude>
                <Longitude>45.5159931789884</Longitude>
                <Heading>57.7012655931207</Heading>
                <Address>1722, Av Van Horne</Address>
                <ToStreet>Av Hartland</ToStreet>
                <FromStreet>Av Antonine Maillet</FromStreet>
            </Location>
            <Image>
                <Purpose>LPR</Purpose>
                <CameraName>Left LPR</CameraName>
                <Data>*</Data>
            </Image>
            <Image>
                <Purpose>Context</Purpose>
                <CameraName>Left context</CameraName>
                <Data>*</Data>
            </Image>
            <Attributes ReadType="5"
                           ZoneName="Zone A BF always 2 mins"
                           ZoneColor="-32640" />
        </Vehicle2>
        <Attributes HitType="Overtime"
                 VehicleOvertimeGUID=
                       "56cef816-2025-4053-a0d1-341f8346b445" />
    </Hit>
</AutoVuReturn>
```

XML example for a permit hit

```
<AutoVuReturn>
    <Hit>
        <HitID>5F20ACE3-192A-4D3B-BD82-F89B1A995E2A</HitID>
        <UserAction>Enforced</UserAction>
        <Vehicle>
            <PlateNumber>JHJ</PlateNumber>
            <TimeStamp>9/9/2008 2:18:04 PM</TimeStamp>
            <UnitName>Unit 1</UnitName>
            <UserName>Default user</UserName>
            <Location>
                <Latitude>-87.6554201136705</Latitude>
                <Longitude>41.7224790875399</Longitude>
                <Heading>-88.0852803934929</Heading>
                <Address>9438, S Throop St</Address>
                <ToStreet>W 95th St</ToStreet>
```

```
                <FromStreet>W 94th St</FromStreet>
            </Location>
            <Image>
                <Purpose>LPR</Purpose>
                <CameraName>Left LPR</CameraName>
                <Data>*</Data>
            </Image>
            <Image>
                <Purpose>Context</Purpose>
                <CameraName>Left context</CameraName>
                <Data>*</Data>
            </Image>
            <Attributes ZoneColor="0" ReadType="3"
                            ZoneName="Zone1" PolygonName="Zone1" />
        </Vehicle>
        <Attributes HitType="Permit" />
    </Hit>
</AutoVuReturn>
```

- **AddNewWanted:** The *AddNewWanted* function allows to push a New Wanted entry to the Patroller. The plate number must not be empty and have less than 10 characters. The expiration duration must be greater than zero.

  The following example would add to Patroller a New Wanted plate number ABC123 from the Quebec province, valid for 10 days.

  ```
  service.AddNewWanted("ABC123", "QC", 10);
  ```

- **RaiseHit:** This function is used to push a Hit to the Patroller. This is used when the logic that determines if a Read event should generate a Hit is executed by an application outside of Patroller.

  The function requires the following input parameters:

  - **readGuid:** GUID corresponding to a Read guid already existing in the Patroller. This value can be obtained by using the *GetReadIDs* and *GetReadData* SimpleHost functions.
  - **hitPlateNumber:** Plate number that has triggered the hit. For example, if the external application supports fuzzy matching, the Read can be ABC123 and the *hitPlateNumber* can be AB8123.
  - **hitPlateState:** State, country or province associated to the hit. This parameter can be empty.
  - **category:** Hit category determined by the third party application doing the matching.
  - **hitColor:** The hit color. The value must be among the predefined colors of the SimpleHost interface.
  - **attributeKeyValuePairs:** This parameter allows to associate different attributes, with their value, to a Hit. These attributes and values (key value pairs) must be presented in the JSON (JavaScript Object Notation) format.
    The following example shows different possible attributes with values in the JSON format:

    ```
    {"Model":"Honda",
     "Year":"2005",
     "Name":"Doe",
     "Surname":"John",
     "License No.":"123456789"}
    ```

XML tag descriptions for Patroller SimpleHost

XML tags are defined to exchange different type of information with the Patroller SimpleHost service.

The following table describes the SimpleHost tags:

Tag Name	Description
Address	Address where the vehicle read occurred. This field is calculated using the GPS coordinates. The application will not be able to calculate an address for all GPS coordinates.
AddNewWanted	Adds a license plate to Patroller's local hotlist file on the in-vehicle computer.
Attributes	List of attributes of a vehicle read (if within Vehicle or Vehicle2 tag) or a hit (if within a Hit tag).
AutoVuReturn	Root tag used by the SimpleHost Service.
CameraName	Name of the camera that took the image.
Data	64-bit encoded image data. Approximately 2 KB for a LPR image and 50 KB for a context image.
FromStreet	Last perpendicular street. Useful to find the block where the address is located.
Heading	Angle. Direction of the unit taking the reads.
Hit	Contains all the information about a hit.
HitID	Identifier of the hit.
HitType	Type of the hit. Overtime, Permit or Hotlist.
Image	Contains the following information about the image <Purpose>, <CameraName> and <Data>.
Latitude	GPS coordinate of the vehicle read.
Location	Contains information about the vehicle read location and address.
Longitude	GPS coordinate of the vehicle read.
NumberOfViolations	(Overtime hits only) A zone can give more than one hit to a parked car. This field contains the number of hits a vehicle can incur in the current zone.
PlateNumber	Plate number of the vehicle read.
Purpose	Purpose of the image. Can have the following values: LPR, Context, Tire, and Overview.
ReadType	The type of the read based on a set of binary flags since more than one hit type can be activated at a time. Standard (Hotlist) = 1, Permit=2, Overtime=4. Example: Standard + Overtime = 5.

Tag Name	Description
TimeStamp	Date and time at which the read was done.
ToStreet	Next perpendicular street. Useful to find the block where the address is located.
UnitName	Name/identifier of the vehicle running the application.
UserAction	How the user responded to the hit (None, Enforced, NotEnforced, Rejected). None means no user action occurred.
UserName	Name/identifier of the user connected to the application.
Vehicle	(Overtime enforcement only) Contains all the information about the second plate read in an overtime enforcement scenario. **NOTE:** An overtime hit is the result of two plate reads, the second read triggering the hit.
Vehicle2	(Overtime enforcement only) References all the information about the first plate read in an overtime enforcement scenario. The Vehicle tag contains all the information about the second vehicle read (which triggers the hit).
VehicletagOvertimeGUID	(Internal use) GUID of the second vehicle.
ZoneColor	Color of the Zone. Used in the map display in BackOffice and Patroller.
ZoneName	Name of the zone that was activated at the time of the vehicle read.

Glossary

A

authorized user — An authorized user is a user who can see (has the right to access) the entities contained in a partition. Users can only exercise their privileges on entities they can see.

access right — An access right is the basic right users must have over any part of the system before they can do anything with it. Other rights, such as viewing and modifying entity configurations, are granted through privileges. In the context of Synergis, an access right is the right granted to a cardholder to pass through an access point at a given date and time.

action — An action is a user-programmable function that can be triggered as an automatic response to an event, such as door held open for too long or object left unattended, or that can be executed according to a specific time table.

active alarm — An active alarm is an alarm that has not yet been acknowledged.

Active Directory — Active Directory is a directory service created by Microsoft, and a type of role that imports users and cardholders from an Active Directory and keeps them synchronized.

Activity trails — Activity trails is a type of maintenance task that reports on the user activity related to video, access control, and LPR functionality. This task can provide information such as who played back which video recordings, who used the Hotlist and permit editor, who enabled hotlist filtering, and much more.

agent — An agent is a subprocess created by a Security Center role to run simultaneously on multiple servers for the purpose of sharing its load.

alarm — An alarm is a type of entity that describes a particular trouble situation that requires immediate attention and how it can be handled in Security Center. For example, an alarm can indicate which entities (usually cameras and doors) best describe it, who must be notified, how it must be displayed to the user, and so on.

alarm acknowledgement — An alarm acknowledgement is a user response to an alarm. In Security Center, the default acknowledgement and alternate acknowledgement are the two variants of alarm acknowledgements. Each variant is associated to a different

	event so that specific actions can be programmed based on the alarm response selected by the user.
Alarm monitoring	Alarm monitoring is a type of operation task that allows you to monitor and respond to alarms (acknowledge, forward, snooze, and so on) in real time, as well as review past alarms.
Alarm report	Alarm report is a type of investigation task that allows you to search and view current and past alarms.
area	An area is a type of entity that represents a concept or a physical location (room, floor, building, site, and so on) used for grouping other entities in the system.
asset	An asset is a type of entity that represents any valuable object with an RFID tag attached, thus allowing it to be tracked by an asset management software.
Audit trails	Audit trails is a type of maintenance task that reports on the configuration changes of the selected entities in the system and also indicates the user who made the changes.
automatic enrollment	Automatic enrollment is when new IP units on a network are automatically discovered by and added to Security Center. The role that is responsible for the units *broadcasts* a discovery request on a specific port, and the units listening on that port respond with a message that contains the connection information about themselves. The role then uses the information to configure the connection to the unit and enable communication.
AutoVu	AutoVu is the 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	AutoVu LPR Processing Unit is the processing component of the SharpX system. The LPR Processing Unit is available with two or four camera ports, with one dedicated processor per camera (if using SharpX) or per two cameras (if using SharpX VGA). This ensures maximum, per-camera, processing performance. The LPR Processing Unit is sometimes referred to as the *trunk unit* because it is typically installed in a vehicle's trunk.

B

block face (2 sides) — A block face (2 sides) is a type of parking regulation characterizing an overtime rule. A block face is the length of a street between two intersections. A vehicle is in violation if it is seen parked within the same block over a specified period of time. Moving the vehicle from one side of the street to the other does not make a difference.

Breakout box — The breakout box is Genetec's proprietary connector box for AutoVu mobile solutions that use Sharp cameras. The breakout box provides power and network connectivity to the Sharp units and the in-vehicle computer.

broadcast — Broadcast is the communication between a single sender and all receivers on a network.

C

canvas — Canvas is one of the panes found in the Security Desk's task workspace. The canvas is used to display multimedia information, such as videos, maps, and pictures. It is further divided into three panels: the tiles, the dashboard, and the properties.

certificate — Designates one of the following: (1) *digital certificate*; (2) *SDK certificate*.

City Parking Enforcement — City Parking Enforcement is a Patroller software installation that is configured for the enforcement of parking permit and overtime restrictions.

City Parking Enforcement with Wheel Imaging — City Parking Enforcement with Wheel Imaging is a *City Parking Enforcement* installation of a Patroller application that also includes wheel imaging. The use of maps and of the Navigator is mandatory.

Config Tool — Config Tool is a Security Center administrative application used to manage all Security Center users, and configure all Security Center entities such as areas, cameras, doors, schedules, cardholders, Patroller/LPR units, and hardware devices.

Conflict resolution utility — Conflict resolution utility is a tool that helps you resolve conflicts caused by importing users and cardholders from an Active Directory.

context camera — A context camera is a camera connected to an LPR unit that produces a wider angle color image of the vehicle whose license plate was read by the LPR camera.

Copy configuration tool — The Copy configuration tool helps you save configuration time by copying the settings of one entity to many others that partially share the same settings.

covert hit — A covert hit is a read (captured license plate) that is matched to a covert hotlist. Covert hits are not displayed on the Patroller screen, but can be displayed in Security Desk by a user with proper privileges.

covert hotlist — A covert hotlist is a hotlist hidden from the AutoVu Patroller users. Reads matching a covert hotlist generate covert hits.

custom event — A custom event is an event added after the initial system installation. Events defined at system installation are called system events. Custom events can be user-defined or automatically added through plugin installations. Unlike system events, custom events can be renamed and deleted.

custom field — A custom field is a user defined property that is associated to an entity type and is used to store additional information that is useful to your particular organization.

D

Daily usage per Patroller — Daily usage per Patroller is a type of investigation task that reports on the daily usage statistics of a selected Patroller (operating time, longest stop, total number of stops, longest shutdown, and so on) for a given date range.

dashboard — A dashboard is one of the three panels that belong to the canvas in Security Desk. It contains the graphical commands (or widgets) pertaining to the entity displayed in the current tile.

database server — A database server is an application that manages databases and handles data requests made by client applications. Security Center uses Microsoft SQL Server as its database server.

Data Server — Data Server is the Plan Manager Server module that manages the Plan Manager database where the map configuration is stored.

Directory — Directory is the main role that identifies your system. It manages all entity configurations and system wide settings in Security Center. Only a single instance of this role is permitted on your system. The server hosting the Directory role is called the *main server*, and must be set up first. All other servers you add in Security Center are called *expansion servers*, and must connect to the main server to be part of the same system.

Directory Manager — Directory Manager is the role that manages the Directory failover and load balancing in order to produce the high availability characteristics in Security Center.

Directory server A Directory server is any one of the multiple servers simultaneously running the Directory role in a high availability configuration.

discovery port A discovery port is a port used by certain Security Center roles (Access Manager, Archiver, LPR Manager) to find the units they are responsible for on the LAN. No two discovery ports can be the same on one system.

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

Driver Development Kit Driver Development Kit is a SDK for creating device drivers.

E

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

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

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

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

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

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

F

failover A failover is a backup operational mode in which a role (system function) is automatically transferred from its primary server to a secondary server that is on standby. This transfer between servers occurs only when the primary server becomes

	unavailable, either through failure or through scheduled downtime.
federated entity	A federated entity is any entity that is imported from an independent system through one of the Federation roles.
federated system	A federated system is a independent system (Omnicast or Security Center) that is unified under your local Security Center via a federation role, so that the local users can view and control its entities, as if they belong to the local system.
Federation™	The Federation™ feature joins multiple, independent Genetec™ IP security systems into a single virtual system. With this feature, Security Center users can view and control entities that belong to remote systems, directly from their local Security Center system.

G

Genetec Server	Genetec Server is the Windows service that is at the core of Security Center architecture, and that must be installed on every computer that is part of the Security Center's pool of servers. Every such server is a generic computing resource capable of taking on any role (set of functions) you assign to it.
geocoding	Geocoding is the process of finding associated geographic coordinates (latitude and longitude) from a street address.
ghost Patroller	A ghost Patroller is an entity automatically created by the LPR Manager when the AutoVu license includes the XML Import module. In Security Center, all LPR data must be associated to a Patroller entity or an LPR unit corresponding to a fixed Sharp camera. When you import LPR data from an external source via a specific LPR Manager using the XML Import module, the system uses the ghost entity to represent the LPR data source. You can formulate queries using the ghost entity as you would with a normal entity.
Geographic information system	Geographic information system (GIS) is a system that captures spatial geographical data. Map Manager can connect to third-party vendors that provide GIS services in order to bring maps and all types of geographically referenced data to Security Center.
Global Cardholder Synchronizer	Global Cardholder Synchronizer is a 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).
global entity	A global entity is an 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.
global partition	Global partition is a partition that is shared across multiple independent Security Center systems by the partition owner, called the sharing host.

H

hardware integration package	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.
Hardware inventory	Hardware inventory is a type of maintenance task that reports on the characteristics (unit model, firmware version, IP address, time zone, and so on) of access control, video, intrusion detection, and LPR units in your system.
Health history	Health history is a type of maintenance task that reports on health issues.
Health Monitor	Health Monitor is the central role that monitors system entities such as servers, roles, units, and client applications for health issues.
Health statistics	Health statistics is a type of maintenance task that gives you an overall view of the health of your system.
High availability	High availability is a design approach that enables a system to perform at a higher than normal operational level. This often involves failover and load balancing.
hit	A hit is a license plate read that matches a hit rule, such as a hotlist, overtime rule, permit, or permit restriction. A Patroller user can choose to reject or accept a hit. An accepted hit can subsequently be enforced.
hit rule	Hit rule is a type of LPR rule used to identify vehicles of interest (called "hits") using license plate reads. The hit rules include the following types: hotlist, overtime rule, permit, and permit restriction.
Hits	Hits is a type of investigation task that reports on hits reported within a selected time range and geographic area.
hot action	A hot action is an action mapped to a PC keyboard function key (Ctrl+F1 through Ctrl+F12) in Security Desk for quick access.
hotlist	A hotlist is a type of entity that defines a list of wanted vehicles, where each vehicle is identified by a license plate number, the issuing state, and the reason why the vehicle is wanted (stolen, wanted felon, Amber alert, VIP, and so on). Optional vehicle

	information might include the model, the color, and the vehicle identification number (VIN).
Hotlist and permit editor	Hotlist and permit editor is a type of operation task used to edit an existing hotlist or permit list. A new list cannot be created with this task, but after an existing list has been added to Security Center, users can edit, add, or delete items from the list, and the original text file is updated with the changes.
hotspot	Hotspot is a type of map object that represents an area on the map which requires special attention. Clicking on a hotspot displays associated fixed and PTZ cameras.

I

identity provider	An internet site that administers user accounts and is responsible for generating and maintaining user authentication and identity information. For example, Google administers Gmail accounts to its users, which allows single sign-on access to other websites using one account.
illuminator	An illuminator is a light in the Sharp unit that illuminates the plate, thereby improving the accuracy of the images produced by the LPR camera.
inactive entity	An inactive entity is an entity that is shaded in red in the entity browser. It signals that the real world entity it represents is either not working, offline, or incorrectly configured.
incident	An incident is an unexpected event reported by a Security Desk user. Incident reports can use formatted text and include events and entities as support material.
Incidents	Incidents is a type of investigation task that allows you to search, review, and modify incident reports.
intrusion detection area	An intrusion detection area is a type of entity that corresponds to a zone or a partition (group of sensors) on an intrusion panel.
Intrusion detection area activities	Intrusion detection area activities is a type of investigation task that reports on activities (master arm, perimeter arm, duress, input trouble, and so on) in selected intrusion detection areas.
intrusion detection unit	An intrusion detection unit is a type of entity that represents an intrusion panel (or alarm panel) that is monitored and controlled by Security Center.
Intrusion detection unit events	Intrusion detection unit events is a type of investigation task that reports on events (AC fail, battery fail, unit lost, input trouble, and so on) related to selected intrusion detection units.
Intrusion Manager	Intrusion Manager is a type of role that monitors and controls *intrusion panels* (or alarm panels). It listens to the events

	reported by the intrusion panels, provides live reports to Security Center, and logs the events in a database for future reporting.
intrusion panel	An intrusion panel is 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.
Inventory management	Inventory management is a type of operation task that allows you to add and reconcile license plate reads to a parking facility inventory.
Inventory report	Inventory report is a type of investigation task that allows you to view a specific inventory (vehicle location, vehicle length of stay, and so on) or compare two inventories of a selected parking facility (vehicles added, vehicles removed, and so on).
I/O linking	I/O (input/output) linking is controlling an output relay based on the combined state (normal, active, or trouble) of a group of monitored inputs. A standard application is to sound a buzzer (through an output relay) when any window on the ground floor of a building is shattered (assuming that each window is monitored by a "glass break" sensor connected to an input).
IPv4	IPv4 is the first generation IP protocol using a 32-bit address space.
IPv6	IPv6 is a video unit incorporating a camera.

K

Keyhole Markup Language	Keyhole Markup Language (KML) is a file format used to display geographic data in an Earth browser such as Google Earth and Google Maps.

L

Law Enforcement	Law Enforcement is a Patroller software installation that is configured for law enforcement: the matching of license plate reads against lists of wanted license plates (hotlists). The use of maps is optional.
license key	A license key is the software key used to unlock the Security Center software. The license key is specifically generated for each computer where the Directory role is installed. To obtain your license key, you need the *System ID* (which identifies your system) and the *Validation key* (which identifies your computer).
license plate inventory	A license plate inventory is a list of license plate numbers of vehicles found in a parking facility within a given time period, showing where each vehicle is parked (sector and row).

license plate read — A license plate read is a license plate number captured from a video image using LPR technology.

License Plate Recognition — License Plate Recognition (LPR) is an image processing technology used to read license plate numbers. License Plate Recognition (LPR) converts license plate numbers cropped from camera images into a database searchable format.

live hit — A live hit is a hit matched by the Patroller and immediately sent to the Security Center over a wireless network.

live read — A live read is a license plate captured by the Patroller and immediately sent to the Security Center over a wireless network.

load balancing — Load balancing is the distribution of workload across multiple computers.

logical ID — Logical ID is a unique ID assigned to each entity in the system for ease of reference. Logical IDs are only unique within a particular entity type.

Logons per Patroller — Logons is a type of investigation task that reports on the logon records of a selected Patroller.

long term — Long term is a type of parking regulation characterizing an overtime rule. The *long term* regulation uses the same principle as the *same position* regulation, but the parking period is over 24 hours. No more than one overtime rule may use the long term regulation in the entire system.

LPR camera — A LPR camera is a camera connected to an LPR unit that produces high resolution close-up images of license plates.

LPR Manager — LPR Manager is a type of role that manages and controls Patrollers and fixed Sharp units. The LPR Manager stores the data (reads, hits, GPS data, and so on) collected by the LPR units and Patrollers into a central database for reporting. The LPR Manager is also responsible for updating fixed Sharps and Patrollers in the field with hotfixes, hotlist updates, and so on.

LPR rule — LPR rule is a method used by Security Center and AutoVu for processing a license plate read. An LPR rule can be a hit rule or a parking facility.

LPR unit — A LPR unit is a type of entity that represents a hardware device dedicated to the capture of license plate numbers. An LPR unit is typically connected to an LPR camera and a context camera. These cameras can be incorporated to the unit or external to the unit.

M

macro	A macro is a type of entity that encapsulates a C# program that adds custom functionalities to Security Center.
main server	Main server is the only server in a Security Center system hosting the Directory role. All other servers on the system must connect to the main server in order to be part of the same system. In an high availability configuration where multiple servers host the Directory role, it is the only server that can write to the Directory database.
manual capture	Manual capture is when license plate information is entered into the system by the user and not by the LPR.
manufacturer extension	Manufacturer extension is the manufacturer specific settings for access control units, video units, and intrusion detection units.
Map Generator	Map Generator is a Map Server module that imports raster and vector maps to Plan Manager database.
map link	A map link is a map object that brings you to another map with a single click.
map mode	Map mode is a Security Desk canvas operating mode where the main area of the canvas is used to display a geographical map, for the exclusive purpose of showing LPR events.
map object	Map objects are graphical representations of Security Center entities on your maps. They allow you to interact with your system without leaving your map.
Map Server	Map Server is a Plan Manager Server module that manages the private maps imported by the Plan Manager administrator. Map Server includes two modules: Map Generator and Tile Server.
map view	A map view is a defined display position and zoom level for a given map.
master arm	Master arm is 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.
Mobile Admin	Mobile Admin is a web-based administration tool used to configure the Mobile Server.
Mobile app	Mobile app is the client component of Security Center Mobile installed on mobile devices. Mobile app users connect to Mobile Server to receive alarms, view live video streams, view the status of doors, and more, from Security Center.
Mobile Data Computer	Mobile Data Computer is a tablet computer or ruggedized laptop used in patrol vehicles to run the AutoVu Patroller

	application. The MDC is typically equipped with a touch-screen with a minimum resolution of 800 x 600 pixels and wireless networking capability.
Mobile License Plate Inventory	Mobile License Plate Inventory is the Patroller software installation that is configured for collecting license plates and other vehicle information for creating and maintaining a license plate inventory for a large parking area or parking garage.
Mobile Server	Mobile Server is the server component of Security Center Mobile that connects Mobile apps and Web Clients to Security Center. The Mobile Server connects to Security Center, and synchronizes the data and video between Security Center and supported Mobile client components.
Monitoring	The *Monitoring* task is a type of operation task that you can use to monitor and respond to real-time events that relate to selected entities. Using the *Monitoring* task, you can also monitor and respond to alarms.
Move unit	Move unit tool is used to move units from one manager role to another. The move preserves all unit configurations and data. After the move, the new manager immediately takes on the command and control function of the unit, while the old manager continues to manage the unit data collected before the move.

N

Navigator box	The Navigator box is Genetec's proprietary in-vehicle device that provides GPS coordinates and odometer readings to Patroller. Because it taps into the vehicle’s odometry signal, it is more accurate than a standard GPS device. The Navigator box can be used with any type of AutoVu mobile deployment that requires positioning information, but it is required for City Parking Enforcement with Wheel Imaging.
network	The network entity is used to capture the characteristics of the networks used by your system so that proper stream routing decisions can be made.
network address translation	Network address translation is the process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device, for the purpose of remapping one IP address space into another.
network view	The network view is a browser view that illustrates your network environment by showing each server under the network they belong to.
new wanted	A new wanted is a manually entered hotlist item in Patroller. When you are looking for a plate that does not appear in the

	hotlists loaded in the Patroller, you can enter the plate in order to raise a hit if the plate is captured.
notification tray	The notification tray contains icons that allow quick access to certain system features, and also displays indicators for system events and status information. The notification tray display settings are saved as part of your user profile and apply to both Security Desk and Config Tool.

O

OCR equivalence	OCR equivalence is the interpretation of OCR (Optical Character Recognition) equivalent characters performed during license plate recognition. OCR equivalent characters are visually similar, depending on the plate's font. For example, the letter "O" and the number "0", or the number "5" and the letter "S". There are several pre-defined OCR equivalent characters for different languages.
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	Omnicast compatibility pack is the software component that you need to install to make Security Center compatible with an Omnicast 4.x system.
Omnicast™ Federation™	The Omnicast™ Federation™ role connects an Omnicast™ 4.x system to Security Center. That way, the Omnicast™ entities and events can be used in your Security Center system.
output behavior	An output behavior is a type of entity that defines a custom output signal format, such as a pulse with a delay and duration.
overtime rule	An overtime rule is a type of entity that defines a parking time limit and the maximum number of violations enforceable within a single day. Overtime rules are used in city and university parking enforcement. For university parking, an overtime rule also defines the parking zone where these restrictions apply.

P

parking facility	A parking facility is a type of entity that defines a large parking area as a number of sectors and rows for the purpose of inventory tracking.

parking lot

A parking lot is a polygon that defines the location and shape of a parking area on a map. By defining the number of parking spaces inside the parking lot, Security Center can calculate its percentage of occupancy during a given time period.

parking zone

Parking zone is the 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.

partition

A partition is a type of entity that defines a set of entities that are only visible to a specific group of users. For example, a partition could include all areas, doors, cameras, and zones in one building.

Patroller

1 Patroller is the AutoVu software application installed on an in-vehicle computer. Patroller connects to Security Center and is controlled by the LPR Manager. Patroller verifies license plates read from LPR cameras against lists of vehicles of interest (hotlists) and vehicles with permits (permit lists). It also collects data for time-limited parking enforcement. Patroller alerts you of hotlist or permit hits so that you can take immediate action.
2 Type of entity that represents a patrol vehicle equipped with the Patroller software.

Patroller Config Tool

Patroller Config Tool is the Patroller administrative application used to configure Patroller-specific settings, such as adding Sharp cameras to the in-vehicle LAN, enabling features such as Manual Capture or New Wanted, and specifying that a username and password are needed to log on to Patroller.

Patroller tracking

Patroller tracking is a type of investigation task that allows you to replay the route followed by a Patroller on a given date on a map, or view the current location of Patroller vehicles on a map.

perimeter arm

Perimeter arm is arming an intrusion detection area in such a way that only sensors attributed to the area perimeter set the alarm off if triggered. Other sensors, such as motion sensors inside the area, are ignored.

permit

A permit is a type of entity that defines a single parking permit holder list. Each permit holder is characterized by a category (permit zone), a license plate number, a license issuing state, and optionally, a permit validity range (effective date and expiry date). Permits are used in both city and university parking enforcement.

permit hit	A permit hit is a hit that is generated when a read (license plate number) does not match any entry in a permit or when it matches an invalid permit.
permit restriction	A permit restriction is a type of entity that applies time restrictions to a series of parking permits for a given parking zone. Permit restrictions are only used by AutoVu Patrollers configured for University Parking Enforcement.
Plan Manager	Plan Manager is a module of Security Center that provides interactive mapping functionality to better visualize your security environment.
Plan Manager Client	Plan Manager Client is the client component of Plan Manager that runs as a tile plugin within Security Desk. It enables operators to use maps to monitor and control cameras, doors, and other security devices, and administrators to create map objects.
Plan Manager Server	Plan Manager Server is the server component of Plan Manager that must be hosted by a Security Center Plugin role. Plan Manager Server includes two server modules, Data Server and Map Server, which can be hosted on the same Plugin role or two separate Plugin roles.
Plate Reader	Plate Reader is the software component of the Sharp unit that processes the images captured by the LPR camera to produce license plate reads, and associates each license plate read with a context image captured by the context camera. The Plate Reader also handles the communications with the Patroller and the LPR Manager. If an external wheel imaging camera is connected to the Sharp unit, the Plate Reader also captures wheel images from this camera.
plugin	A plugin is a software module that adds a specific feature or service to a larger system.
Plugin	Plugin is a type of role that hosts a specific plugin.
Point of sale	Point of sale (POS) is a system that typically refers to the hardware and software used for checkouts - the equivalent of an electronic cash register. These systems are used to capture detailed transactions, authorize payments, track inventory, audit sales, and manage employees. Point of sale systems are used in supermarkets, restaurants, hotels, stadiums, casinos, retail establishments.
primary server	Primary server is the default server chosen to perform a specific function (or role) in the system. To increase the system's fault-tolerance, the primary server can be protected by a secondary server on standby. When the primary server becomes unavailable, the secondary server automatically takes over.

private IP address A private IP address is an IP address chosen from a range of addresses that are only valid for use on a LAN. The ranges for a private IP address are: 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.16.255.255, and 192.168.0.0 to 192.168.255.255. Routers on the Internet are normally configured to discard any traffic using private IP addresses.

private task A private task is a saved task that is only visible to the user who created it.

privilege Privileges define what users can do, such as arming zones, blocking cameras, and unlocking doors, over the part of the system they have access rights to.

public task A public task is a saved task that can be shared and reused among multiple Security Center users.

R

Reads Reads is a type of investigation task that reports on license plate reads performed within a selected time range and geographic area.

Reads/hits per day Reads/hits per day is a type of investigation task that reports on license plate reads performed within a selected time range and geographic area.

Reads/hits per zone Reads/hits per zone is a type of investigation task that reports on the number of reads and hits per parking zone for a selected date range.

Report Manager Report Manager is a type of role that automates report emailing and printing based on schedules.

report pane Report pane is one of the panes found in the Security Desk task workspace. It displays query results or real-time events in a tabular form.

reverse geocoding Reverse geocoding is an AutoVu feature that translates a pair of latitude and longitude into a readable street address.

role A role is a software module that performs a specific job within Security Center. Roles must be assigned to one or more servers for their execution.

S

same position Same position is a type of parking regulation characterizing an overtime rule. A vehicle is in violation if it is seen parked at the exact same spot over a specified period of time. Patroller must be equipped with GPS capability in order to enforce this type of regulation.

schedule	A schedule is a type of entity that defines a set of time constraints that can be applied to a multitude of situations in the system. Each time constraint is defined by a date coverage (daily, weekly, ordinal, or specific) and a time coverage (all day, fixed range, daytime, and nighttime).
scheduled task	A scheduled task is a type of entity that defines an action that executes automatically on a specific date and time, or according to a recurring schedule.
Software Development Kit	The Software Development Kit (SDK) allows end-users to develop custom applications or custom application extensions for Security Center.
secondary server	A secondary server is any alternate server on standby intended to replace the primary server in the case the latter becomes unavailable.
Security Center	Security Center is the unified security platform that seamlessly blends Genetec™ security and safety systems within a single innovative solution. The systems unified under Security Center include Genetec™ Omnicast™ IP video surveillance system, Synergis™ IP access control system, and AutoVu™ IP license plate recognition (LPR) system.
Security Center Federation™	The Security Center Federation™ role connects a remote, independent Security Center system to your local Security Center. That way, the remote system's entities and events can be used in your local system.
Security Center Mobile	Security Center Mobile is a feature of 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.
Security Desk	Security Desk is the unified user interface of Security Center. It provides consistent operator flow across all of the Security Center's main systems, Omnicast, Synergis, and AutoVu. Security Desk's unique task-based design lets operators efficiently control and monitor multiple security and public safety applications.
server	A server is a type of entity that represents a server machine on which Genetec Server is installed.
Server Admin	Server Admin is the web application running on every server machine in Security Center that allows you to configure the settings of Genetec Server. Server Admin also allows you to configure the Directory role on the main server.

sharing guest	Sharing guest is when Security Center system gives the rights to view and modify entities shared by another system.
sharing host	Sharing host is when Security Center system owns partitions that are shared with other Security Center systems.
Sharp EX	Sharp EX is the Sharp unit that includes an integrated image processor and supports two standard definition NTSC or PAL inputs for external cameras (LPR and context cameras).
SharpOS	SharpOS is the software component of a Sharp or SharpX unit. SharpOS is responsible for everything related to plate capture, collection, processing, and analytics. For example, a SharpOS update may include new LPR contexts, new firmware, Sharp Portal updates, and updates to the Sharp's Windows services (Plate Reader, HAL, updater service, and so on).
Sharp Portal	Sharp Portal is a web-based administration tool used to configure Sharp cameras for fixed or mobile AutoVu systems. From a web browser, you log on to a specific IP address (or the Sharp name in certain cases) that corresponds to the Sharp you want to configure. When you log on, you can configure options such as selecting the LPR context (e.g. Alabama, Oregon, Quebec, etc), selecting the read strategy (e.g. fast moving or slow moving vehicles), viewing the Sharp's live video feed, and more.
Sharp unit	Sharp unit is Genetec's proprietary LPR unit that integrates license plate capturing and processing components, as well as digital video processing functions, inside a ruggedized casing.
Sharp VGA	Sharp VGA is a Sharp unit that integrates the following components: an infrared illuminator; a standard definition (640 x 480) LPR camera for plate capture; an integrated image processor; an NTSC or PAL color context camera with video streaming capabilities.
SharpX	SharpX is the camera component of the SharpX system. The SharpX camera unit integrates a pulsed LED illuminator that works in total darkness (0 lux), a monochrome LPR camera (1024 x 946 @ 30 fps), and a color context camera (640 x 480 @ 30 fps). The LPR data captured by the SharpX camera unit is processed by a separate hardware component called the AutoVu LPR Processing Unit.
Sharp XGA	Sharp XGA is a Sharp unit that integrates the following components: an infrared illuminator; a high-definition (1024 x 768) LPR camera for plate capture; an integrated image processor; an NTSC or PAL color context camera with video streaming capabilities and optional internal GPS.
SharpX VGA	SharpX VGA is the camera component of the SharpX system. The SharpX VGA camera unit integrates a pulsed LED

	illuminator that works in total darkness (0 lux), a monochrome LPR camera (640 x 480 @ 30 fps), and a color context camera (640 x 480 @ 30 fps). The LPR data captured by the SharpX VGA camera unit is processed by a separate hardware component called the AutoVu LPR Processing Unit.
standard schedule	A standard schedule is a type of schedule entity that may be used in all situations. Its only limitation is that it does not support daytime or nighttime coverage.
Synergis™	Synergis™ is the IP access control system of the Security Center designed to offer end-to-end IP connectivity, from access control reader to client workstation. Synergis™ seamlessly integrates a variety of access control capabilities including, but not limited to, badge design, visitor management, elevator control, zone monitoring and more.
system event	A system event is a predefined event that indicates the occurrence of an activity or incident. System events are defined by the system and cannot be renamed or deleted.
System status	System status is a type of maintenance task that monitors the status of all entities of a given type in real time, and allows you to interact with them.

T

task	A task is the central concept on which the entire Security Center user interface is built. Each task corresponds to one aspect of your work as a security professional. For example, use a monitoring task to monitor system events in real-time, use an investigation task to discover suspicious activity patterns, or use an administration task to configure your system. All tasks can be customized and multiple tasks can be carried out simultaneously.
taskbar	A taskbar is a user interface element of the Security Center client application window, composed of the Home tab and the active task list. The taskbar can be configured to appear on any edge of the application window.
task cycling	A task cycling is a Security Desk feature that automatically cycles through all tasks in the active task list following a fixed dwell time.
task workspace	A task workspace is an area in the Security Center client application window reserved for the current task. The workspace is typically devided into the following panes: canvas, report pane, dashboard, and Logical view.

threat level — Threat level is an emergency handling procedure that a Security Desk operator can enact on one area or the entire system to deal promptly with a potentially dangerous situation, such as a fire or a shooting.

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

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

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

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

tile plugin — A tile plugin is a type of entity that represents an application that runs inside a Security Desk tile.

Tile Server — Tile Server is the Map Server module that answers the map requests issued from Plan Manager Client.

timeline — A timeline is a graphic illustration of a video sequence, showing where in time, motion, and bookmarks are found. Thumbnails can also be added to the timeline to help the user select the segment of interest.

twilight schedule — A twilight schedule is a type of schedule entity that supports both daytime and nighttime coverages. A twilight schedule cannot be used in all situations. Its primary function is to control video related behaviors.

U

unit — A unit is a hardware device that communicates over an IP network that can be directly controlled by a Security Center role. We distinguish four types of units in Security Center:

- Access control units, managed by the Access Manager role
- Video units, managed by the Archiver role
- LPR units, managed by the LPR Manager role
- Intrusion detection units, managed by the Intrusion Manager role

Unit discovery tool — Starting with Security Center 5.4 GA the Unit discovery tool has been replaced by the Unit enrollment tool.

Unit replacement — Unit replacement is a tool that is used to replace a failed hardware device with a compatible one, while ensuring that

	the data associated to the old unit gets transferred to the new one. For an access control unit, the configuration of the old unit is copied to the new unit. For a video unit, the video archive associated to the old unit is now associated to the new unit, but the unit configuration is not copied.
University Parking Enforcement	University Parking Enforcement is a Patroller software installation that is configured for university parking enforcement: the enforcement of scheduled parking permits or overtime restrictions. The use of maps is mandatory. Hotlist functionality is also included.
unreconciled read	A unreconciled read is a MLPI license plate read that has not been committed to an inventory.
user	A user is a type of entity that identifies a person who uses Security Center applications and defines the rights and privileges that person has on the system. Users can be created manually or imported from an Active Directory.
user group	A user group is a type of entity that defines a group of users who share common properties and privileges. By becoming member of a group, a user automatically inherits all the properties of the group. A user can be a member of multiple user groups. User groups can also be nested.
user level	A user level is a numeric value assigned to users to restrict their ability to perform certain operations, such as controlling a camera PTZ, viewing the video feed from a camera, or to stay logged on when a threat level is set. The smaller the value, the higher the priority.

V

validation key	A validation key is a serial number uniquely identifying a computer that must be provided to obtain the license key.
vehicle identification number	A vehicle identification number (VIN) is an identification number that a manufacturer assigns to vehicles. This is usually visible from outside the vehicle as a small plate on the dashboard. A VIN can be included as additional information with license plate entries in a hotlist or permit list, to further validate a hit and ensure that it is the correct vehicle.
virtual zone	A virtual zone is a zone entity where the I/O linking is done by software. The input and output devices can belong to different units of different types. A virtual zone is controlled by the Zone Manager and only works when all the units are online. It can be armed and disarmed from Security Desk.

W

watchdog	Watchdog is a Security Center service installed alongside the Genetec Server service on every server computer. The watchdog monitors the Genetec Server service, and restarts it if abnormal conditions are detected.
Web-based SDK	The Web-based SDK role exposes the Security Center SDK methods and objects as web services to support cross-platform development.
Web Client	Web Client is 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.
Web Map Service	Web Map Service (WMS) is a standard protocol for serving georeferenced map images over the Internet that are generated by a map server using data from a GIS database.
wheel imaging	Wheel imaging is a virtual tire-chalking technology that takes images of the wheels of vehicles to prove whether they have moved between two license plate reads.
widget	A widget is a component of the graphical user interface (GUI) with which the user interacts.
Windows Communication Foundation	Windows Communication Foundation (WCF) is a communication architecture used to enable applications, in one machine or across multiple machines connected by a network, to communicate. AutoVu Patroller uses WCF to communicate wirelessly with Security Center.

Z

zone	A zone is a 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.
Zone activities	Zone activities is a type of investigation task that reports on zone related activities (zone armed, zone disarmed, lock released, lock secured, and so on).
Zone Manager	Zone Manager is a type of role that manages virtual zones and triggers events or output relays based on the inputs configured for each zone. It also logs the zone events in a database for zone activity reports.
Zone occupancy	Zone occupancy is a type of investigation task that reports on the number of vehicles parked in a selected parking zone, and the percentage of occupancy.

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ Technical Information Site:** The latest documentation is available on the Technical Information Site. To access the Technical Information Site, log on to Genetec™ Portal and click Technical Information. Can't find what you're looking for? Contact documentation@genetec.com.
- **Installation package:** The Installation Guide and Release Notes are available in the Documentation folder of the installation package. These documents also have a direct download link to the latest version of the document.
- **Help:** Security Center client and web-based applications include help, which explain how the product works and provide instructions on how to use the product features. Patroller and the Sharp Portal also include context-sensitive help for each screen. To access the help, click **Help**, press F1, or tap the **?** (question mark) in the different client applications.

Technical support

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

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

  Before contacting GTAC or opening a support case, it is recommended to search the Technical Information Site for potential fixes, workarounds, or known issues.

  To access the Technical Information Site, log on to Genetec™ Portal and click Technical Information. Can't find what you're looking for? Contact documentation@genetec.com.

- **Genetec™ Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec™ Lifecycle Management (GLM) documents: EN_GLM_ASSURANCE and EN_GLM_ADVANTAGE.

Additional resources

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

- **Forum:** The Forum is an easy-to-use message board that allows clients and employees of Genetec Inc. to communicate with each other and discuss 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/support/training/training-calendar.

Licensing

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

Hardware product issues and defects

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