AlertVU™

Back Office Administrator's Guide

version 3.12

L-3 Mobile-Vision, Inc.

Table of Contents

Chapter 3: Hotlists (cont'd)

1   Introduction

This manual provides data entry instructions and technical reference information for users of *AlertVU Back Office*, the companion software for the AlertVU license plate reader sold by L3 Mobile-Vision, Inc. AlertVU is used to capture digital images of license plates using either an in-car (mobile) or stationary (fixed) camera system.

This guide is geared primarily towards *administrative* users and other supervisory users.

AlertVU Back Office allows you to search for and view the plate reads or *events* that AlertVU captures via its camera system. You can also use the application to create or import "hotlists." A hotlist is a list of wanted license plates. Once you have a hotlist, you can push that list out to all your AlertVU units.

AlertVU Back Office was designed to run on server-class hardware. It is a web-based application, meaning that you access the software via a standard web browser. You can use either *Internet Explorer* or *Mozilla Firefox* to access AlertVU.

For more information, see:

User Roles

In AlertVU, users are granted access to various system functions by assigning them a *user role*. A user role is simply a group of permissions. Whenever a user logs into AlertVU, the system will grant him access to various system functions according to the user role that's associated with his User ID. As System Administrator, you are responsible for assigning permissions to each user role.

There are two types of user roles: *system-defined* and *custom*, as described below.

System-Defined User Roles

System-defined user role*s* are pre-defined user groups that come standard with AlertVU Back Office. They include:

- ❒ Administrator
- ❒ Officer
- ❒ Supervisor
- ❒ View Only–Event.

These roles are customizable. You can add or remove permissions from them as desired. However, the names of these roles cannot be changed, nor can they be deleted from the system.

Custom User Roles

Custom user roles are user-defined user groups that you can create and then assign any number of permissions to. You can add, change, or delete custom user roles as desired.

User Groups

AlertVU includes a "user groups" option that enables you to group like users together (such as users that share the same role or are in the same department) and assign hotlists to those groups. This feature allows you to assign hotlists to multiple users at the same time.

Permissions

As System Administrator, you need to determine which options you want each *user role* to have access to. If an officer's assigned user role allows him to perform a particular task, he will have access to that function. Otherwise he will *not* have access to that function.

To view the system tasks that are permission-driven, see "Permissions-Driven Tasks" in chapter 7.

L3 Mobile-Vision, Inc.

Logging into the System

This section describes how to login to the AlertVU Back Office application. During installation, your Systems Implementation Specialist (SIS) will provide you with the following login information:
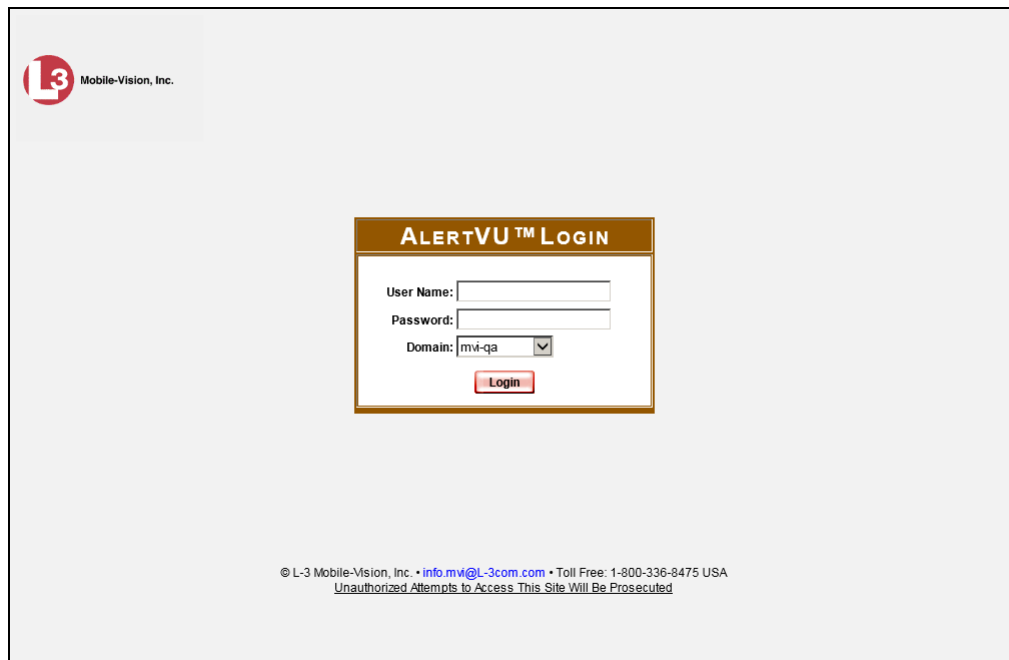
❒ URL needed to access your AlertVU server
❒ User ID
❒ AlertVU User Password (if needed)[*]

1 Double-click on the AlertVU desktop icon.

– OR –

Copy the AlertVU URL into your web browser.

The AlertVU Login screen displays.

If your organization is using the Active Directory Interface, a field labeled *Domain* will also display beneath the *Password* field.

2 Enter your user name in the *User Name* field.

3 Enter your security password in the *Password* field.

---

[*] If your organization is using the Active Directory Integration feature, you will not need a new password for AlertVU, as the application will be integrated with your existing Windows Active Directory or Novell eDirectory.

⇒ If your organization is using the Active Directory Integration feature, this is the same password that you use to login to your regular Windows network or Novell eDirectory.

⇒ If your organization is *not* using the Active Directory Integration feature, this is the initial password that your Systems Installation Specialist (SIS) provided you with.

Passwords are case-sensitive.

4 If the *Domain* field appears on your screen, proceed to the next step. Otherwise skip to step 6.

5 Go to the *Domain* field and select the correct domain name from the drop-down list.

ALertVU™ Login

User Name:
Password:
Domain: mvi-qa
Local Server
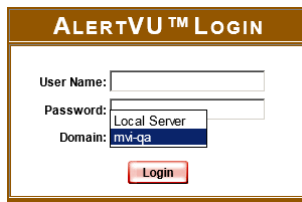
Login

6 Click the **Login** button *or* press **Enter**.

⇒ If the AlertVU Home Page displays (pictured on the next page), **End of Procedure**.

Two-factor
authentication ⇒ If the Authentication Code popup displays (pictured below), it indicates that your agency is using the two-factor authentication feature. This feature requires that you enter an additional code whenever you log into AlertVU Back Office. As soon as you click the **Login** button, the system automatically generates an Authentication Code and sends it to the email address saved in your user record. *Proceed to the next step*.
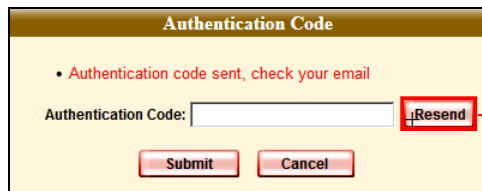
Authentication Code

• Authentication code sent, check your email

Authentication Code: [Resend]

Submit   Cancel

If your Authentication Code expires before you have a chance to click **Submit**, click here to have a new code emailed to you

7 Check your email for a message with the subject line "User Notification." Highlight the Authentication Code contained in this email message, then copy it to your clipboard (**Ctrl + C**).

8 Position your cursor in the *Authentication Code* field, then press **Ctrl + V**.

9 Click **Submit**. The AlertVU Home Page displays.

L3 Mobile-Vision, Inc.

For a detailed description of this page, see "AlertVU Home Page" on page 6.

Changing Your Password

Unless your agency is using the Active Directory Integration feature, you should change your password the first time you login to AlertVU, as described below.

Please note that passwords are case-sensitive.

1 Go to ▼ Home Menu and click **Change Password**. The Enter New Password page displays.
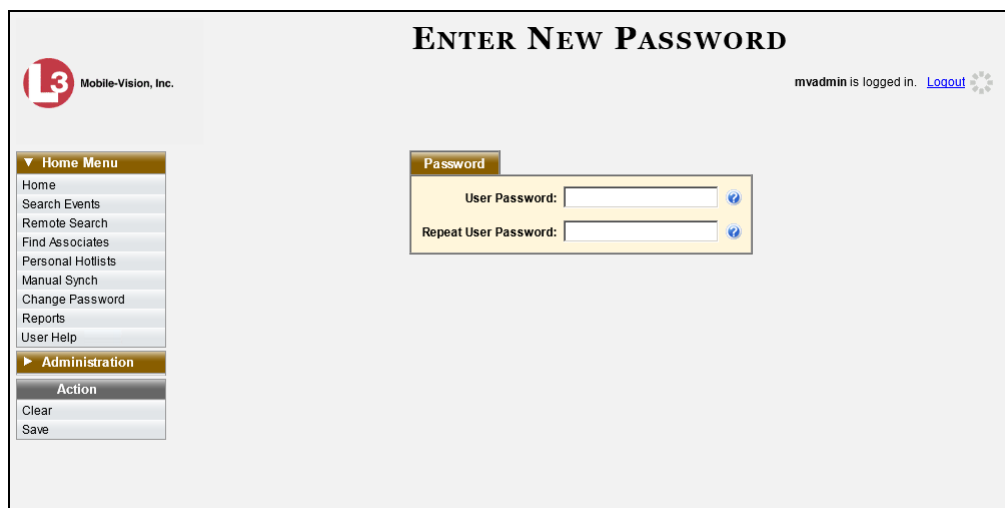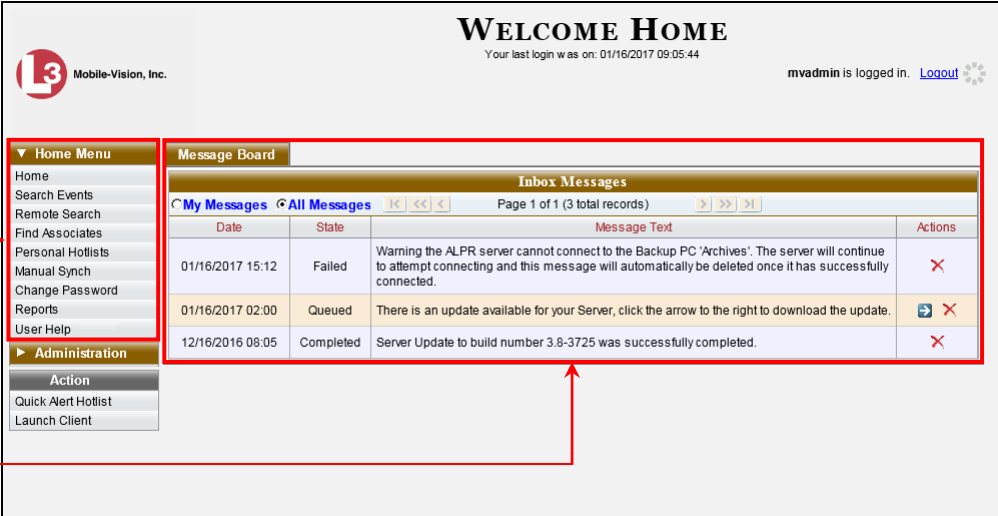
2 Enter your new password in the *User Password* field. For security reasons, your password will not display as you type it.

3 Re-enter your new password in the *Repeat User Password* field.

4 Go to the Action column and click **Save**. A confirmation message displays at the top of the page.

> **Password has been updated**

AlertVU Home Page

The Home Page is divided into two components: a *Main Menu* and a *Message Board*.

The Main Menu is the starting point for all system tasks, such as searching for an event →

The Message Board contains messages sent to you by the system

Message Board

Whenever you login to AlertVU, the Message Board displays. As an administrative user, you will see messages related to system problems and administrative functions.

By default, the system displays the messages that the system sent to *you*. To view all messages for all users, click the *All Messages* radio button.

Main Menu

Search for event(s) that were captured in the same location at the same time as another event

Home Menu	
Home	→ View system messages
Search Events	→ Search for events on your local server
Remote Search	→ Search for events on remote server(s)
Find Associates	
Personal Hotlists	→ Create a license plate list for your own use
Manual Synch	→ Synchronize an AlertVU unit with the local server
Change Password	→ Change your login password
Reports	→ View predefined reports on hotlist hits and plate reads
User Help	→ Search the online help system

View/update AlertVU units

Administration	
System Setup	→ Configure the AlertVU application; change system defaults
System Status	→ View system logs and statuses; access manuals; check for updates
Asset Monitoring	→ View the current status of your AlertVU units
System Hotlists	→ Create a license plate list to push out to all AlertVU units
Import Events	→ Import a license plate list from an AlertVU backup file, event export file, or ELSAG export file
Manage Units	
Manage Users	→ Add/update system users
Manage User Groups	→ Add/update user groups
Manage Locations	→ Define a geographical location that you can apply to hotlists
Manage Hotlist Formats	→ Import new hotlist formats or update existing ones

Action	
Quick Alert Hotlist	→ Send an "Amber Alert" type notification to all AlertVU units
Launch Client	→ Activate the Live Alert utility, used to provide users with "real time" plate capture notifications from other units

Definitions

This section describes some of the key terms and concepts that are central to the AlertVU Back Office application.

Software Concepts

Event

An event is the file that's created when an AlertVU unit captures the digital image of a license plate. Because the same license plate can be read multiple times, some license plate numbers have more than one event record associated with them.

Hotlist

A hotlist is a list of wanted license plates, such as BOLOs, Amber Alerts, persons of interest, etc. There are two types of hotlists in AlertVU: a *personal* hotlist and a *system* hotlist. For more on these hotlist types and how they are used, see "Creating Hotlists" in chapter 3.

Alert

An alert is a notification that the system sends you any time an AlertVU unit receives a possible hit on a license plate that's on either one of your personal hotlists *or* a system hotlist for which you have Notification rights. For more on this topic, see "Alerts" in chapter 3.

Associate

An associate is an event that was captured in the same region and within the same timeframe as another event. The Associates search function allows you to link a suspect with other possible suspects or associates who happened to be in the same region at the same time as your suspect. For more information, see "Searching for Associates" in chapter 3.

User Group

A container that allows you to combine like users for the purpose of assigning hotlists to them.

In-Unit PC Applications

In addition to AlertVU Back Office, your AlertVU LPR system comes with several PC applications that run on the mobile data computers or laptops that are connected to your AlertVU units. Most of these applications run "behind the scenes" to facilitate the capture and transmission of events. Other applications allow you to perform various tasks in the field, as described below.

PC Application	Primary Function
L3 AlertVU Mobile *(mobile units only)*	Enables officers to monitor plate read activity within their vehicles.
AlertVU Proxy	Enables officers to manually synchronize their unit with the server. This involves transferring events from the unit to the server and transferring hotlists from the server to the unit. Because data transmission typically occurs *automatically* without any action on your part, you only need to use this application when a unit has lost its wireless signal for a prolonged period of time. For more on this topic, see "Manually Synchronizing Your Unit with the Server" in chapter 4.

Hardware Components

This user guide focuses on the back office software component of the AlertVU LPR system. However, AlertVU has several *hardware* components as well. These components interface with AlertVU back office, so it's important to understand what each hardware component is and how it relates to the AlertVU system as a whole.

Server

The server is the network computer that hosts the AlertVU back office application and stores all of your event and hotlist data.

AlertVU Unit

An AlertVU unit is the license plate reader that's installed either in a vehicle, such as a patrol car (mobile unit), or on a stationary device, such as a pole (fixed unit). The AlertVU cameras capture digital license plate images and transfer those files to a storage server over a wireless network.

Mobile Data Computer (MDC) or Laptop

Every AlertVU unit is connected to a PC of some kind. AlertVU *mobile* units connect to a mobile data computer. AlertVU *fixed* units connect to a laptop. These PCs control and transmit plate reads to the server via the AlertVU PC applications.

Backup PC

A Backup PC is a computer used to process DVD burn requests. AlertVU comes with an optional backup facility that automatically sends backup burn requests to a *robotic DVD burner*. The resulting archive discs, termed *Certified Backup Discs*, contain system events and hotlists. Because the process of burning DVDs is resource-intensive, one PC is dedicated to this task.

If you are using a *Bravo* robotic DVD burner, then the backup PC is a separate computer workstation connected to the disc burner. If you are using a *Rimage* DVD/Blu-Ray burner that combines a disc burner with a computer, the Backup PC refers to the computer component of the Rimage.

Robotic DVD Burner

A robotic DVD burner is a disc duplicator that burns and labels your *Certified Backup Discs* (see definition below). L3 Mobile-Vision sells two types of burners: the *Bravo*, a stand-alone unit, and the *Rimage*, a combination disc burner/computer. If you have a Rimage, you do not need a separate Backup PC.

Rimage units can burn CDs, DVDs, and Blu-Ray discs. Most Bravo units can burn CDs and DVDs. The higher-end Bravos can burn Blu-Ray discs as well.

Certified Backup Disc (CBD)

A Certified Backup Disc or "CBD" for short is an archive disc. When the archive function is enabled, the system automatically sends CBD burn requests to the Backup PC without any action on your part. These discs contain the event records and hotlists that were previously stored on the server.
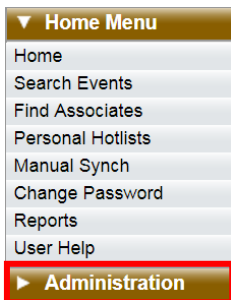
Software Navigation

When you first login to AlertVU, you will see two main menus on the far left of your screen: *Home Menu* and *Administration*. These menus are the starting point for all AlertVU functions. By default, the Home Menu is *maximized* (open) upon login and the Administration menu is *minimized* (closed).
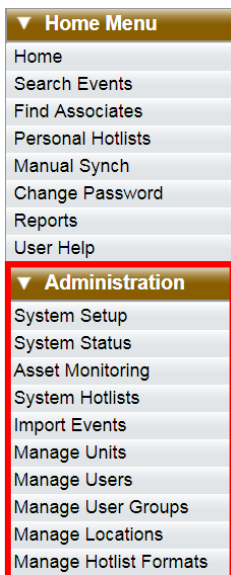
Minimizing/Maximizing Menus

When you click on one of the menu buttons on the left side of your screen, you can toggle back and forth between a minimized (closed) and maximized (open) view.

Minimized menu

When the arrow points RIGHT, the menu options are hidden

Maximized menu

When the arrow points DOWN, the menu options are visible

Scrolling Through Multiple Records

Whenever you search for records in the application (events, hotlists, units, etc.), your search results may yield a large number of records. The following navigation buttons are used to advance forward or backward through a results list.

Button	Description
> <	Next Page/Previous Page. Used to scroll through the search results one page at a time.
>> <<	Fast forward/fast rewind. Used to scroll through the search results ten pages at a time.
I< >I	First Page/Last Page. Used to advance to the first page or last page of the search results, respectively.

Sorting Multiple Records

Whenever you display a list of records, you have the option of changing the manner in which those records are sorted. For example, by default, the Event Search Results Basic View page is sorted by *Event Date*. However, you can change the sort value to *Plate* or *Unit*, as described on the next page.

Plate ▲

To sort a list in *ascending* order—that is, from lowest value to highest value—click *once* on the new column header you wish to sort by. An *up* arrow displays.

– OR –

Plate ▼

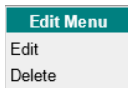To sort a list in *descending* order—that is, from highest value to lowest value—click *twice* on the new column header you wish to sort by. A *down* arrow displays.

Right-clicking on a Row

If you right-click on a row that is editable, the system will display a "shortcut" popup similar to this one:

Edit Menu
Edit
Delete

You can also select these same options from the Action column on the left of your screen.

L3 Mobile-Vision, Inc.

Content Summary

Chapter	Description
1: Introduction	Provides an overview of the *AlertVU Back Office* application and describes key system concepts
2: Events	Describes how to search for, view, report on, and correct event records
3: Hotlists	Describes how to create and update hotlists, hotlist formats, and hotlist locations
4: Units	Describes how to view and update AlertVU units
5: Backups	Describes how to: ▪ Turn the auto-backup feature on/off ▪ Create and update Backup PC records ▪ Customize archive disc labels
6: Utilities	Describes how to perform system maintenance procedures
7: Security	Describes how to: ▪ Create and assign user roles ▪ Define login password parameters ▪ Change the security log settings
8: Users	Describes how to create and update user records and user groups

The manual also includes a glossary and topical index.

2   Events

This chapter describes how to search for and view event records. An event is a *plate read*. Every time an AlertVU unit captures a plate image via an AlertVU camera, that image becomes an event record in the application. Because the same license plate can be read multiple times, some license plate numbers may have more than one event record associated with them.

Each of your AlertVU units has a wireless connection to the AlertVU server. Whenever an in-car or stationary AlertVU unit captures an event, the system transfers that data to the server over a wireless network. This process occurs automatically without any action on your part. Once an event resides on the server, you can access it by logging into the AlertVU Back Office application from your PC workstation.

If you are using AlertVU Mobile, the transmission process may occasionally be delayed when a vehicle moves outside the signal range of the wireless network. As soon as the vehicle comes back within signal range, however, the data will transmit to the server.

For more information, see:

❒   Searching for Events, below
❒   Viewing Event Search Results, page 35
❒   Displaying Event Details, page 51
❒   Viewing/Exporting an Event Report, page 54
❒   Correcting a License Plate Read Error, page 65
❒   Changing Events' Days Online, page 67
❒   Exporting Events, page 69
❒   Importing Events, page 82
❒   Deleting Imported Events, page 84
❒   Extending the Life of an Event, page 86
❒   Canceling an Event Extension, page 88.

Searching for Events

The AlertVU search facility includes several unique features. For example, you can:

❒   Enter more than one set of search criteria.
❒   Limit your search to those events that are included on a specific Hotlist.
❒   Incorporate wildcard characters into your search criteria.
❒   Employ a "fuzzy" search, which enables you to search for characters that appear similar to other characters, such as **Q** and **O** (for more on fuzzy searches, see page 19).
❒   Search for *associates*—events that were captured in the same region during the same time period as another event.

You have the ability to search for events that reside on your agency's local server *or* on a remote server or servers.
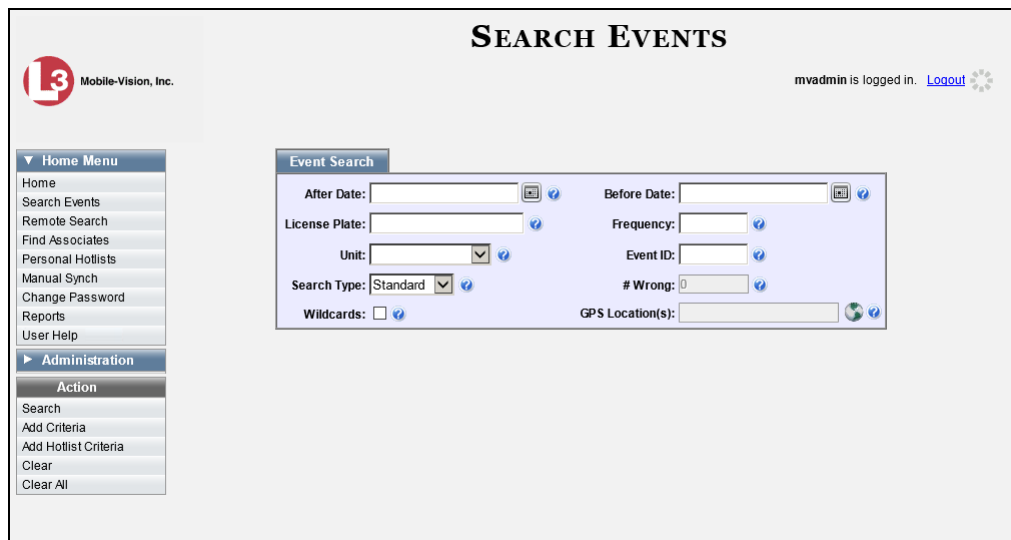
For specific instructions, see:

❒ Searching for Events on Your Local Server, below
❒ Searching for Events on Remote Servers, page 25
❒ Searching for Associates, page 32.

Searching for Events on Your Local Server

This section describes how to search for an event that resides on your agency's AlertVU server. For an overview of the AlertVU search function, see the previous section.

To search for events that are stored on other agencies' servers, see "Searching for Events on Remote Servers" on page 25 instead.

1 Go to ▼ Home Menu and click **Search Events**. The Search Events page displays.

This page is used to enter search criteria, as described in the following table.

L3 Mobile-Vision, Inc.

Event Search	
Search Field	**Description**
After Date	Limits your search to those events that were captured after this date and time. *Select a date from the calendar popup OR enter a date/time directly in mm/dd/yyyy hh:mm:ss format.* Once you enter this field, the system will automatically populate the *Before Date* field with a date/time that is equal to the *After Date*'s **end of day** (i.e., 23:59:59). That's because the *After Date* and *Before Date* fields are typically used in tandem to search for all events that were captured on a particular day. If you prefer an open ended search, simply delete the value in the *Before Date* field.
Before Date	Limits your search to those events that were captured before this date and time. If you entered a value in the *After Date* field, the system will automatically populate this field with a date/time that is equal to the *After Date*'s **end of day** (i.e., 23:59:59). To search for all events that were captured within this time period, leave the *Before Date* value as is. To search for a time range that is longer/shorter than this time period, *select a new date from the calendar popup OR enter a new date/time directly in mm/dd/yyyy hh:mm:ss format.* If you did *not* enter a value in the *After Date* field, *select a date from the calendar popup OR enter directly in mm/dd/yyyy hh:mm:ss format.*
License Plate	Limits your search to those events that match this license plate number. If the *Wildcards* checkbox is also selected, the value you enter here may include the asterisk (*****) and/ or question mark (**?**) wildcard characters. For more information, see *Wildcards* on the next page.
Frequency	Limits your search to those events that were captured a minimum of **X** times. For example, if you enter **2** in this field, the system will search for all plates that your Alert-VU units have captured two or more times.
Unit	Limits your search to those events that were captured by a specific AlertVU unit. *Select this value from the drop-down list provided.*
Event ID	Limits your search to the event that matches this Event ID. An Event ID is a unique identification number that the system automatically assigns to each event.

(Continued)

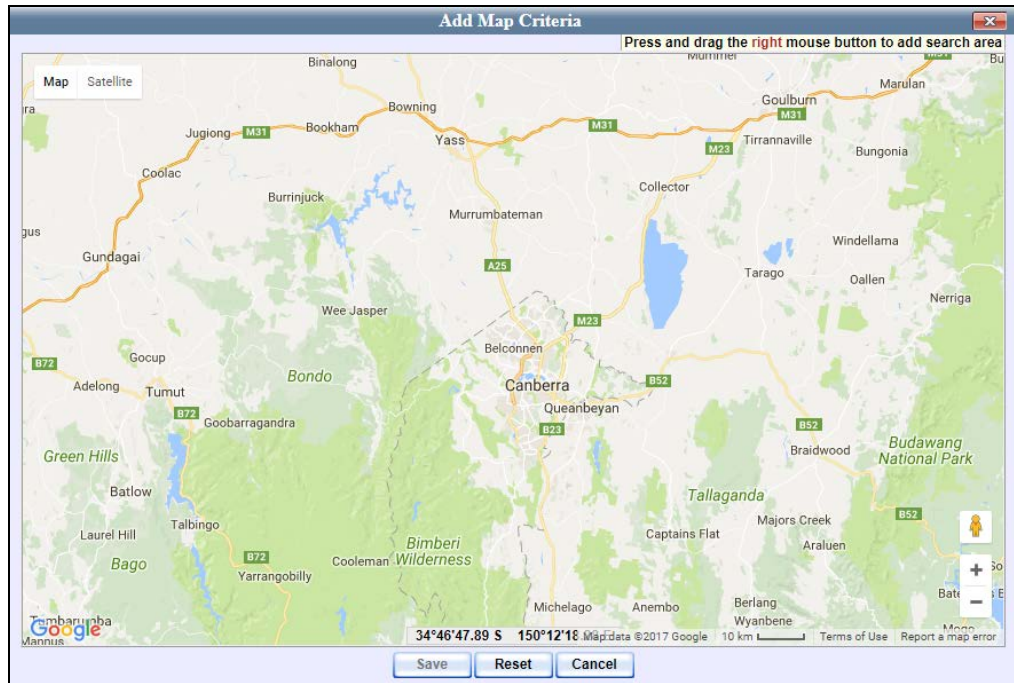| Event Search (cont'd)	
Search Field	**Description**
Search Type	The type of search you wish to perform: ▪ *Standard* (default). A fuzzy "starts with" search that allows for wildcard entries. For more on fuzzy searches, see "What is a 'fuzzy' search?" on page 19. ▪ *Exact*. An exact "starts with" search that allows for wildcard entries. ▪ *Any order*. An exact search that allows you to search for characters in any position (i.e., out of sequential order). For example, if a witness reported seeing a license plate that starts with either **PV7** or **P7V**, you might perform this type of search. ▪ *Mismatch*. A search that allows for a certain number of mismatched characters, as specified in the *# Wrong* field. *Select this value from the drop-down list provided.*
# Wrong	Used in conjunction with the "mismatch" *Search Type* to specify the number of mismatched characters you wish to allow in a search. If the value of the *Search Type* field is something other than **Mismatch**, this field will be disabled (i.e., "grayed-out").
Wildcards (*Standard* or *Exact* search only)	A checkbox used to enable the use of the asterisk (*****) and/or question mark (**?**) wildcards when performing a *Standard* or *Exact* search (see *Search Type* definitions above). Wildcards let you substitute a character in your search for any other character or range of characters: **?** Match *one* of any character, e.g., L62?9N = L6249N ***** Match *one or more* of any character, e.g., L62* = L6249N
GPS Location(s)	Limits your search to a specific geographical location. *Select this location by clicking the 🌐 icon and drawing a box on a map, as described in steps 4 – 5.*

Available Actions	
Action	**Description**
Search	Execute your search.
Add Criteria	Add entered search fields to your list of search criteria. This function allows you to include more than one set of search criteria in your search.
Add Hotlist Criteria	Search within a selected Hotlist only. This type of search will only return events that meet *all* the criteria sets included in your search.
Clear	Remove all entries and selections from the Event Search form.
Clear All	Remove all entries, selections, and added criteria from the Event Search form.

If you enter/select a value in one or more of the search fields, it will narrow your search results. If you leave all fields blank, the system will display all event files that are currently stored on your local server.

> **What is a 'fuzzy' search?** A fuzzy search is one that looks for characters that are similar looking to other characters. This type of search addresses the problem of misreads from the capture device. For example, to the AlertVU capture device, a **6** might look like a **G**, a **Q** might look like an **O**, a **Z** might look like an **2**, etc. If, for instance, there's an event in the system with a plate of **R6Q2KZY**, then fuzzy search results would include not only the exact match to that plate but R GO 2KZY, R GQ2KZY, R6 O 2KZY, R6Q2K 2 Y, R6 O 2K 2 Y, R GO 2K 2 Y, etc.

2 Enter/select the field values you wish to search on, as described in the previous table.

3 To include a geographical location in your search, proceed to the next step. Otherwise skip to step 10.

4 Go to the *GPS Location(s)* field and click the 🌐 icon. The Add Map Criteria popup displays.

(Continued)

This map defaults to the location of your local precinct.

5 To reposition the map, proceed to the next step. Otherwise skip to step 7.

6 Left-click your mouse, then drag the map to the desired position.

7 To zoom in/out on the map, use the plus and minus arrows in the lower right corner of the page. Otherwise proceed to the next step.

8 Press and drag the right mouse button over the area you wish to search in. A shaded box appears in that area. If desired, you may draw more than one box.

9 Click **Save**. The latitudinal and longitudinal coordinates for the area(s) you selected
   display in the *GPS Location(s)* field.

10 To enter another set of search criteria, proceed to the next step. Otherwise skip to
   step 15.

11 Go to the Action column and click **Add Criteria**.

   The set of search criteria you just entered displays on your Search Criteria list.

12 Enter/select the next set of field values you wish to search on.

13 Go to the Action column and click **Add Criteria**. The set of search criteria you just entered displays at the bottom of the page.

14 To add another set of search criteria to your search, repeat steps 12 and 13. Otherwise proceed to the next step.

15 To limit your search to those events that are included on a specific Hotlist, proceed to the next step. Otherwise skip to step 20.

16 Go to the Action column and click **Add Hotlist Criteria**. The Add Hotlist Criteria popup displays.

17 Select a hotlist from the drop-down list provided.

18 To perform a *fuzzy* search (see definition on page 19), proceed to the next step.

– OR –

To perform an *exact match* search, select the *Exact Match* checkbox.

19 Click **Save** to close the popup. The Hotlist displays on your Search Criteria list.

20 Go to the Action column and click **Search**. All events that match your search criteria display on the Events page in either Basic View (typical) or Count View (if you searched on a Hotlist).

For a detailed description of the components on this page, see "Viewing Event Search Results" on page 35.

If you entered multiple lines of search criteria, then what the system selects will depend in part on whether or not you included a hotlist in your search. When you enter multiple sets of search criteria *that do **not** include a hotlist*, the system will select those events that meet any of your criteria sets. When you enter multiple sets of search criteria *that include a hotlist*, the system will first select those events that meet any of your criteria sets, then it will compare those results to your Hotlist. If there are any complete matches (i.e., a UUU90D plate on the preliminary search results list and a UUU90D plate on the Hotlist), your final results will include those plates only.

21 By default, events are sorted chronologically by event date. To sort the results differently, proceed to the next step. Otherwise skip to step 23.

22 Go to the column heading you wish to sort by. For example, if you are in Basic View, go to the *Plate* column.

To sort in *ascending* order—that is, from lowest value to highest value—click the column header *once*. An *up* arrow displays: Plate ▲ .

– OR –

To sort in *descending* order—that is, from highest value to lowest value—click the column header *twice*. A *down* arrow displays: Plate ▼ .

23 If your search yielded more than one page of results (i.e., Page 1 of 6), use the navigation buttons at the top of the page to scroll through the results list.

24 To view an event's details, first make sure the **Basic View** tab is selected. Next, hover your mouse over the *Info* icon to the left of the event.

– OR –

Click on the event record to select it, then go to the Action column and click **Show Detail** (see **HINT** below).

HINT: If you clicked on an event record but the **Show Detail** option is grayed-out, it indicates that you have more than one record selected. Click **Clear Selected**, then reselect the single event you wish to view.

The Event Detail popup displays.

For a detailed description of the components on this popup, see the table beginning on page 52.

Searching for Events on Remote Servers
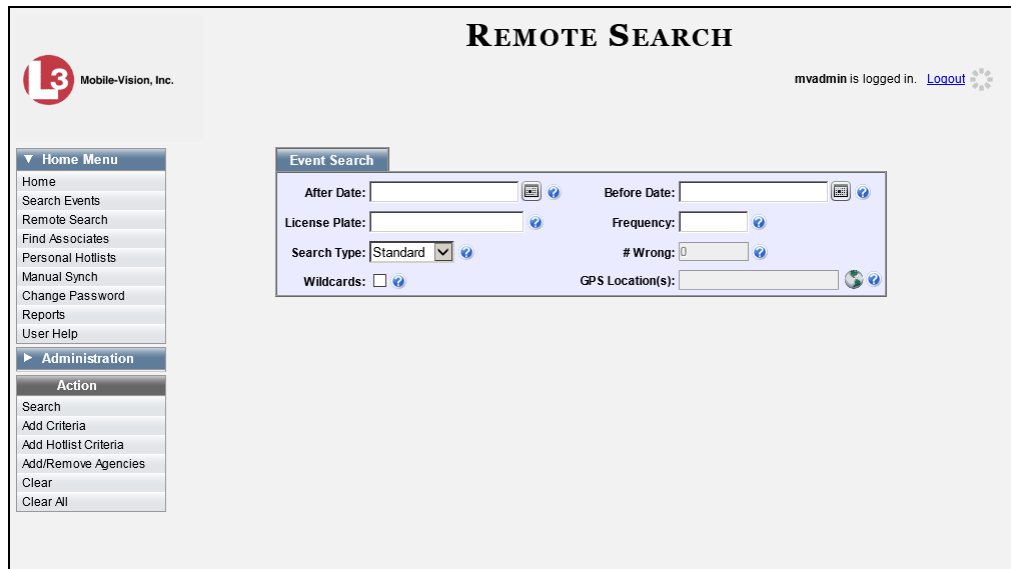
This section describes how to search for an event that resides on other agencies' server(s). You can remotely search both AlertVU databases *and* non-AlertVU databases that conform to NIJ (National Institute of Justice) standards.

To use the remote search function, specific configurations are required on both your local server and the remote servers. For more information, see "Configuring the System to Perform Remote Searches" in chapter 6.

To search for events that are stored on your *local* AlertVU server, see "Searching for Events on Your Local Server" on page 16 instead.

For an overview of the AlertVU search function, see "Searching for Events" on page 15.

1   Go to ▼ Home Menu and click **Remote Search**. The Remote Search page displays.

This page is used to enter search criteria. For a description of the components on this page, see the table on page 17.

If you enter/select a value in one or more of these fields, it will narrow your search results. If you leave all fields blank, the system will display all event files that are currently stored on the selected server(s).

2   Enter/select the field values you wish to search on, as described in the table on page 17.

3   To include a geographical location in your search, proceed to the next step. Otherwise skip to step 10.

4   Go to the *GPS Location(s)* field and click the 🌐 icon. The Add Map Criteria popup displays.
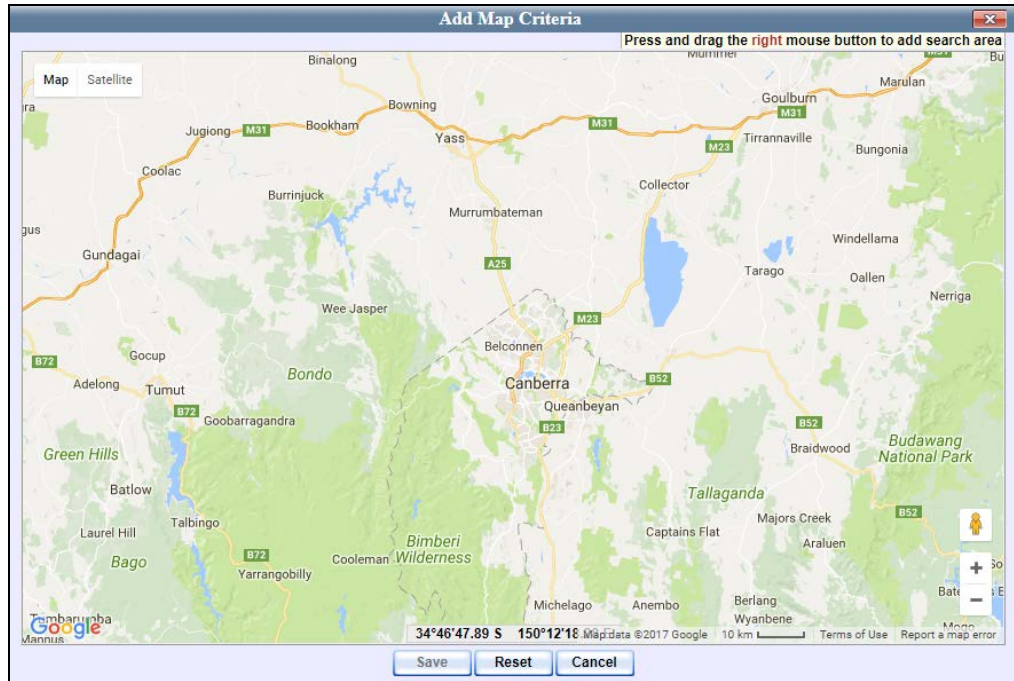
This view defaults to the location of your local precinct.

5   To reposition the map, proceed to the next step. Otherwise skip to step 7.

6   Left-click your mouse, then drag the map to the desired position.

7   To zoom in/out on the map, use the plus and minus arrows in the lower right corner of the page. Otherwise proceed to the next step.

8   Press and drag the right mouse button over the area you wish to search in. A shaded box appears in that area. If desired, you may draw more than one box.

9   Click **Save**. The latitudinal and longitudinal coordinates for the area(s) you selected display in the *GPS Location(s)* field.

10 To enter another set of search criteria, proceed to the next step. Otherwise skip to step 15.

11 Go to the Action column and click **Add Criteria**. The set of search criteria you just entered display on your Search Criteria list.

12 Enter/select the next set of field values you wish to search on.

13 Go to the `Action` column and click **Add Criteria**. The set of search criteria you just entered displays at the bottom of the page.

14 To add another set of search criteria to your search, repeat steps 12 and 13. Otherwise proceed to the next step.

15 To limit your search to those events that are included on a specific Hotlist, proceed to the next step. Otherwise skip to step 20.

16 Go to the `Action` column and click **Add Hotlist Criteria**. The Add Hotlist Criteria popup displays.

17 Select a hotlist from the drop-down list provided.

18 To perform a *fuzzy* search (see definition on page 19), proceed to the next step.

– OR –

To perform an *exact match* search, select the *Exact Match* checkbox.

19 Click **Save** to close the popup. The Hotlist displays on your Search Criteria list.

20 Go to the Action column and click **Add/Remove Agencies**. The Agencies popup displays.

Agencies

Unselected	Selected
Search: ☐ Case	Search: ☐ Case
⏮ ⏪ ◀ 1 of 1 (2) total ▶ ⏩ ⏭	⏮ ⏪ ◀ 1 of 1 (0) total ▶ ⏩ ⏭
MVI-Leslie-Documentation	
Remote Precinct #1	

Save   Cancel
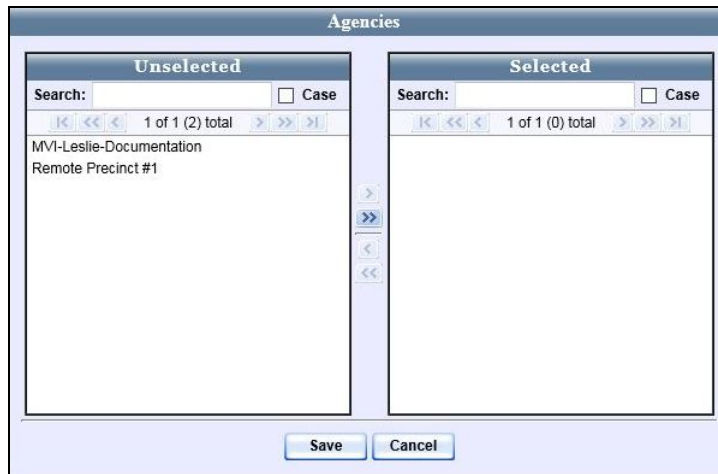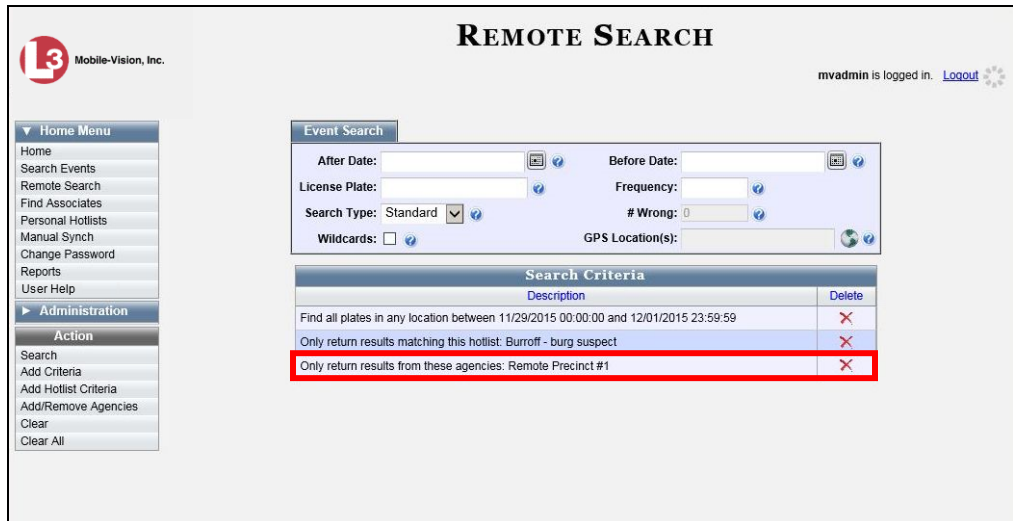
21 Go to the left column (Unselected) and click on each of the agencies you wish to add. If an agency you're looking for does not appear onscreen, use the navigation arrows at the top of the column to scroll through the agency list.

22 Once you've highlighted the desired agency(ies), click the ▶ icon located between the two columns. The selected agency(ies) display in the right column (Selected).

Agencies

Unselected	Selected
Search: ☐ Case	Search: ☐ Case
⏮ ⏪ ◀ 1 of 1 (1) total ▶ ⏩ ⏭	⏮ ⏪ ◀ 1 of 1 (1) total ▶ ⏩ ⏭
MVI-Leslie-Documentation	Remote Precinct #1

Save   Cancel
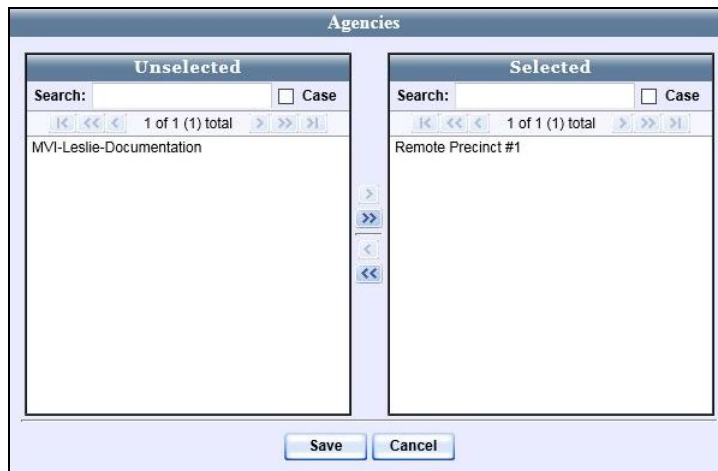
23 Click **Save**. The selected agency(ies) display on your Search Criteria list.

(Continued)

24 Go to the `Action` column and click **Search**. All events that match your search criteria display on the Events page in either Basic View (typical) or Count View (if you searched on a Hotlist).

For a detailed description of the components on the Events page, see "Viewing Event Search Results" on page 35.

L3 Mobile-Vision, Inc.

If you entered multiple lines of search criteria, what the system selects will depend in part on whether or not you included a hotlist in your search. When you enter multiple sets of search criteria *that do **not** include a hotlist*, the system will select those events that meet any of your criteria sets. When you enter multiple sets of search criteria *that include a hotlist*, the system will first select those events that meet any of your criteria sets, then it will compare those results to your Hotlist. If there are any complete matches (i.e., a UUU90D plate on the preliminary search results list and a UUU90D plate on the Hotlist), your final results will include those plates only.

25 By default, events are sorted chronologically by event date. To sort the results differently, proceed to the next step. Otherwise skip to step 27.

26 Go to the column heading you wish to sort by. For example, if you are in Basic View, go to the *Plate* column.

To sort in *ascending* order—that is, from lowest value to highest value—click the column header *once*. An *up* arrow displays: | Plate ▲ |.

– OR –

To sort in *descending* order—that is, from highest value to lowest value—click the column header *twice*. A *down* arrow displays: | Plate ▼ |.

27 If your search yielded more than one page of results (i.e., Page 1 of 6), use the navigation buttons at the top of the page to scroll through the results list.

|◁ ◁◁ ◁   ▷ ▷▷ ▷|

28 To view an event's details, first make sure the **Basic View** tab is selected. Next, hover your mouse over the Info icon to the left of the event.

– OR –

Click on the event record, then go to the Action column and click **Show Detail** (see **HINT** below).

HINT: If you clicked on an event record but the **Show Detail** option is grayed-out, it indicates that you have more than one record selected. Click **Clear Selected**, then reselect the single event you wish to view.

The Event Detail popup displays.

(Continued)

For a detailed description of the components on the Event Details popup, see the table beginning on page 52.

Searching for Associates

Occasionally, you may be interested in knowing if an accomplice or associate was in the same region at the same general time as a suspect. AlertVU can help you search for this type of data using the Associates feature. An associate is an event that is associated with another event based on the following criteria:
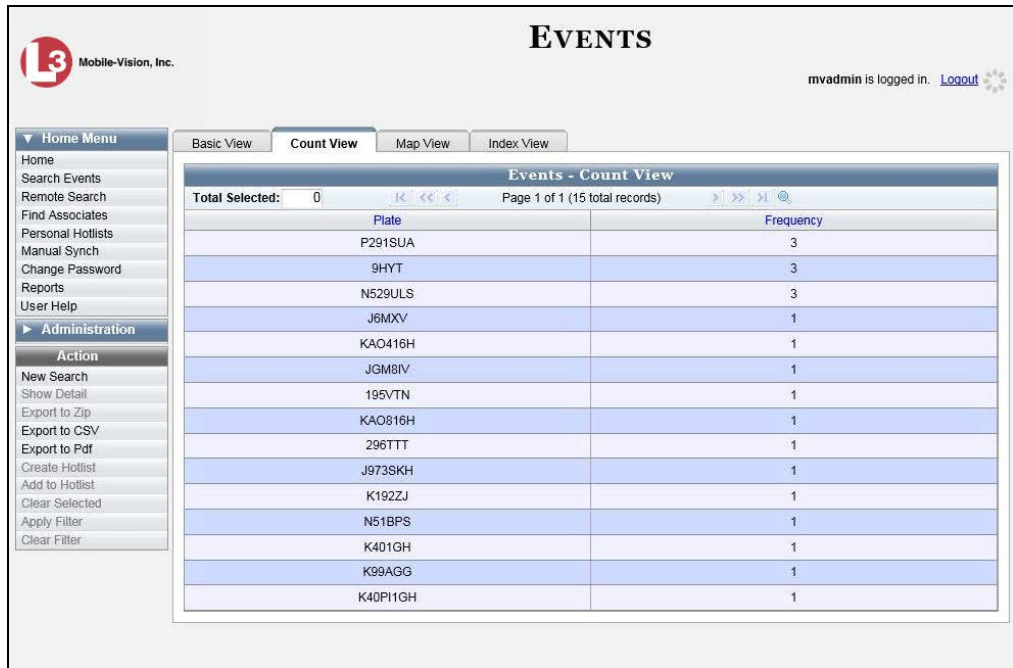
❑ The event was captured during the same time period as the other event.
❑ The event was captured within a 25-yard radius of the other event.

1 Go to ▼ Home Menu and click **Find Associates**. The Find Associates page displays.
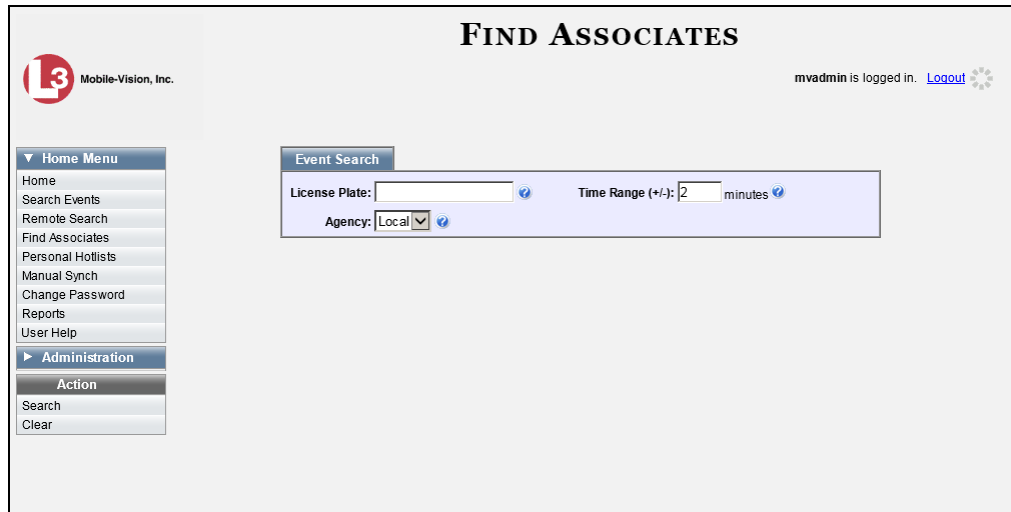
2 Go to the *License Plate* field and enter the **complete** license plate number that you wish to try and match to possible associates/accomplices.

3 Go to the *Time Range* field and enter the time range, in minutes, that you wish to search within. For example, if you're interested in knowing which events were captured within a half hour range of the captured license plate, enter **30** in the *Time Range* field.

4 To search for events stored on your local agency's server (default), proceed to the next step.

– OR –

To search for events stored on an outside agency's server, select an agency from the *Agency* drop-down list.

5 Go to the Action column and click **Search**. All events that match your search criteria (if any) display in Count View.

(Continued)
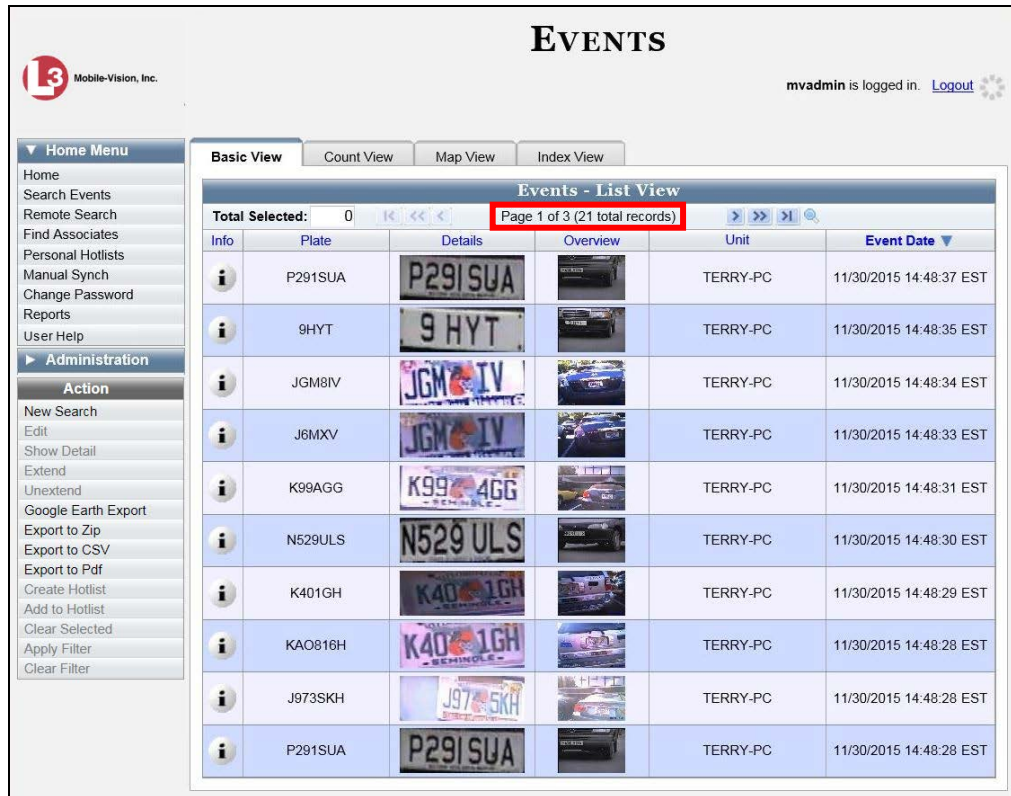
For more information on Count View as well as the other available event views, see the next section, "Viewing Event Search Results."

L3 Mobile-Vision, Inc.

Viewing Event Search Results

After you execute a search, the Events page will display. Note the heading at the top of the events list. This information tells you how many pages are included in your results (e.g., **3**), as well as the total number of event records (e.g., **21**).

To scroll through a multi-page results list, use the navigation buttons at the top of the form.

If your search results yield ten or less events, these buttons will be grayed out.

There are four available views for the Events page: *Basic*, *Count*, *Map*, and *Index*. Each of these views offers different advantages and features, as described in the next four sections. In addition, you have the option of viewing your search results in Google Earth.
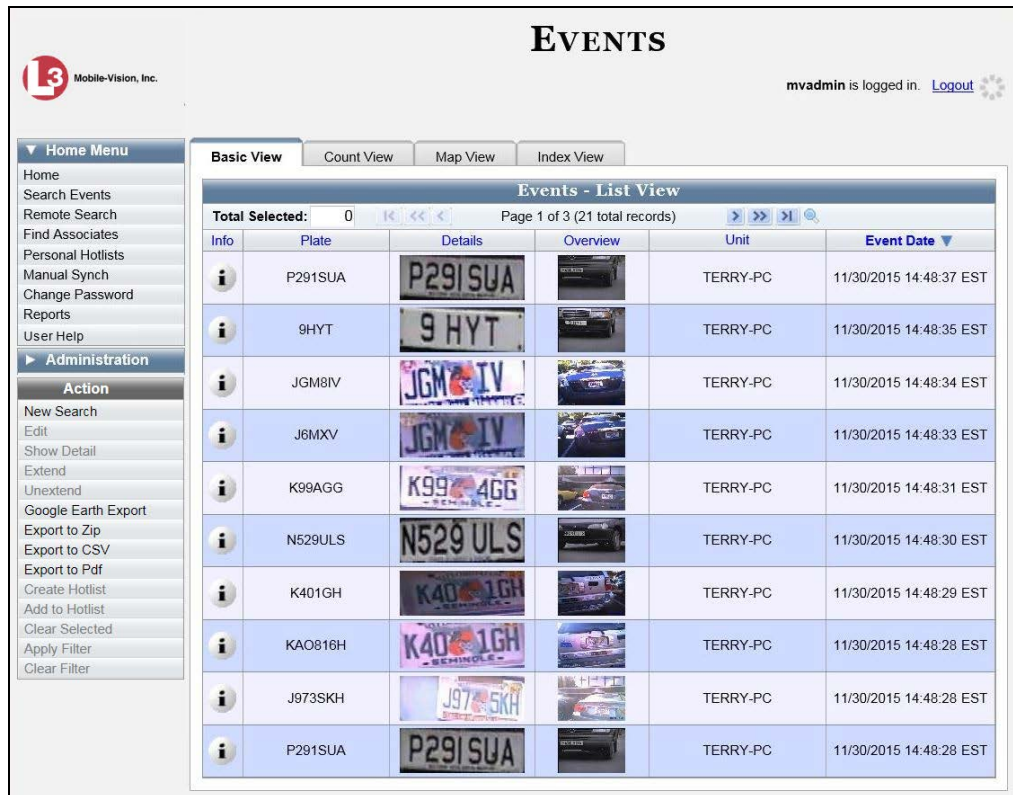
For more information, see:

❐ Viewing Event Search Results in Basic View, next page
❐ Viewing Event Search Results in Count View, page 38
❐ Viewing Event Search Results in Map View, page 41
❐ Viewing Event Search Results in Index View, page 47
❐ Viewing Event Search Results in Google Earth, page 50.

Viewing Event Search Results in Basic View

This section describes how to view a search results list in *Basic* view. This view consists of a table with information about each event.

1 Search for and display the events you wish to view. (If necessary, review "Searching for Events" on page 15.) The Events page displays.

2 If your search yielded more than one page of results (i.e., Page 1 of 6), use the navigation buttons at the top of the page to scroll through the entire plate list.

The components of the Events page in Basic View are described in the following table.

Event Information	
Column	**Description**
Info	The View Event Detail icon. Hover your mouse over this icon to display the Event Detail page.
Plate	The license plate number. If you need to correct this number due to a read error, see "Correcting a License Plate Read Error" on page 65, beginning with step 2.
Details	A close-up image of the license plate.
Overview	A broad angle image of the front or back of the vehicle from which AlertVU captured this license plate.
Unit	The name of the AlertVU unit that captured this license plate.
Event Date	The date and time at which the AlertVU unit captured this license plate. Displays in mm/dd/yyyy hh:mm:ss format.
Available Actions	
If an action is "grayed out" (i.e., unavailable), it indicates that you must select one or more event records first before you can perform that action.	
Action	**Description**
New Search	Return to the Search Events page in order to perform a new search. For instructions, see "Searching for Events on Your Local Server" on page 16 or "Searching for Events on Remote Servers" on page 25, beginning with step 2.
Edit	Change the license plate number for a selected event record on this search results list. For instructions, see "Correcting a License Plate Read Error" on page 65, beginning with step 2.
Show Detail	Display the Event Detail page for a selected event record. (Select one record only.)
Google Earth Export	Download a KLM file in order to display event search results in a stand-alone version of Google Earth. For instructions, see "Viewing Event Search Results in Google Earth" on page 50, beginning with step 2.
Export to Zip	Export selected events to a zip file. For instructions, see "Exporting Event Search Results to a Zip File" on page 70, beginning with step 2.
Export to CSV	Export selected events to a CSV spreadsheet file. For instructions, see "Exporting Event Search Results to a CSV File" on page 74, beginning with step 2.
Export to Pdf	Export selected events to a PDF file. For instructions, see "Exporting Event Search Results to a Pdf File" on page 76, beginning with step 2.

Available Actions (cont'd)	
Action	**Description**
Create Hotlist	Create a new personal Hotlist from selected events. For instructions, see "Creating a Personal Hotlist from Existing Events" in chapter 3, beginning with step 2.
Add to Hotlist	Add selected events to an existing Hotlist. For instructions, see "Adding Events to an Existing Hotlist" in chapter 3, beginning with step 2.
Clear Selected	Deselect all event records that are currently selected.
Apply Filter	Display only those license plate records that are currently selected (i.e., highlighted).
Clear Filter	Undo "Apply Filter" action (i.e., redisplay all events that met the original search criteria).

3 To view an event's details, hover your mouse over the Info icon to the left of the event.

– OR –

Click on the event record, then go to the Action column and click **Show Detail** (see **HINT** below).

HINT: If you clicked on an event record but the **Show Detail** option is grayed-out, it indicates that you have more than one record selected. Click **Clear Selected**, then reselect the single event you wish to view.

The Event Detail popup displays. For a detailed description of the components on this popup, see the table beginning on page 52.

Viewing Event Search Results in Count View

This section describes how to view a search results list in *Count* view. This view groups multiple reads of one license plate under one record, thus reducing the number of records you have to scroll through.

1 Search for and display the events you wish to view. (If necessary, review "Searching for Events" on page 15.)

2 Click the **Count View** tab. The license plates display in Count View.

3 If your search yielded more than one page of results (i.e., Page 1 of 6), use the navigation buttons at the top of the page to scroll through the entire plate list.

⟨ ⟨⟨ ⟨   ⟩ ⟩⟩ ⟩⟩

The components of the Events page in Count View are described below.

Count View	
Column	**Description**
Plate	The license plate number. If you need to correct this number due to a read error, see "Correcting a License Plate Read Error" on page 65, beginning with step 2.
Frequency	The total number of reads for this license plate that match the search criteria.
Available Actions	
If an action is "grayed out" (i.e., unavailable), it indicates that you must select one or more license plate records first before you can perform that action.	
Action	**Description**
New Search	Return to the Search Events page in order to perform a new search. For instructions, see "Searching for Events on Your Local Server" on page 16 or "Searching for Events on Remote Servers" on page 25, beginning with step 2.
Show Detail	Display all the event records associated with a particular license plate. (Select one record only.)
Export to CSV	Export selected plates to a CSV spreadsheet file. For instructions, see "Exporting Search Results to a CSV File" on page 74, beginning with step 2.
Export to Pdf	Export selected events to a PDF file. For instructions, see "Exporting Event Search Results to a Pdf File" on page 76, beginning with step 2.
Create Hotlist	Create a new personal Hotlist from selected plates. For instructions, see "Creating a Personal Hotlist from Existing Events" in chapter 3, beginning with step 2.
Add to Hotlist	Add selected plates to an existing Hotlist. For instructions, see "Adding Events to an Existing Hotlist" in chapter 3, beginning with step 2.
Clear Selected	Deselect all plate records that are currently selected.
Apply Filter	Display only those plate records that are currently selected (i.e., highlighted).
Clear Filter	Undo the "Apply Filter" action (i.e., redisplay all license plates that met the original search criteria).

4 To view all the event records for a particular license plate, click on that plate's record, then go to the Action column and click **Show Detail**. The Tag popup displays.

Info	Plate	Details	Overview	Unit	Event Date ▼
ℹ	395TXJ	395 TXJ		L3-02	10/22/2010 17:55:49 GMT
ℹ	395TXJ	395 TXJ		L3-02	10/22/2010 17:55:46 GMT

Tag: 395TXJ — Total Selected: 1 — Page 1 of 1 (2 total records)

5 To view additional information on one of the events, hover your mouse over the *Info* icon. Otherwise click ☒ to close the popup.

Viewing Event Search Results in Map View

This section describes how to view a search results list on a map. This view allows you to perform a "search within a search" by selecting an additional geographic area to search within.

1 Search for and display the events you wish to view. (If necessary, review "Searching for Events" on page 15.)

This document consists of general capabilities information that is not defined as controlled technical data under ITAR part 120.10 or EAR

2 Click the **Map View** tab. The events display in map view. Each event is represented by a blue "event marker" icon: K446ZI
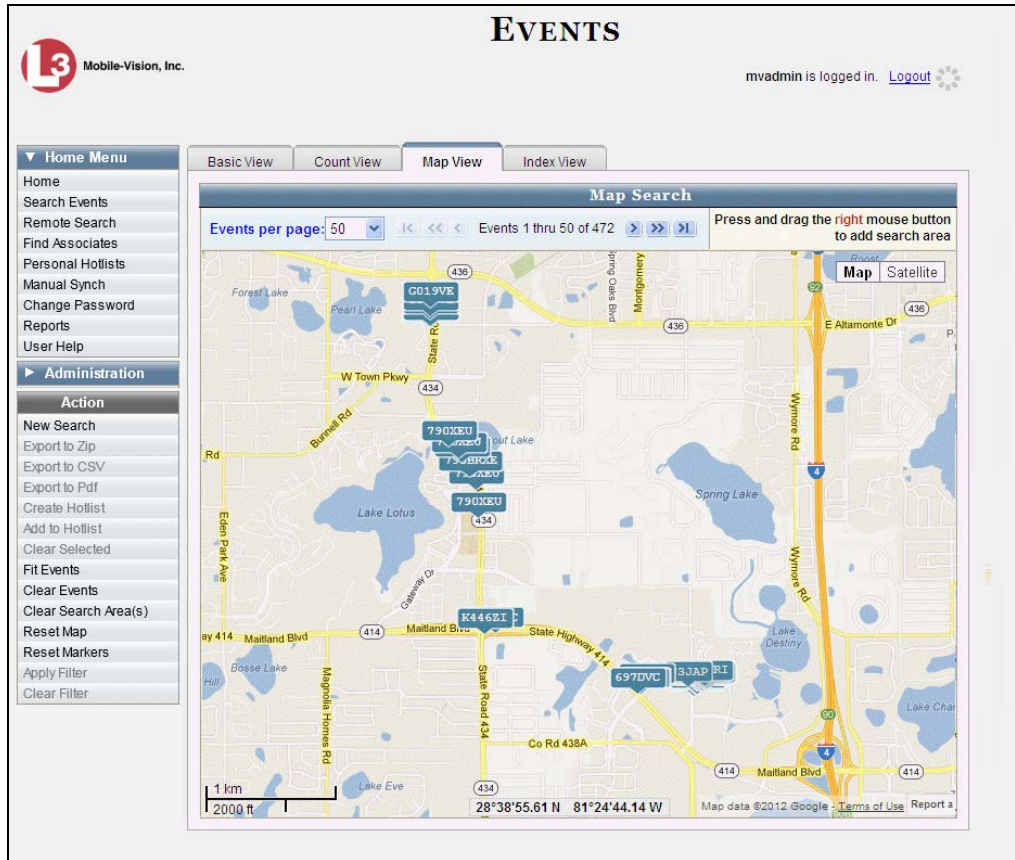
The available actions in Map View are described in the following table.

L3 Mobile-Vision, Inc.

Available Actions	
Action	**Description**
New Search	Return to the Search Events page in order to perform a new search. For instructions, see "Searching for Events on Your Local Server" on page 16 or "Searching for Events on Remote Servers" on page 25, beginning with step 2.
Fit Events	Zoom the map in or out to fit all matching results within the map view. To zoom *in*, double-click using the *left* mouse button. To zoom *out*, double-click using the *right* mouse button.
Clear Events	Remove all event markers from the map.
Clear Search Area(s)	Remove all search boxes from the map (i.e., any boxes that you drew by right-clicking and dragging the mouse).
Reset Map	Reset the map to its original position before you scrolled it up, down, left, or right.
Reset Markers	Reset all markers to their original position.

3 By default, the system displays 50 events per map. To change this number, select a new value from the *Events per page* drop-down list. Otherwise proceed to the next step.

4 If your search yielded more than one page of results (i.e., Page 1 of 6), use the navigation icons at the top of the page to scroll through the results list.

|< << <   > >> >|

5 To view details for an individual event, proceed to the next step. Otherwise skip to step 9.

K446ZI **6** Locate and click on the event marker you wish to view. If the event appears to be hidden by other markers, simply drag those markers to another part of the map. This will reveal those tags that are stacked behind it. Later you can restore the markers to their original positions by clicking on the **Reset Markers** link in the Action column.

Once you click on an event marker, the details popup will display.

(Continued)
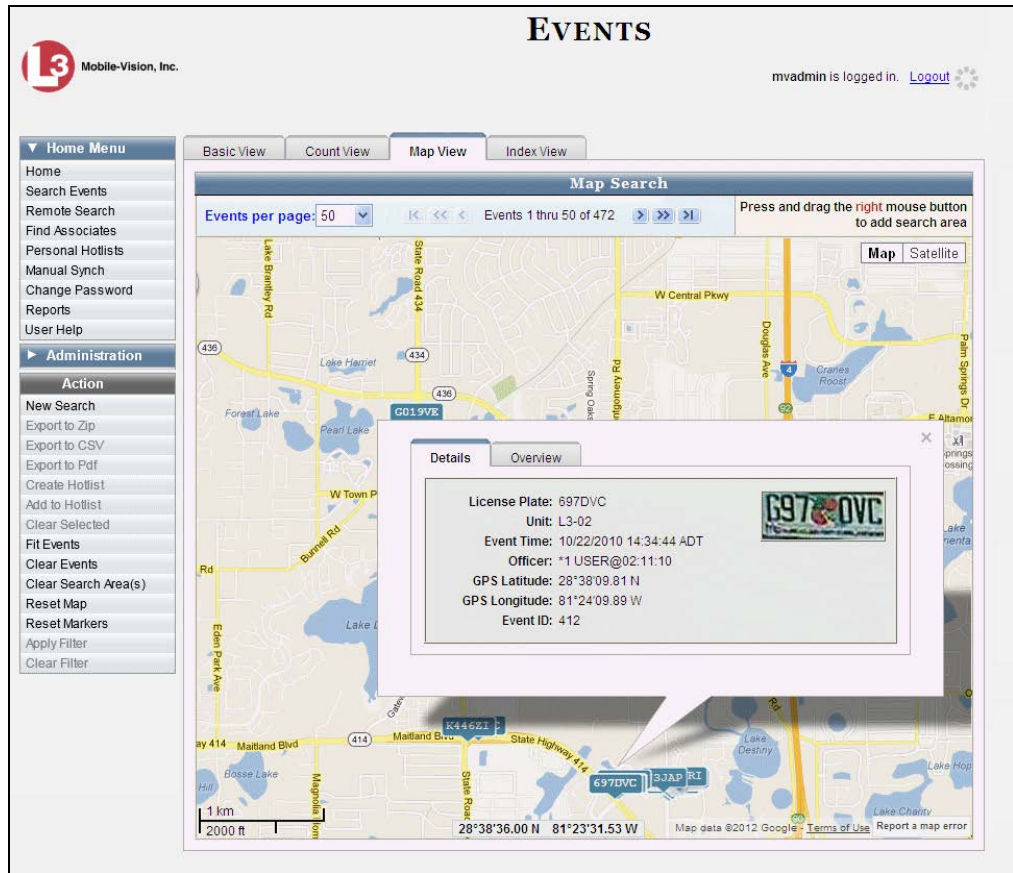
The event detail fields are described below.

Event Details	
Field	**Description**
License Plate	The license plate number. If you or another AlertVU user previously corrected a license plate read error, the updated value will display here.
Unit	The name of the AlertVU unit that captured this license plate.
Event Time	The date and time at which the AlertVU unit captured this license plate.
Officer*	The officer who was logged into the AlertVU unit at the time this license plate was captured.
GPS Latitude*	The latitudinal reading for the location at which AlertVU captured this license plate.

---

* Mobile units only

Event Details (cont'd)	
Field	**Description**
GPS Longitude[*]	The longitudinal reading for the location at which AlertVU captured this license plate.
Event ID	The numeric identification code that AlertVU assigned this plate read.

7 To view a digital image of the area from which AlertVU captured the license plate (i.e., *front* or *rear* of vehicle), click the **ANPR** or **Overview** tab. Otherwise proceed to the next step.

8 To view any metadata associated with this plate (if available), click the **MetaData** tab. Otherwise proceed to the next step.

9 When you're finished viewing the event details, click the ⊠ in the upper right corner of the popup to close it.

10 To reposition the map, proceed to the next step. Otherwise skip to step 12.

11 Left-click your mouse, then drag the map to the desired position.

12 To zoom in/out on the map, use the plus and minus arrows in the lower right corner of the page. Otherwise proceed to the next step.

13 To further narrow your search results by geographic location, proceed to the next step. Otherwise skip to step 16.

14 Press and drag the right mouse button over the area you wish to search in. A shaded box appears in that area. If desired, you may draw more than one box.

(Continued)
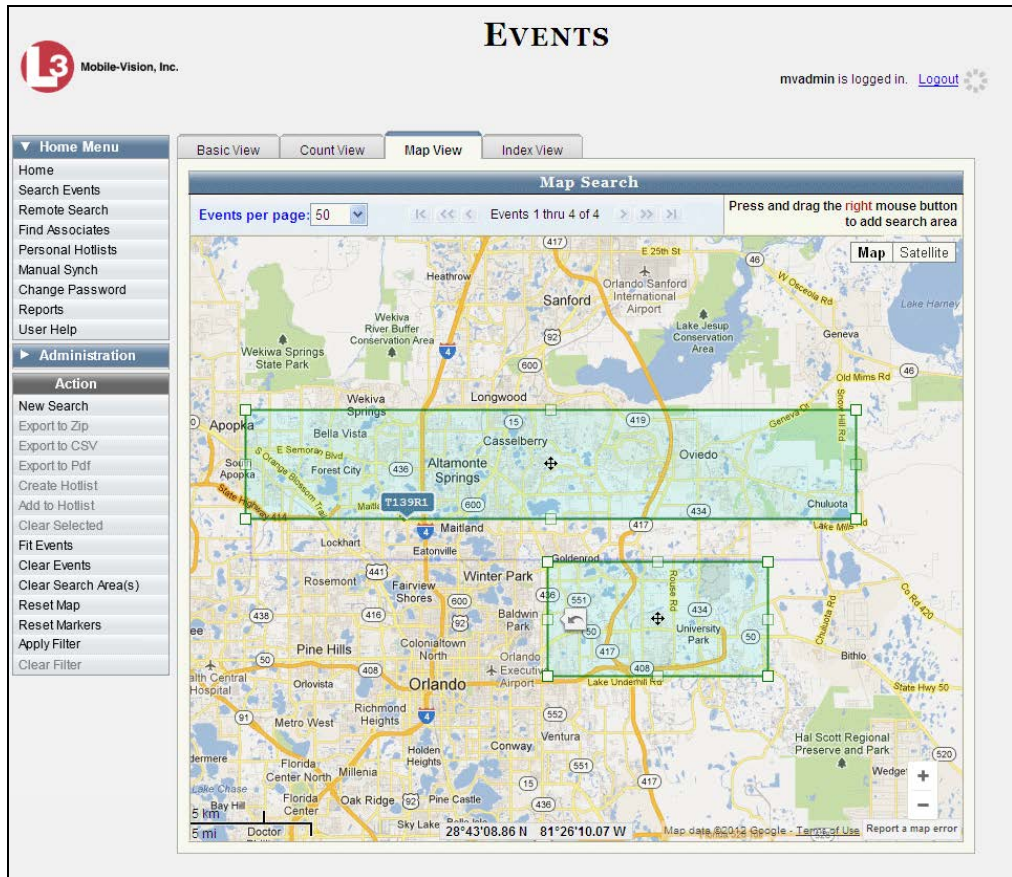
15 Go to the Action column and click **Apply Filter**. The system searches for and
selects any events that meet your original search criteria **and** were captured within
the highlighted area(s). If you look at the Events total, you will see the total events
that meet your new search criteria.
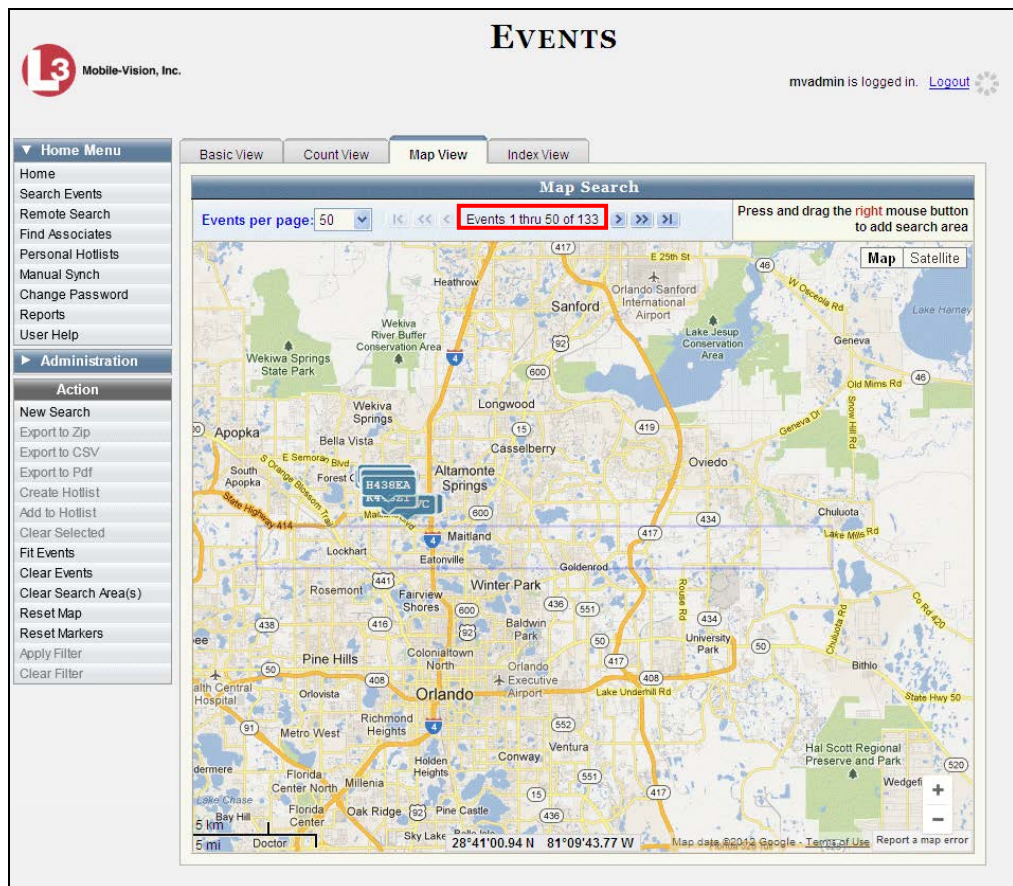
In the example above, the total number of events increased from **4** pages of 50 (200 events) to **133** pages of 50 (6,650 events) after the search area was enlarged.

16 To display this map in satellite view, click the **Satellite** button in the upper right corner of the page.

17 To return to map view, click the **Map** button.

Viewing Event Search Results in Index View

This section describes how to view a search results list in *Index* view. This view displays a digital image of the area from which AlertVU captured each license plate (i.e., *front* or *rear* of vehicle). The advantage of this view is that it allows you to select all of the records in your search results without having to click on each record.

1 Search for and display the events you wish to view. (If necessary, review "Searching for Events" on page 15.)

(Continued)

2 Click the **Index View** tab. The events display in index view.

3 If your search yielded more than one page of results (i.e., Page 1 of 6), use the navigation buttons at the top of the page to scroll through the entire events list.

|◁ ◁◁ ◁   ▷ ▷▷ ▷|

4 If you wish to perform an action on some or all of these events (e.g., export events, add events to a hotlist, etc.) proceed to the next step.

– OR –

If you do *not* wish to perform an action on some or all of these events, **End of Procedure**.

5 Select the events you wish to work with:

To select *all* events, go to top of the page and click **Select All**. The system selects all events in your search results, including those that are not currently displayed.

– OR –

To select *some* events, click the checkbox in the upper left corner of the appropriate event(s). If necessary, use the navigation arrows at the top of the page to scroll through the complete list.

6 Go to the Action column and click on the appropriate action, as described below.
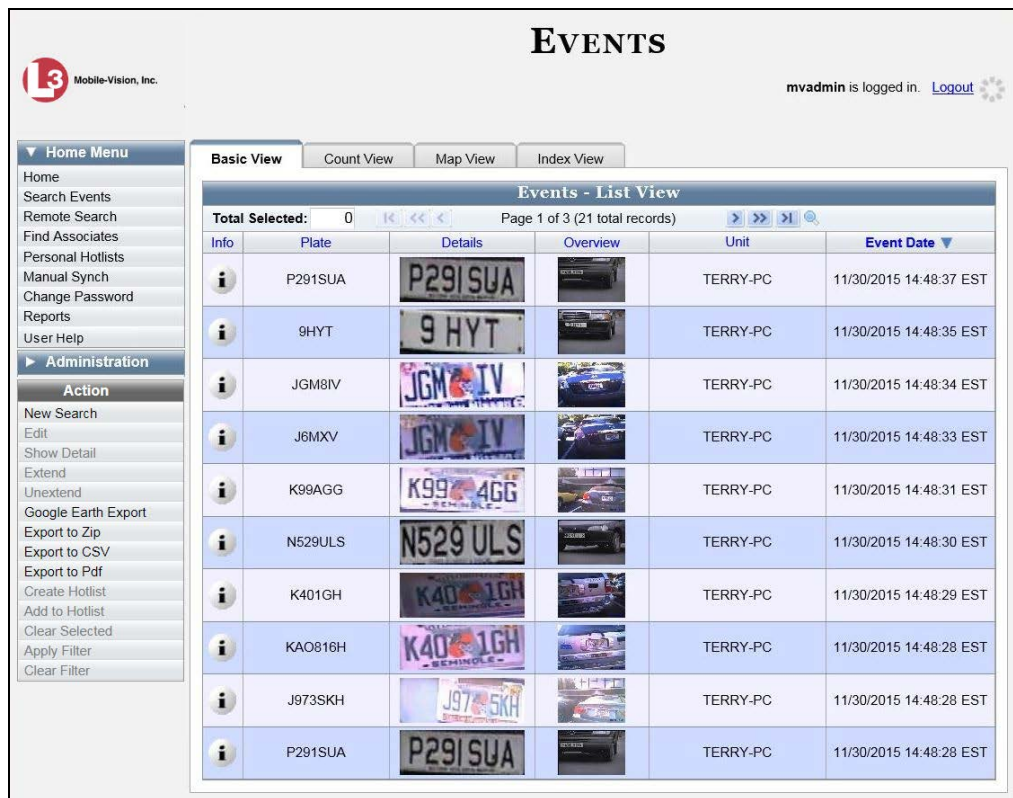
Available Actions	
Action	**Description**
New Search	Return to the Search Events page in order to perform a new search. For instructions, see "Searching for Events on Your Local Server" on page 16 or "Searching for Events on Remote Servers" on page 25, beginning with step 2.
Create Hotlist	Create a new personal Hotlist using selected events. For instructions, see "Creating a Personal Hotlist from Existing Events" in chapter 3, beginning with step 2.
Add to Hotlist	Add selected events to an existing Hotlist. For instructions, see "Adding Events to an Existing Hotlist" in chapter 3, beginning with step 2.
Apply Filter	Display only those event records that are currently selected (i.e., checked).
Clear Filter	Undo the geographical filter which you previously applied while in Map View. This will display only those events that met your original search criteria.

Viewing Event Search Results in Google Earth

This section describes how to use the Google Earth application to display an aerial view of search results. To accomplish this, the system downloads GPS data into a KML file format that can be read by Google Earth.

You can download and install Google Earth from the internet by going to: www.google.com/earth

1 Search for and display the events you wish to view. (If necessary, review "Searching for Events" on page 15.)

2 Make sure the **Basic View** tab is selected, as pictured above.

3 Go to the Action column and click **Google Earth Export**. The following popup displays.
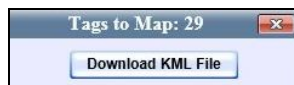
4 Click the **Download KML File** button. A Windows message displays.

5 Click **Open**. An aerial view of the events displays in Google Earth.
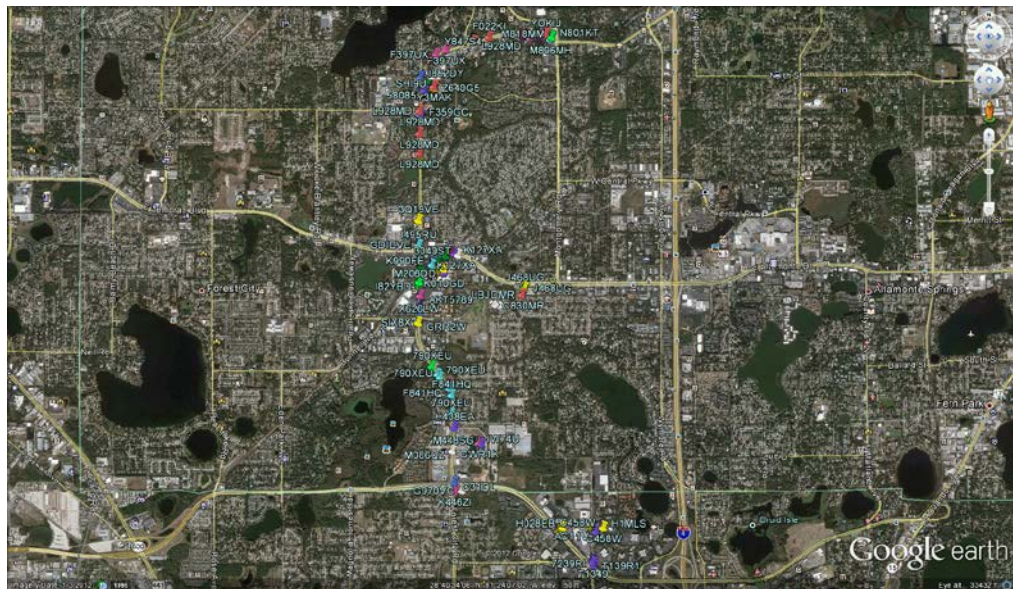
6 To reposition the map and/or zoom in or out, use the Google Earth controls located in the upper right portion of the screen. For information on Google Earth functions and features, refer to the Google Earth user manual and/or online help.

7 When you are ready to exit Google Earth, click the ⊠ in the upper right corner of the window, then click **Discard**.

Displaying Event Details

This section describes how to view the Details page for a selected event.

1 Search for the event you wish to view, as described in "Searching for Events" on page 15. The Events page displays, as pictured on the previous page.

2 Hover your mouse over the *Info* icon to the left of the event you wish to view.

– OR –

Click on the event record, then go to the Action column and click **Show Detail** (see **HINT** below).

HINT: If you clicked on an event record but the **Show Detail** option is grayed-out, it indicates that you have more than one record selected. Click **Clear Selected**, then reselect the single event you wish to view.

The Event Details popup displays.

(Continued)
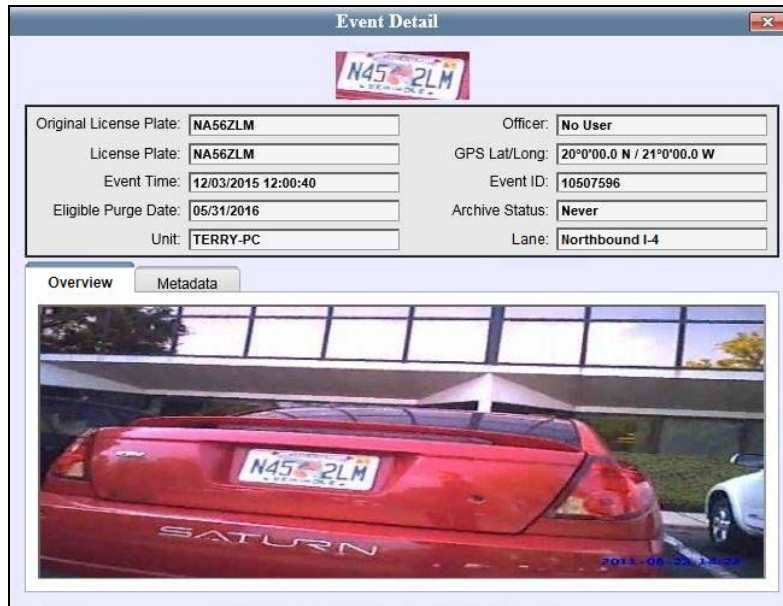
NOTE: If you imported this event from a spreadsheet, this popup will not include any digital images.

The information on the Event Detail popup is described below.

Event Details	
Field	**Description**
Original License Plate	The license plate number that was captured by AlertVU in the field. Depending on the capture device's ability to clearly read the license plate (influenced by such factors as lighting, camera angles, condition of plate, weather, etc.), this number may or may not be identical to the value in the *License Plate* field.
License Plate	The actual license plate number. By default, this value is equal to the value in the *Original License Pl*ate field. However, you have the ability to change/update this field as needed. For example, if you look at the license photo and observe that what the capture device interpreted as an **O** is actually a **C**, you can manually correct the license plate number. For more information, see "Correcting a License Plate Read Error" on page 65.
Event Time	The date and time at which the AlertVU capture device read the license plate. *Displays in mm/dd/yyyy hh:mm:ss format.*
Eligible Purge Date	The earliest date on which the system may purge this record from the AlertVU server.

Event Details (cont'd)	
Field	**Description**
Eligible Purge Date (cont'd)	This date is determined by the system backup/purge settings selected by your System Administrator.
Unit	The name of the AlertVU unit that captured this license plate. If this event was imported from a spreadsheet, the words **AlertVU Importer** will display here.
Officer (*Mobile Units only*)	The display name of the officer who was logged into the AlertVU unit at the time the license plate was captured.
GPS Lat/Long (*Mobile units only*)	The latitudinal and longitudinal coordinates of the vehicle at the time the license plate was captured.
Event ID	The event identification number that the system automatically assigned to this record.
Archive Status	The current backup status of this event: ▪ *Archived*. Event has already been burned to a backup disc ▪ *In-Progress*. Event is in the process of being burned to a backup disc ▪ *Restored*. Event was restored (i.e., copied) from a backup disc to the server. ▪ *Never*. The system has not assigned this record to a backup job yet, for one of two reasons: 1) either the event *just* transmitted to the server (in which case the system will soon assign the event to a backup job) or the system's backup feature is currently disabled (in which case the system will *never* assign the event to a backup job). ▪ *Unknown*. The current backup status of this event is unknown, as the record resides on a remote server.
Lane	The camera lane from which this event was captured.
Extend Reason	The reason provided by the user who extended this event's online life. This is typically the agency case number that the event is associated with. This field will display in place of the *Lane* field for extended event records.

3 To close the Event Details popup, either click the ❎ in the upper right corner of the popup (if applicable), or move your cursor off of the *Info* icon.

Viewing/Exporting an Event Report

AlertVU comes with several predefined reports. The *Summary* report lists the total number of events captured for all units within the last 24 hours, 7 days, and 30 days. The *Hotlist Hits* report shows the total number of hits for a selected unit, hotlist, and timeframe. And finally, the *Plate Reads* report lists the total number of events captured for a selected unit and timeframe.
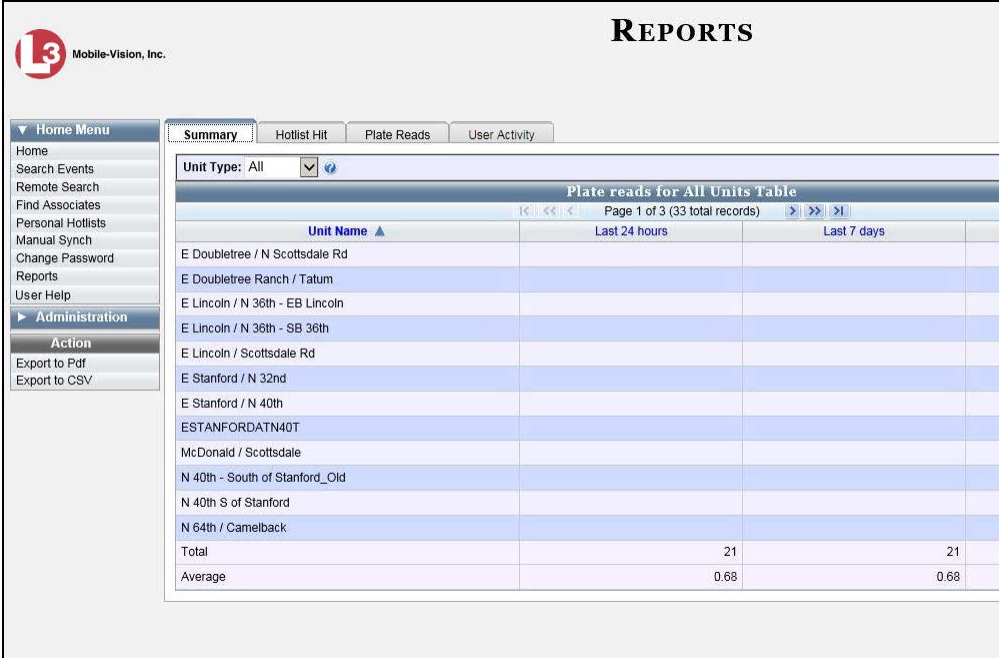
For more information, see:

❒ Viewing/Exporting the Summary Report, below
❒ Viewing/Exporting the Hotlist Hits Report, page 58
❒ Viewing/Exporting the Plate Reads Report, page 61.

Viewing/Exporting the Summary Report

The Summary report shows the total number of events that your AlertVU units have captured and transmitted to the server within the last 24 hours, 7 days, and 30 days.

1 Go to ▼ Home Menu and click **Reports**. The Reports page displays.

2   To generate a report for all types of AlertVU units (*stationary*, *in-car*, and *trailer-mounted*), proceed to the next step.

– OR –

To generate a report for *stationary*[*] AlertVU units only, select **Fixed** from the *Unit Type* drop-down list.

– OR –

To generate a report for *in-car* AlertVU units only, select **Mobile** from the *Unit Type* drop-down list.

– OR –

To generate a report for *trailer-mounted* AlertVU units only, select **Portable** from the *Unit Type* drop-down list.

3   If you wish to export this report, proceed to the next step.

– OR –

If you do *not* wish to export this report, **End of Procedure**.

4   To export this report to a *pdf* file, go to the Action column and click **Export to pdf**.

– OR –

To export this report to a *csv* spreadsheet file, go to the Action column and click **Export to CSV**.

A Windows message displays. The appearance of this message may vary slightly depending on the version of Windows that you have.

PDF
Download
Messages

Do you want to open or save **report-1448999380696.pdf** from **166.20.101.93**?   Open   Save ▼   Cancel   ×

report-150153386....pdf ∧

CSV
Download
Messages

Do you want to open or save **report-1448999409287.csv** (205 bytes) from **166.20.101.93**?   Open   Save ▼   Cancel   ×

report-150153411....csv ∧
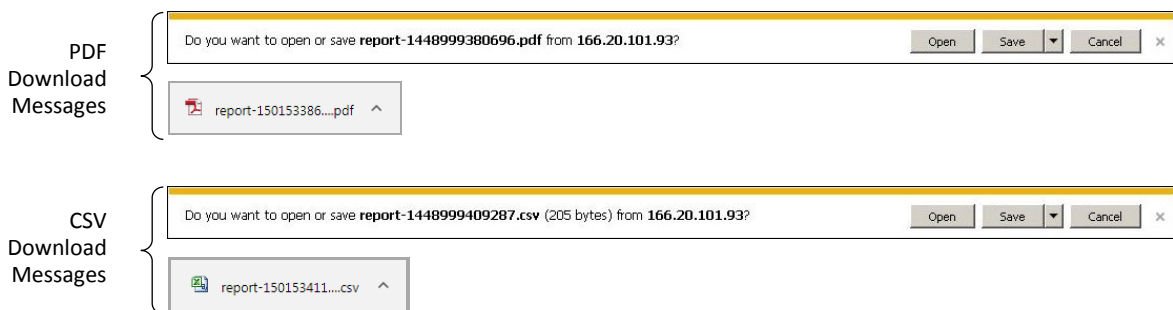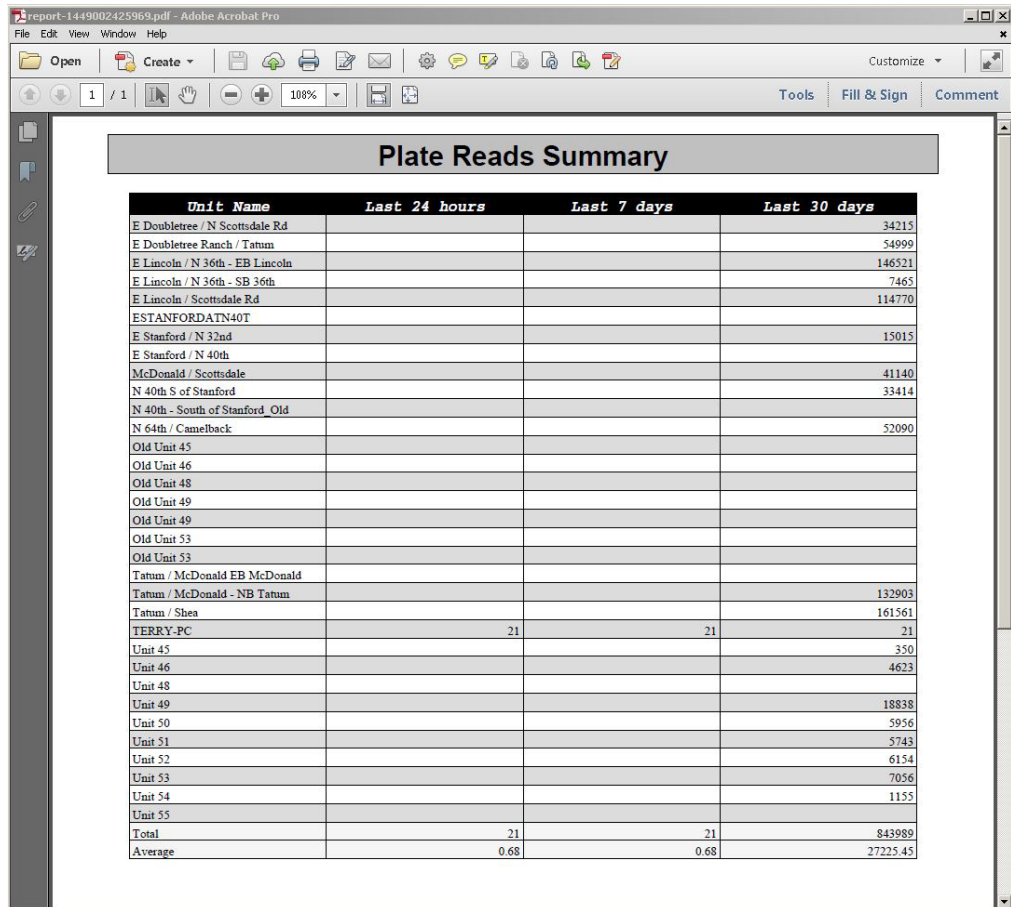
5   Click **Open**.

– OR –

Double-click on the Windows download tab.

(Continued)

---

[*]   Units that are permanently mounted to a pole or other apparatus

$\Rightarrow$ If you selected the **Export to pdf** option, the report displays in Adobe Reader.
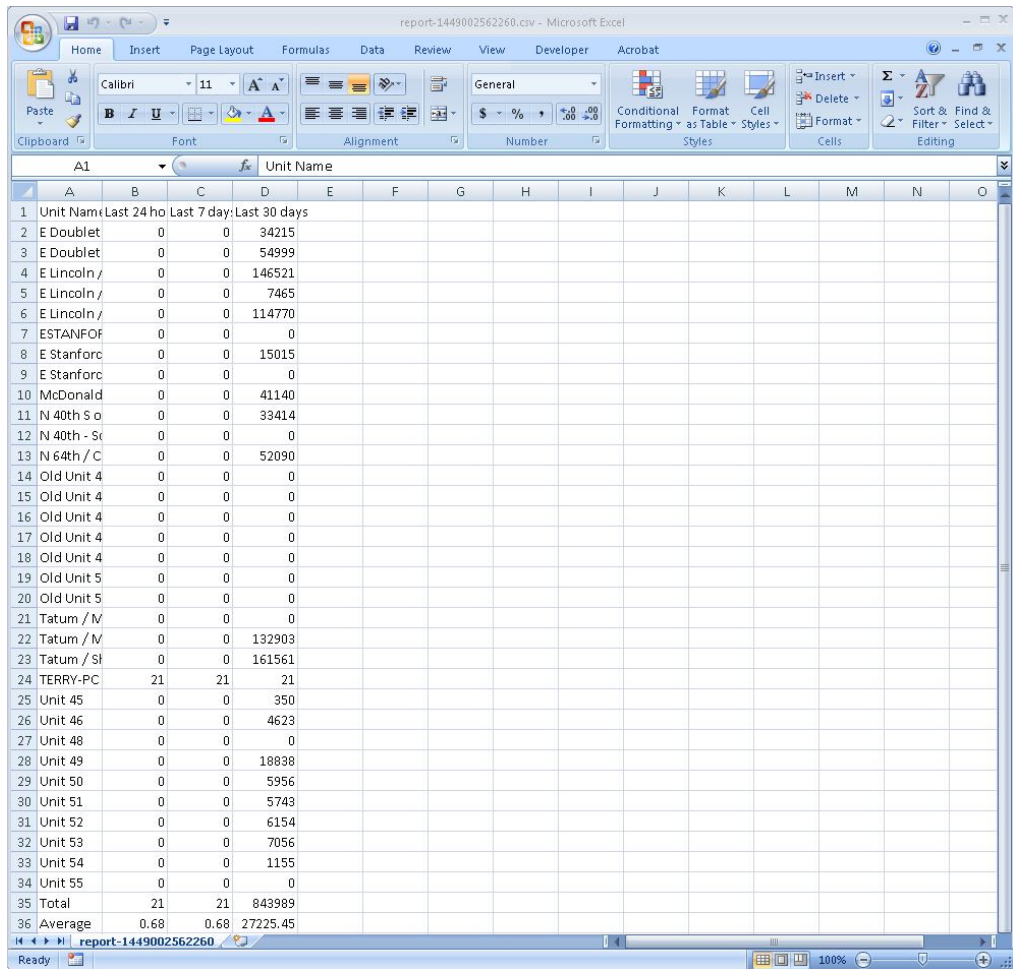
PDF file in Acrobat

Unit Name	Last 24 hours	Last 7 days	Last 30 days
E Doubletree / N Scottsdale Rd			34215
E Doubletree Ranch / Tatum			54999
E Lincoln / N 36th - EB Lincoln			146521
E Lincoln / N 36th - SB 36th			7465
E Lincoln / Scottsdale Rd			114770
ESTANFORDATN40T			
E Stanford / N 32nd			15015
E Stanford / N 40th			
McDonald / Scottsdale			41140
N 40th S of Stanford			33414
N 40th - South of Stanford_Old			
N 64th / Camelback			52090
Old Unit 45			
Old Unit 46			
Old Unit 48			
Old Unit 49			
Old Unit 49			
Old Unit 53			
Old Unit 53			
Tatum / McDonald EB McDonald			
Tatum / McDonald - NB Tatum			132903
Tatum / Shea			161561
TERRY-PC	21	21	21
Unit 45			350
Unit 46			4623
Unit 48			
Unit 49			18838
Unit 50			5956
Unit 51			5743
Unit 52			6154
Unit 53			7056
Unit 54			1155
Unit 55			
Total	21	21	843989
Average	0.68	0.68	27225.45

$\Rightarrow$ If you selected the **Export to CSV** option, the report displays in Microsoft Excel.

CSV file in Excel

6 When you're finished viewing/printing the report, click the ⊠ in the upper right corner of the report to exit Acrobat or Excel.

Viewing/Exporting the Hotlist Hits Report

A "hit" occurs when an AlertVU unit reads a plate that matches a plate number found on a system or personal hotlist. The Hotlist Hits report shows the total number of events captured by a selected unit (or all units) that hit on a selected hotlist (or hotlists) within a particular timeframe.

1   Go to ▼ Home Menu and click **Reports**. The Reports page displays.

2   Click the **Hotlist Hit** tab.

3   Go to the *Start Date* field and enter or select a start date for this report. Observe *mm/dd/yyyy* format. System defaults to today's date.

This document consists of general capabilities information that is not defined as controlled technical data under ITAR part 120.10 or EAR

4 Go to the *# Weeks* field and select the total number of weeks you wish to report on (1 – 12) from the start date. System defaults to **6**.

5 Go to the *View By* field and select the manner in which you wish to display report totals: by *hours in day*, *days in week*, *days in month*, or *months in year*.

6 To report on *all* hotlist hits (default), proceed to the next step.

– OR –

To report on only *one* hotlist, select that hotlist from the *Hotlist* drop-down list.

7 To report on *all* AlertVU units (default), proceed to the next step.

– OR –

To report on only *one* AlertVU unit, select that unit from the *Unit* drop-down list.

8 To export this report, proceed to the next step. Otherwise skip to step 12.

9 To export this report to a *pdf* file, go to the Action column and click **Export to pdf**.

– OR –

To export this report to a *csv* spreadsheet file, go to the Action column and click **Export to CSV**.

A Windows message displays. The appearance of this message may vary slightly depending on the version of Windows that you have.

PDF Download Messages

Do you want to open or save **report-1448999380696.pdf** from **166.20.101.93**?   Open   Save ▾   Cancel   ✕

🔴 report-150153386....pdf   ⌃

CSV Download Messages

Do you want to open or save **report-1448999409287.csv** (205 bytes) from **166.20.101.93**?   Open   Save ▾   Cancel   ✕

📊 report-150153411....csv   ⌃

10 Click **Open**.

– OR –

Double-click on the Windows download tab.

(Continued)

⇒ If you selected the **Export to pdf** option, the report displays in Adobe Reader.

PDF file in Acrobat

⇒ If you selected the **Export to CSV** option, the report displays in Microsoft Excel.

CSV file in Excel

11 When you're finished viewing/printing the report, click the ⊠ in the upper right corner of the report to exit Acrobat or Excel.

12 By default, the system displays this report in table format. To view the same data on a bar chart, click the **…Hotlist Bar** tab.
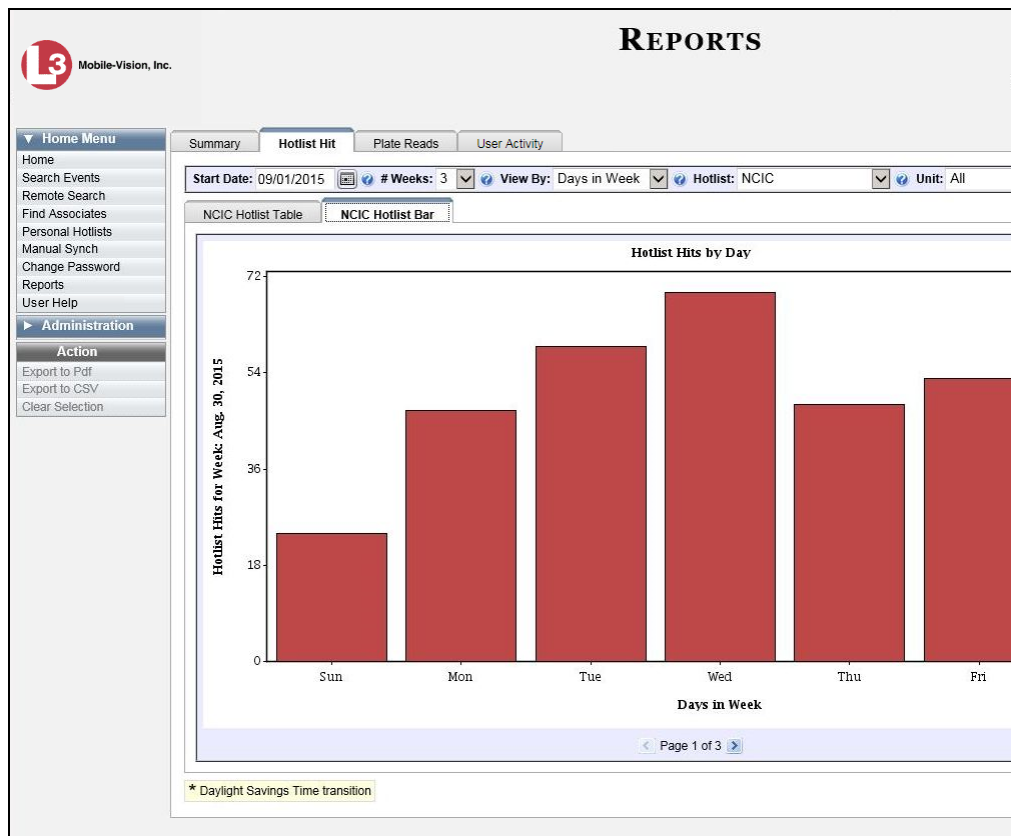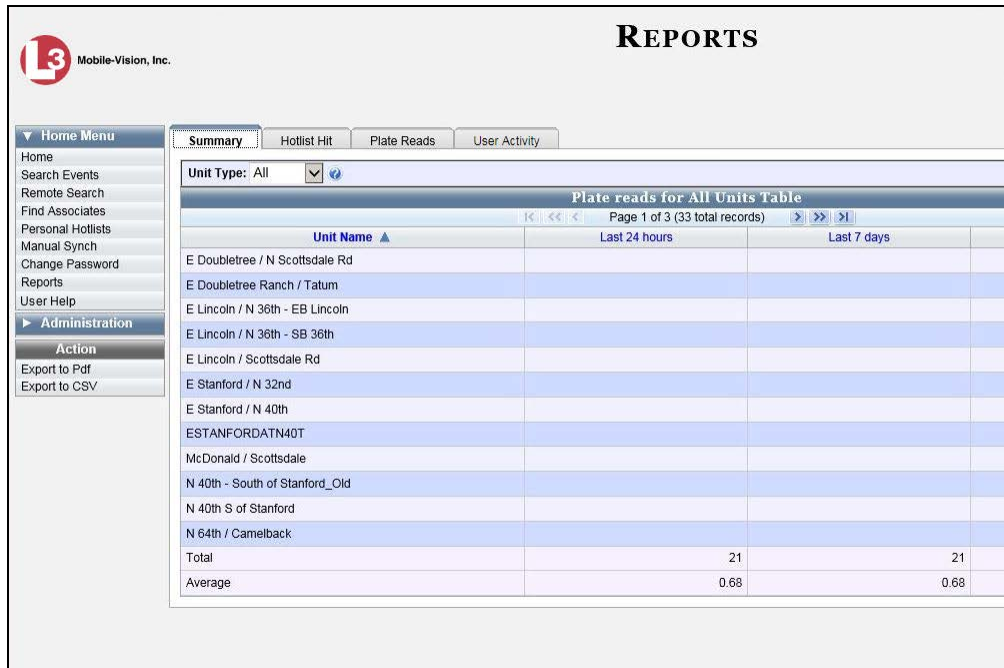
Viewing/Exporting the Plate Reads Report

The Plate Reads report shows the total number of events that a selected AlertVU unit (or all units) captured and transmitted to the server within a particular timeframe.

1 Go to ▼ Home Menu and click **Reports**. The Reports page displays.

(Continued)

2 Click the **Plate Reads** tab.

3 Go to the *Start Date* field and enter or select a start date for this report. Observe *mm/dd/yyyy* format. System defaults to today's date.

4 Go to the *# Weeks* field and select the total number of weeks you wish to report on (1 – 12) from the start date. System defaults to **6**.

L3 Mobile-Vision, Inc.

5   Go to the *View By* field and select the manner in which you wish to display report totals: by *hours in day*, *days in week*, *days in month*, or *months in year*.

6   To generate a report for all types of AlertVU units (*stationary*, *in-car*, and *trailer-mounted*), proceed to the next step.

   – OR –

To generate a report for *stationary*[*] AlertVU units only, select **Fixed** from the *Unit Type* drop-down list.

   – OR –

To generate a report for *in-car* AlertVU units only, select **Mobile** from the *Unit Type* drop-down list.

   – OR –

To generate a report for *trailer-mounted* AlertVU units only, select **Portable** from the *Unit Type* drop-down list.

7   To report on *all* AlertVU units (default), proceed to the next step.

   – OR –

To report on only *one* AlertVU unit, select that unit from the *Unit* drop-down list.

8   To export this report, proceed to the next step. Otherwise skip to step 12.

9   To export this report to a *pdf* file, go to the Action column and click **Export to pdf**.

   – OR –

To export this report to a *csv* spreadsheet file, go to the Action column and click **Export to CSV**.

A Windows message displays. The appearance of this message may vary slightly depending on the version of Windows that you have.
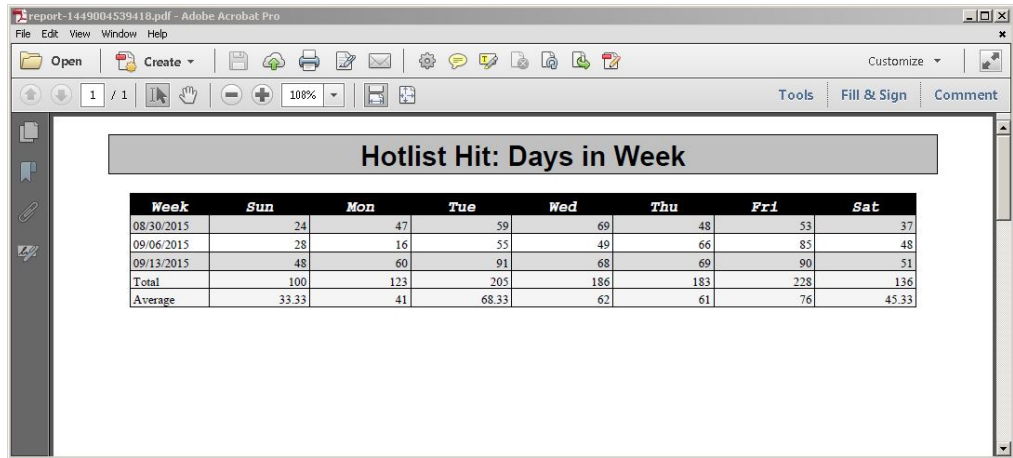
PDF
Download
Messages

> Do you want to open or save **report-1448999380696.pdf** from **166.20.101.93**?   Open | Save ▼ | Cancel | ×
>
> 📕 report-150153386....pdf   ^

CSV
Download
Messages

> Do you want to open or save **report-1448999409287.csv** (205 bytes) from **166.20.101.93**?   Open | Save ▼ | Cancel | ×
>
> 📊 report-150153411....csv   ^

---

[*]   Units that are permanently mounted to a pole or other apparatus

10 Click **Open**.

– OR –

Double-click on the Windows download tab.

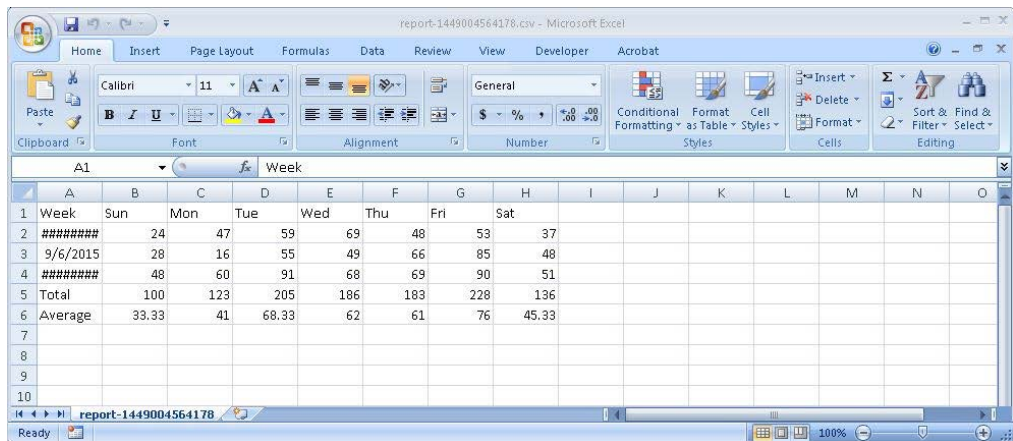⇒ If you selected the **Export to pdf** option, the report displays in Adobe Reader.

PDF file in Acrobat

⇒ If you selected the **Export to CSV** option, the report displays in Microsoft Excel.

CSV file in Excel

11 When you're finished viewing/printing the report, click the ⊠ in the upper right corner of the report to exit Acrobat or Excel.

This document consists of general capabilities information that is not defined as controlled technical data under ITAR part 120.10 or EAR

12 By default, the system displays this report in table format. To view the same data on a bar chart, click the **…Plate Reads Bar** tab.

Correcting a License Plate Read Error

This section describes how to correct a license plate number when the system misinterprets one or more characters on a plate. For example, the system might misinterpret a **6** as a **G**, a **Q** as an **O**, a **Z** as a **2** etc. Whenever possible, compare a plate's actual photo to the value in the *Plate* column to check for accuracy.

1 Search for the event record you wish to correct. (If necessary, review "Searching for Events" on page 15.)

(Continued)
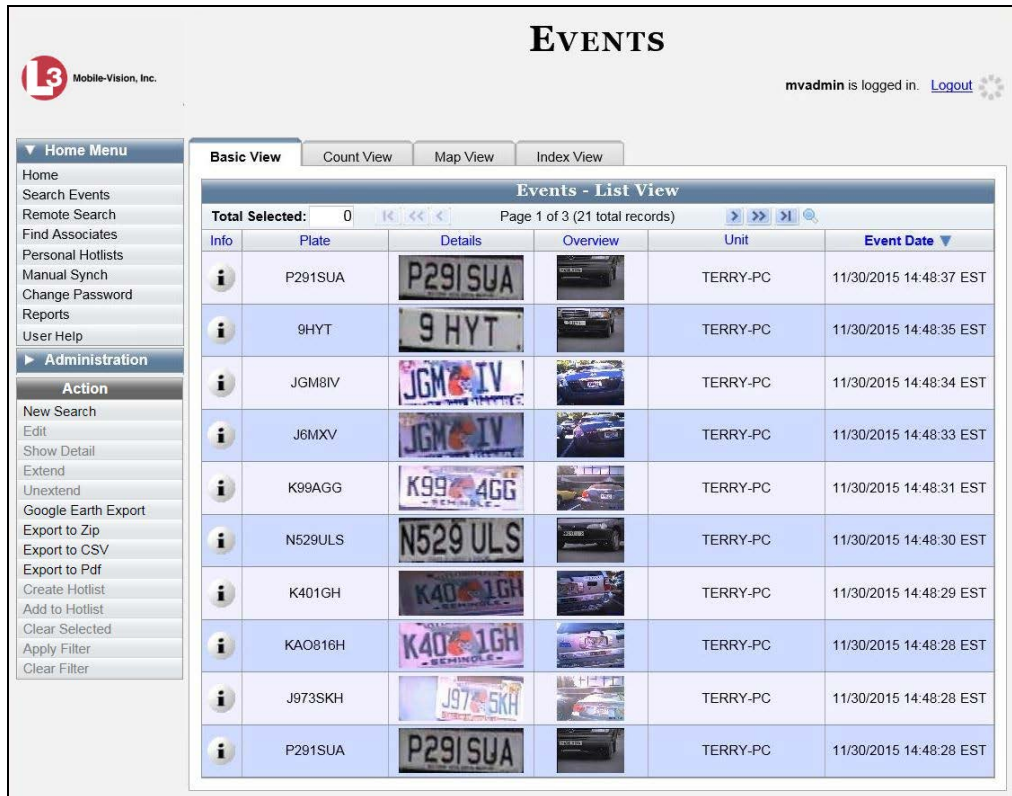
2 Click on the event row to highlight it.

3 Go to the Action column and click **Edit**.

– OR –

Right-click on the record and select **Edit Plate Name** from the popup menu.

The Edit Plate Name popup displays.
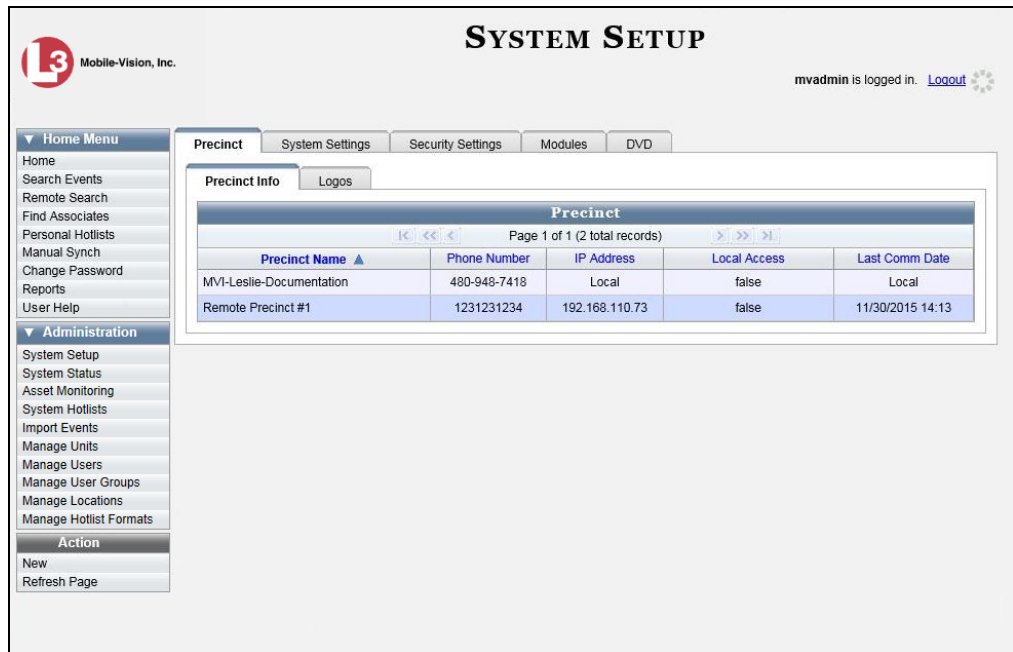
4 Enter the correct plate number in the *Plate* field.

5 Click **Save**. The corrected plate number displays in the *Plate* column.

L3 Mobile-Vision, Inc.

Changing Events' Days Online

This section describes how to change the settings that determine how long event files will remain on your local server.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 Click the **System Settings** tab.

3   Click the **System Options** tab.

4   Go to the Action column and click **Edit**. The System Options popup displays.

The first two fields on this popup will determine when the system will remove events from the server, as described in the following table.

L3 Mobile-Vision, Inc.

Field	Description
Minimum Days Online	The minimum number of days that an event will remain online before it can be purged from the server.
Enable Strict Purger	☑ If this checkbox is selected, the system will move events offline as soon as 1) the event ages out and 2) the event has been archived (assuming backups are enabled). ☐ If this checkbox is *not* selected, the system will move aged-out events offline only when space is needed on the server. Until then, they will remain online.

5   Go to the *Minimum Days Online* field and enter the minimum number of days that you want an event to remain online before it can be purged from the server.

6   If you want an event to be removed from the server as soon as it ages out, select the *Enable Strict Purger* checkbox.

– OR –

If you want an event to remain on the server as long as possible, deselect the *Enable Strict Purger* checkbox.

7   Click **Save**.

Exporting Events

AlertVU allows you to export events in one of two ways. You can export events contained in a search results list, or you can export *all* events for use with another application.

For more information, see:

❐ Exporting Search Results, below
❐ Exporting Incoming Events, page 78.

Exporting Search Results

This section describes how to export a search results list of 1,000 events or less to one of three file types:

❐ Zip file that contains that contains the event image (JPEG) files and associated metadata
❐ CSV spreadsheet file, which can be viewed in Microsoft Excel
❐ Pdf file, which can be viewed in Adobe Reader.
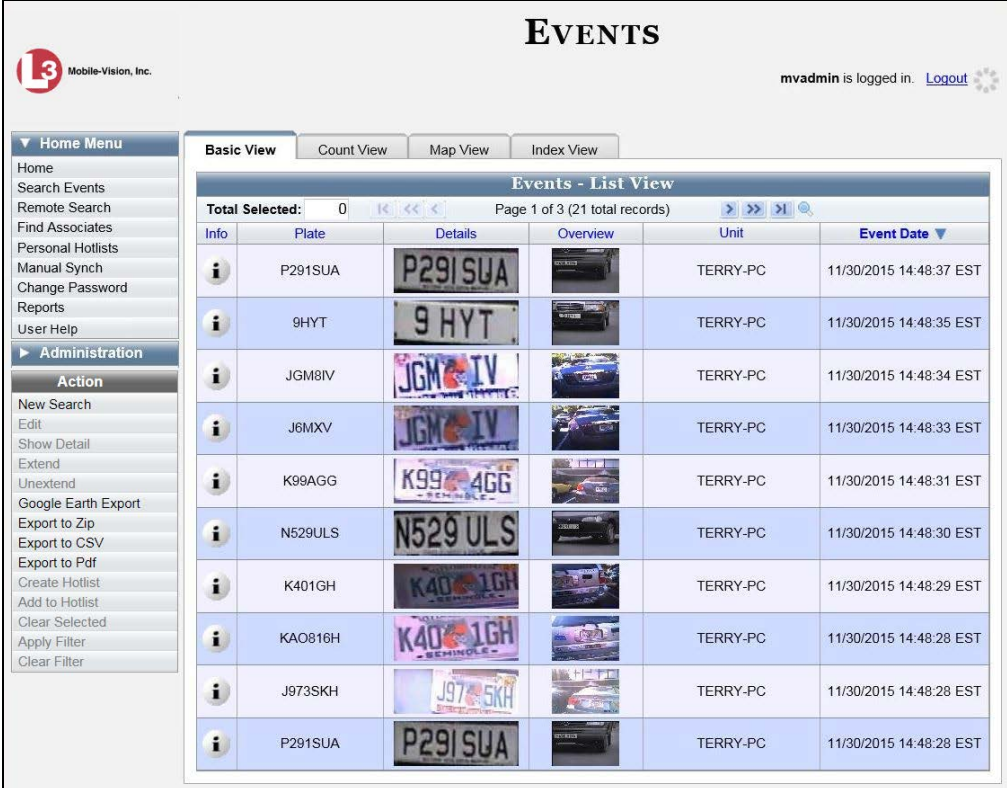
For specific instructions, see:

❒ Exporting Event Search Results to a Zip File, below
❒ Exporting Event Search Results to a CSV File, page 74
❒ Exporting Event Search Results to a Pdf File, page 76.

Exporting Event Search Results to a Zip File

This section describes how to export selected events to a zip file that contains the event image (JPEG) files and associated metadata. You can export up to 1,000 events at a time.

1 Search for the events you wish to export. (If necessary, review "Searching for Events" on page 15.)

2 Go to the Action column and click **Export to Zip**. The Export to Zip popup displays.
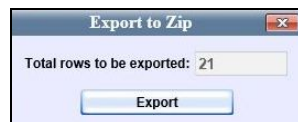
3 Click **Export**. The system begins exporting the selected events. After a momentary delay, the following message displays at the top of the page.

> The search results are being queued for export. Check your *Inbox* on the *Home* page for the status of your export. When the export is complete, a message will be sent to your *Inbox* with a clickable link allowing you to download the exported results.

4 Go to ▼ Home Menu and click **Home**.

5 Locate the export message on your *Inbox Messages* list.

Initially, the status of your export request will be "Queued". Once the system has finished processing your request (see **HINT** below), the value in the *State* column will change to "Completed."

HINT: To refresh your screen and update the value in the *State* column, go to ▼ Home Menu and click **Home**.

6 Once the status of your export request is *Completed*, click the ⦿ icon to the right of that request. A Windows prompt displays.

Do you want to open or save **export_1425417344251.csv** from **trinity**? | Open | Save ▼ | Cancel | ✕

7 Select **Save As** from the *Save* drop-down list. The Save As popup displays.
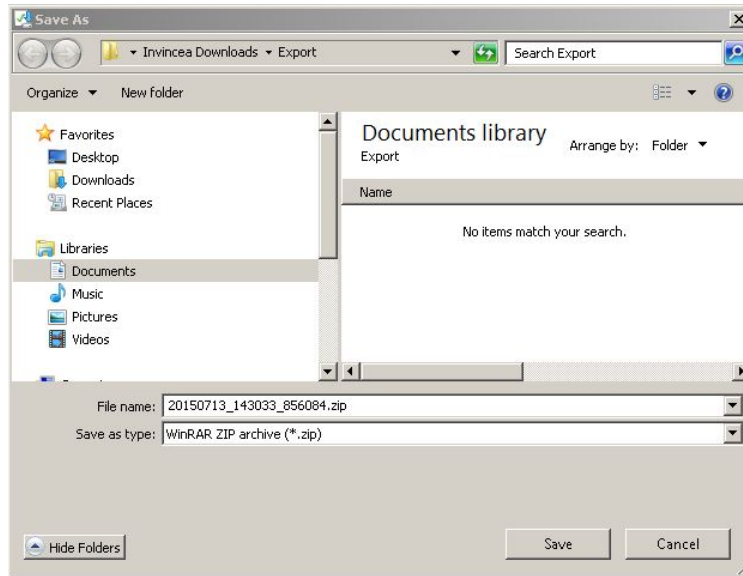
8 Navigate to the directory where you wish to save the export file, then click **Save**. A download confirmation message displays.

The 20150713_143033_856084.zip download has completed. | Open ▼ | Open folder | View downloads | ✕

9 Click **Open folder**. The events' .zip file displays in the selected directory.
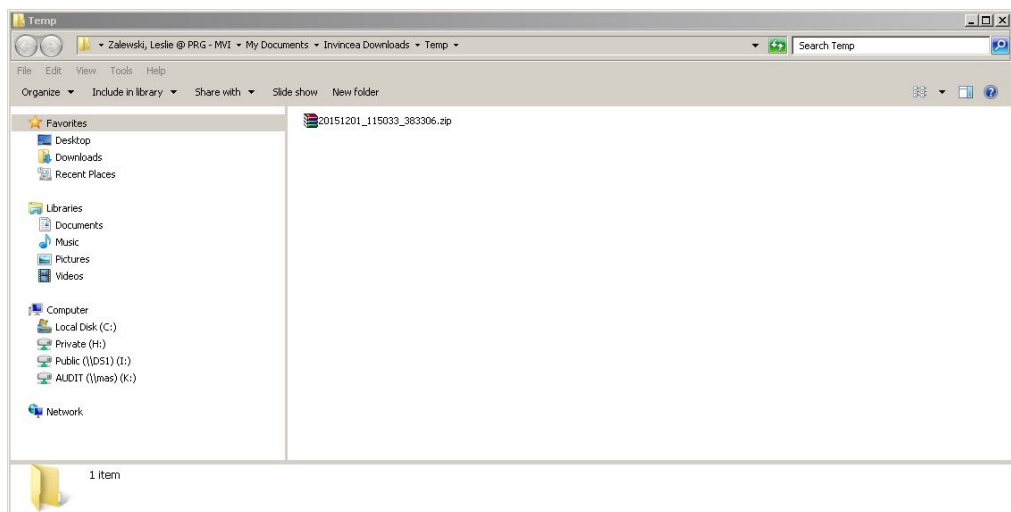
10 Right-click on the .zip file, then select **Extract Here** from the popup menu. The contents of the Export folder display.
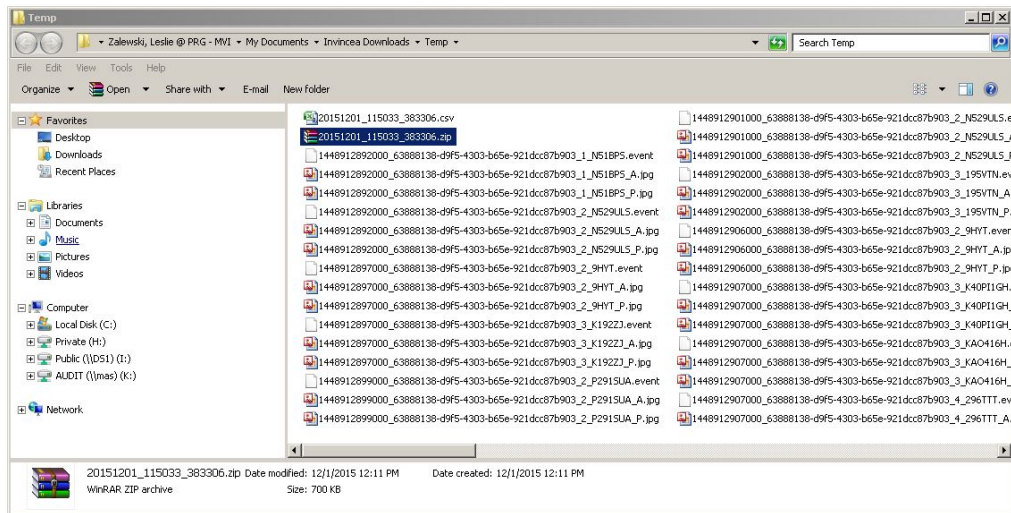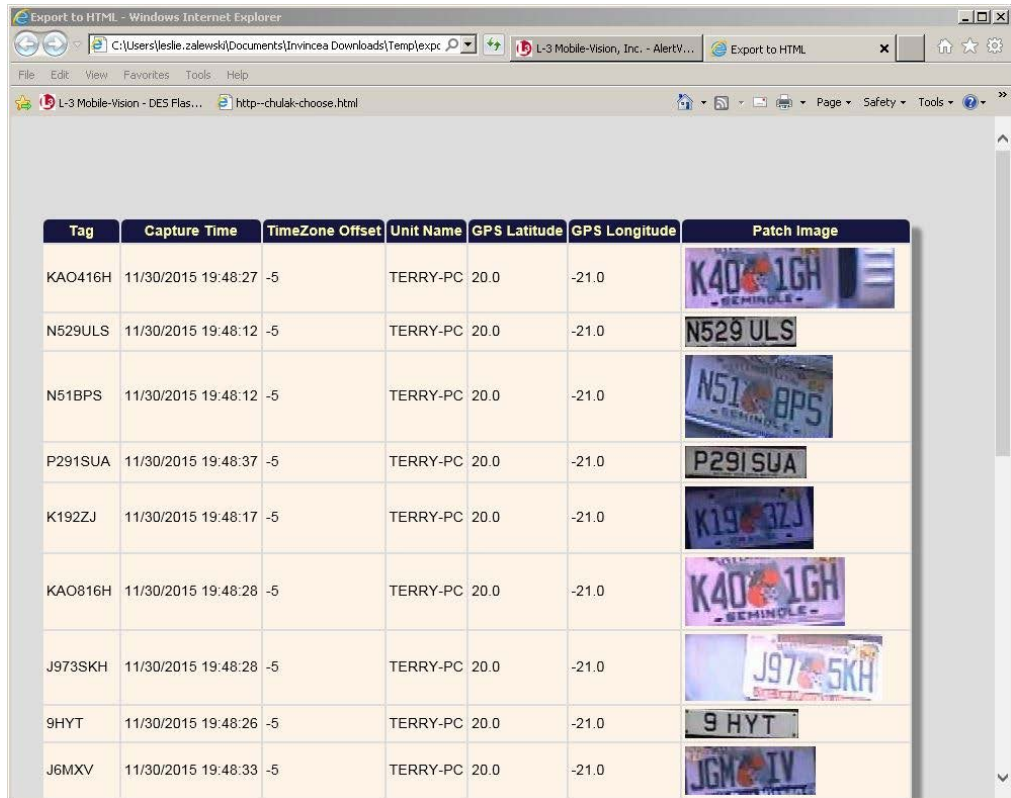
11 Double-click on the HTML Document, typically located at the bottom of the list.
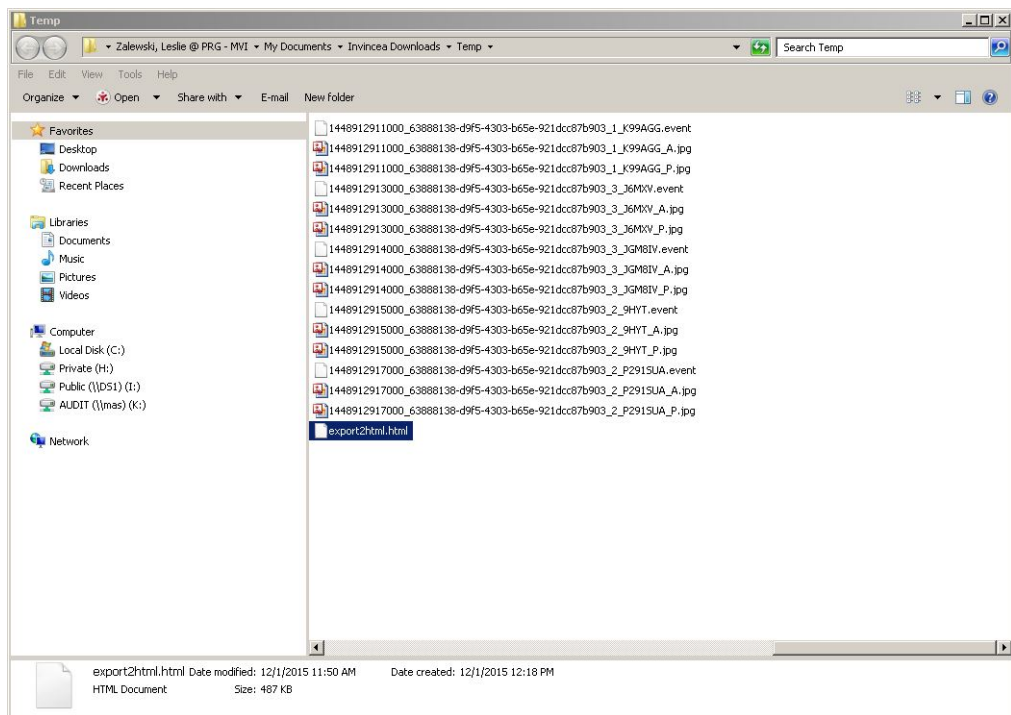
12 If you are prompted with a security message, click the **Allow Blocked Content** button. Otherwise proceed to the next step.

(Continued)

The export data displays.
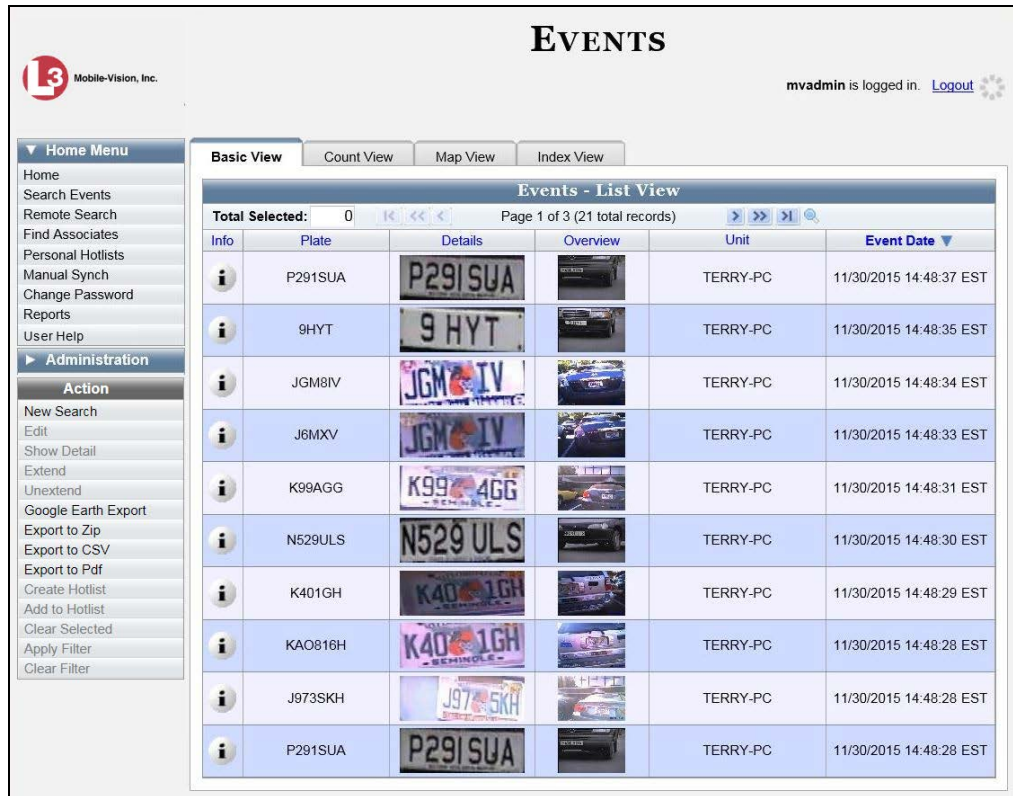
13 When you're finished viewing the export data, click the ⊠ in the upper right corner of the browser to exit.

Exporting Event Search Results to a CSV File

This section describes how to export selected events to a CSV file, which can be viewed in Microsoft Excel. You can export up to 1,000 events at a time.

1 Search for the events you wish to export. (If necessary, review "Searching for Events" on page 15.)

2 Go to the Action column and click **Export to CSV**. The Export to CSV popup displays.
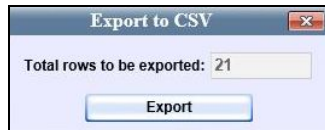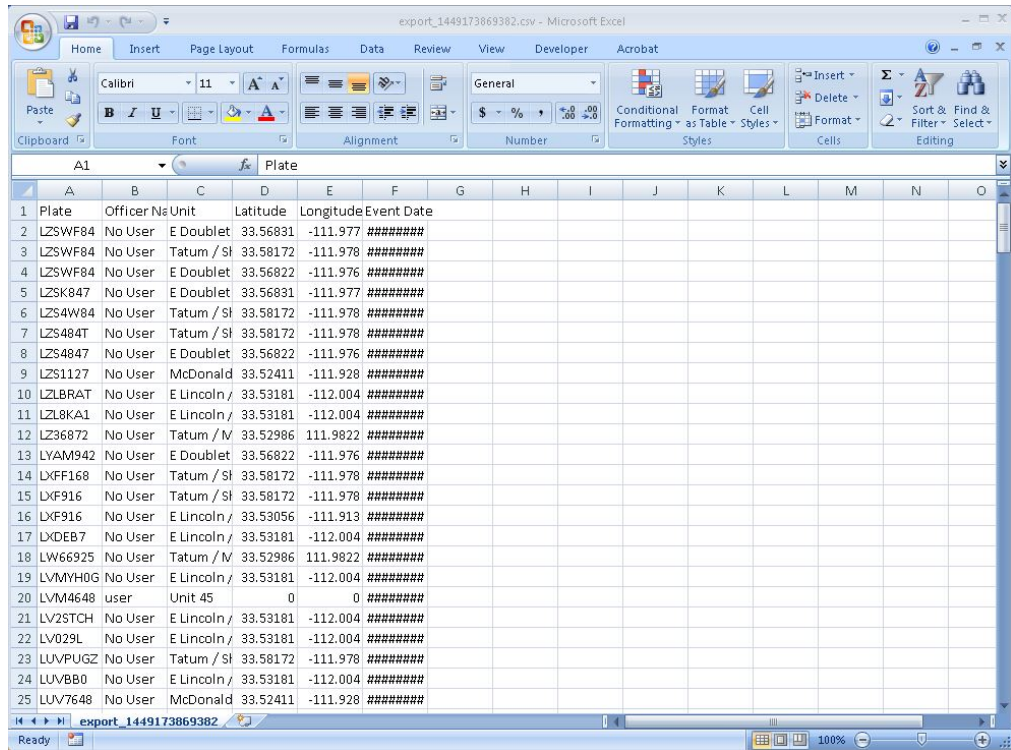
3 Click **Export**. A Windows prompt displays.

4 Click **Open**. The Event data displays in Microsoft Excel.

(Continued)

5 When you're finished viewing the report, click the ⊠ in the upper right corner of the window to exit Excel.

Exporting Event Search Results to a Pdf File

This section describes how to export selected events to a PDF file, which can be viewed in Adobe Acrobat or other PDF viewer software. You can export up to 1,000 events at a time.

1 Search for the events you wish to export. (If necessary, review "Searching for Events" on page 15.) The Events page displays.

2 Go to the `Action` column and click **Export to Pdf**. The Export to Pdf popup displays.
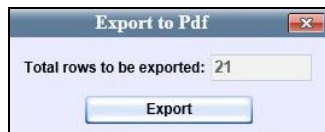
3 Click **Export**. A Windows prompt displays.

4 Click **Open**. The Event data displays in Adobe Acrobat.

(Continued)
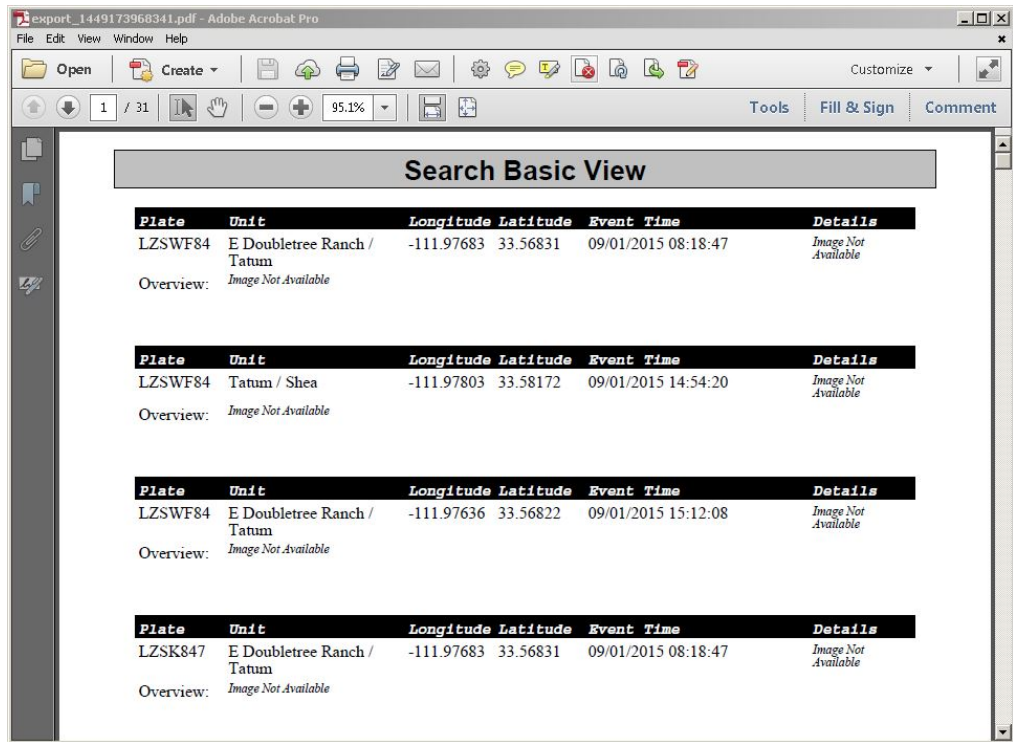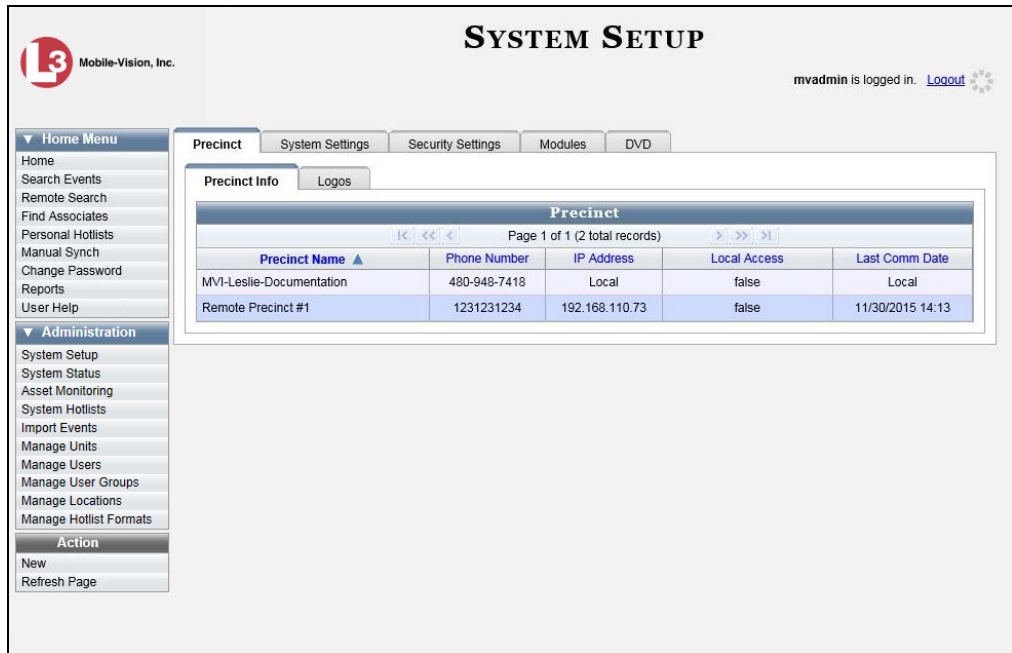
5 When you're finished viewing the report, click the ⊠ in the upper right corner of the window to exit Acrobat.

Exporting Incoming Events

This section describes how to activate the "event exporter" feature, which enables you to automatically copy your incoming event data into zip files on the /fbdata/00/ alpr/export-data directory, or other directory of your choice. This makes it possible for you to import your event data into other applications, such as other LPR systems.

1 Go to **▼ Administration** and click **System Setup**. The System Setup page displays.

2 Click the **System Settings** tab.

3 Click the **Event Exporter** tab.

(Continued)

4 Go to the Action column and click **Edit**. The Edit Event Exporter Settings popup displays.

The fields on this form are described in the following table.

L3 Mobile-Vision, Inc.

Edit Event Exporter Settings	
Field	**Description**
Home Directory	The directory in which the Exporter Service will place export packages. An export package is a zip file that contains the following data: ▪ Multiple image files (i.e., plate reads) ▪ A .csv file that contains the following data fields: *Tag*, *Capture Time*, *TimeZone Offset*, *Unit Name*, *GPS Latitude*, *GPS Longitude*, *Image File Basename*.
Delete Packages After (in minutes)	The time period, in minutes, from when the Exporter Service places a new package in the Home Directory to when the system is allowed to delete that package. For example, if this field is set to the default of **120**, then 120 minutes (2 hours) after the Exporter Service places a new package in the Home Directory, the system will delete that package. Maximum minutes allowed are 20,160 (2 weeks).
Create Packages Starting From (in minutes)	The time period, in minutes, for which the Exporter Service will group events in an event package. For example, if this field is set to the default of **10**, then events found in the system from the current time to 10 minutes prior will be placed in an event package. Maximum minutes allowed are 1,440 (24 hours).
Enabled Exporter Service	A checkbox used to indicate whether or not the Exporter Service is enabled (i.e., in use). ☑ The Exporter Service is enabled ☐ The Exporter Service is disabled

⚠️ **WARNING:** Do not change the first three fields on this form unless instructed to do so by an L3 Mobile-Vision Technical Support Engineer (TSE) or other Support professional.

5 Make sure the *Enabled Exporter Service* checkbox is selected.

6 Click **Save**.

Importing Events

This section describes how to import events into the system. There are three types of imports:

❑ Archived AlertVU data. These are events that the system previously backed up to a system archive disc, also referred to as a *Certified Backup Disc*.

❑ Exported AlertVU data. These are events that you or another user previously exported to a .csv file using the system export function. For more information on this function, see "Exporting Search Results" on page 69.

❑ Exported ELSAG data. These are events that were previously exported from the ELSAG license plate reader.

1 Go to ▼ Administration and click **Import Events**. The Import Events page displays.

If you previously imported one or more files, they will display on this page, as described in the following table.

L3 Mobile-Vision, Inc.

Imports	
Column	**Description**
Description	A description of the imported events list. This description is provided by the user who imported the list (see *User* field).
Import Type	The type of import: ▪ AlertVU Archive. Events that the system previously backed up to a system archive disc. ▪ AlertVU Import. Events that you or another user previously exported to a .csv file using the system export function. ▪ ELSAG Import. Events that were previously exported from the ELSAG license plate reader.
Imported	The date and time at which this list was imported.
User	The User ID of the individual who imported this list.
Status	The status of this event list's import: ▪ Uploaded. The system has finished uploading the events file. ▪ Processing. The system is in the process of importing the events file into the events database. ▪ Completed. The system has successfully imported the events file into the events database. ▪ Deleting. The system is in the process of removing all the events that were on this list from the events database. ▪ *Error*. A problem occurred that interfered with the successful importing of this events list. Contact L3 Mobile-Vision Support for assistance.

2 Go to the Action column and click **Import**. The Import Events popup displays.

3 Click **Browse**. The Choose File to Upload popup displays.

4 Search for and select the events file you wish to upload. This file must have an extension of **.csv**.

5 Click **Open**. The selected file name displays in the *Import File* field.

(Continued)
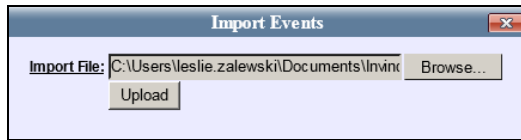
6 Click **Upload**. The Import Details popup displays.
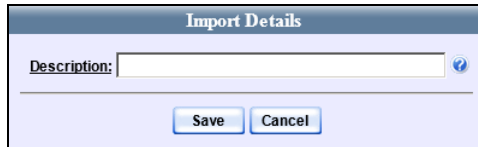
7 Enter a description of this event list in the field provided.

8 Click **Save**. The new list displays on the Imports list.

Note that the list's *Status* is now **Uploaded**. That means that the system has uploaded the events file to AlertVU, but hasn't yet updated the database. When the update is complete, the word **Completed** will display in the *Status* column.

Deleting Imported Events

This section describes how to delete a list of events that was previously imported into the system using the *Import Events* function.

1 Go to ▼ Administration and click **Import Events**. The Import Events page displays.

2 Click on the import record you wish to delete.

3 Go to the Action column and click **Delete**. Note that the import's status is now *Deleting*.

4 To check on the progress of the deletion, go to the Action column and click **Refresh Page**. Once the import record disappears from the *Imports* list, it indicates that the system has finished deleting all events associated with that import record.

Extending the Life of an Event

This section describes how to prevent an event from being purged from the server on its scheduled purge date. When a case becomes very active, for example, you may want to extend the online life of any events that are associated with that case.

An event's purge date is determined by several system settings, including:

❑ *Minimum Days Online* (*see* System Setup→ System Settings→ System Options)
❑ *Enable Strict Purger* (*see* System Setup→ System Settings→ System Options)
❑ *Backup Mode* (*see* System Setup→ Backup→ Backup Options)
❑ *Maximum Days Between Archives* (*see* System Setup→ Backup→ Backup Options)

Once you extend an event's online life, it will remain online until you *unextend* that event, as described in the next section, "Canceling an Event Extension."
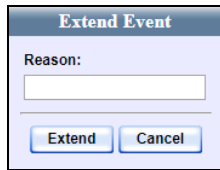
1   Search for and select the event you wish to extend. (If necessary, review "Searching for Events" on page 15.)

2   Go to the Action column and click **Extend**. The Extend Event popup displays.

Extend Event

Reason:

[   ]

[Extend]   [Cancel]

3   Enter a case number in the *Reason* field (i.e., the agency case that is associated with this event).

4   Click **Extend**. Once an event is extended, the Extend Reason will display in the lower right corner of the event's record.

Event Detail

Original License Plate:	CMQJ21	Officer:	*1 USER@01:03:39
License Plate:	CMQJ21	GPS Lat/Long:	0º0'00.0 S / 0º0'00.0 W
Event Time:	03/26/2014 14:46:22	Event ID:	3202
Eligible Purge Date:	03/26/2015	Archive Status:	In-Progress
Unit:	Ford Exp	Extend Reason:	2017-00089

Overview

Canceling an Event Extension

This section describes how to release an extended event record. An *extended* event is one which has a "hold" on it, preventing it from being purged from the server. (For more on this topic, see the previous section, "Extending the Life of an Event.") Perform this procedure when the case associated with an extended event is no longer active, indicating that it is safe to remove that event from the server.

1 Search for and select the extended event. (If necessary, review "Searching for Events" on page 15.)

2 Go to the Action column and click **Unextend**.

3 Hotlists

This chapter describes how to create and maintain hotlists. A hotlist is list of wanted license plates, such as BOLOs, Amber Alerts, persons of interest, etc. There are five ways to create hotlists in the system. You can:

1 Create a hotlist from existing event records. You can create this type of hotlist for your personal use or "promote" it to a system hotlist. System hotlists, in turn, can be pushed out to your AlertVU units.

2 Automatically import a hotlist from an agency server or website based on a set of predefined rules.

3 Manually import a hotlist from a file.

4 Create a one plate "Amber Alert" style hotlist by manually typing a license plate onto a popup screen. As with other system hotlists, the system will immediately push a Quick Alert hotlist out to your AlertVU units.

5 Create a hotlist from a subset of another, larger hotlist.

If you want to limit a hotlist to vehicles within a specific geographical area, you can apply one or more predefined *Locations* to that hotlist. For more on this feature, see "Maintaining Locations" on page 192.

If desired, you can have the system send you an alert any time an AlertVU unit receives a hit on a license plate that's on either one of your personal hotlists *or* a system hotlist for which you have Notification rights.

This chapter also describes how to define the hotlist formats that you will be using with AlertVU.

For more information, see:

Alerts

An alert is a notification that the system sends you any time an AlertVU unit receives a possible hit on a license plate that's on either one of your personal hotlists *or* a system hotlist for which you have Notification rights.

You can receive alerts in several different ways:

❒ A message sent to your *Inbox Messages* list on the Home page (see sample on next page).
❒ A message sent to your regular email account (see sample below). In order to receive this type of alert, you must supply the system with information on your agency's SMTP mail server, as described in chapter 6, "Forwarding System Messages to Your Regular Mailbox."
❒ A real-time popup displayed on your PC desktop (see sample on next page). In order to receive this type of alert, you must select specific settings both in the car and on the server. For detailed instructions, refer to the "Live Alerts Setup Guide", available for download from the **Tools** tab. (For downloading instructions, see "Viewing/Printing Manuals" in chapter 6.) To use live alerts, you must also activate the Live Alert Utility on your PC whenever you login, as described in "Activating the Live Alert Utility" on page 161. Please note that real-time alerts are only available for *system* hotlists. If you wish to receive alerts on a *personal* hotlist, you will first have to promote that list, as described in "Promoting a Personal Hotlist to a System Hotlist" on page 130.

In order for alerts to work properly, they have to be set up **both** at the user level **and** at the hotlist level, as described on page 92.

Regular
Email Alert

Inbox Messages Alert

Message Board				
Inbox Messages				
⦿ My Messages ○ All Messages		|< << < Page 1 of 1 (5 total records) > >> >|		
Date	State	Message Text		Actions
07/10/2015 15:21	Completed	Incoming match detected on Hotlist 'quick-alert-test'. Plate 'J97SKH' spotted on 2015.07.10 15:21:21 EDT by 'MVI-PC'.		➡ ✕

Real-Time Popup Alert

L3 Mobile-Vision - Notification Client - Version: 1.0.6 - 05/21/15 16:25

File Edit Tools Help

#	License Plate	Event Time	Hotlist
1	SCHK9	2015.07.09 13:45:24 EDT	cc-quick-alert-test
2	J97SKH	2015.07.09 13:44:47 EDT	critical
3	SCHK9	2015.07.09 13:44:23 EDT	cc-quick-alert-test
4	J97SKH	2015.07.09 13:43:45 EDT	critical
5	J97SKH	2015.07.09 13:42:44 EDT	critical

Message Details ✕

	High Severity
Dismiss Sound	
License Plate:	SCHK9
Event Time:	2015.07.09 13:45:24 EDT
Unit Name:	TERRY-PC
Lane:	undefined
Hotlist Name:	cc-quick-alert-test
Reason:	
Originating State:	
GPS Coordinates:	28.62867,-81.39555
Patch Image:	
Overview Image:	

*Connected

For more information on real-time popup alerts, see "Using the Live Alert Facility" on page 161.

Setting Alerts at the User Level

To set an alert at the *user* level, first display that user's record, then select the appropriate notification type(s). For specific instructions, see "Changing a User" in chapter 8.

Select the type of notifications that you want a user to receive whenever an AlertVU unit captures a plate that's on either one of his personal hotlists *or* a system hotlist for which he has Notification rights
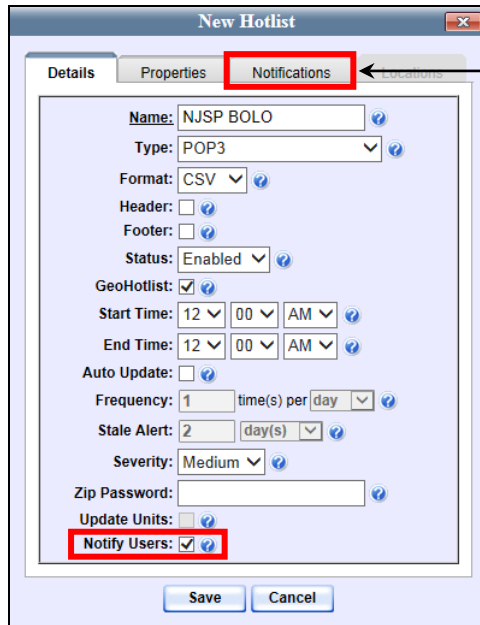
WARNING: If you select the *Inbox* and/or *Email* notifications, please be aware that you may receive dozens or even hundreds of notifications per day. You will have to review and delete these notifications on a daily basis.

Setting Alerts at the Hotlist Level

To set an alert at the *hotlist* level, first right click on the hotlist and select "edit" from the drop down menu, then select the appropriate "notify" checkbox, as shown in examples 1 – 3. If the hotlist is a *system* hotlist (including Quick Alerts), you will also need to add the appropriate users to the hotlist's **Notifications** tab.

Example 1:
Personal
Hotlist

L3 Mobile-Vision, Inc.

Example 2:
Regular
System Hotlist

New Hotlist

Details | Properties | **Notifications** | Locations

Name: NJSP BOLO
Type: POP3
Format: CSV
Header: ☐
Footer: ☐
Status: Enabled
GeoHotlist: ☑
Start Time: 12 : 00 AM
End Time: 12 : 00 AM
Auto Update: ☐
Frequency: 1 time(s) per day
Stale Alert: 2 day(s)
Severity: Medium
Zip Password:
Update Units: ☐
Notify Users: ☑

Save | Cancel

Use the **Notifications** tab to add all the users that you want to be notified whenever there's a hit on a system hotlist

Example 3:
Quick Alert
System Hotlist

New Quick Alert

Details | **Notifications**

Record Name: Missing Child
Tag: UUU90D
Description: Possible abduction
Severity: Critical
Expiration: 2 days
Update Units: ☑
Notifications: ☑

Save | Cancel

Creating Hotlists

There are two types of hotlists, as described below.

Personal   A *personal* hotlist is a list of license plates that only *you* have access to. If desired, you can have the system notify you whenever an AlertVU unit captures a license plate that is on one of your personal hotlists.

If you want to share a personal hotlist with other AlertVU users, you must first "promote" that list to a *system* hotlist, as described on page 130.

System   A *system* hotlist is a list of license plates that you can share with other users and transmit to all your AlertVU units. If desired, you can have the system notify selected users whenever an AlertVU unit captures a license plate that's on a system hotlist.

System hotlists come in four types: *automatic*, *manual*, *derivative*, and *quick alert*:

❐ *Automatic*. As its name implies, the system automatically imports this type of hotlist from a specified source, such as an agency server or website. Such imports occur on a schedule, such as daily or weekly.
❐ *Manual*. If you have access to a hotlist file on your PC or agency network, you can manually import that hotlist into AlertVU.
❐ *Derivative*. If desired, you can create a hotlist that is a subset of another, larger, hotlist.
❐ *Quick Alert*. This is a one plate "Amber Alert" style hotlist that you can quickly transmit to all your AlertVU units.

If you want to limit an *Automatic*, *Manual*, or *Derivative* hotlist to vehicles within a specific geographical area, you can apply one or more predefined *Locations* to that hotlist. For more on this feature, see "Maintaining Locations" on page 192.

For more information, see:

❐ Creating a Personal Hotlist, below
❐ Creating a System Hotlist, page 99.

Creating a Personal Hotlist

This section describes how to create a personal hotlist. For a description of this type of hotlist and how it's used, see the previous section.
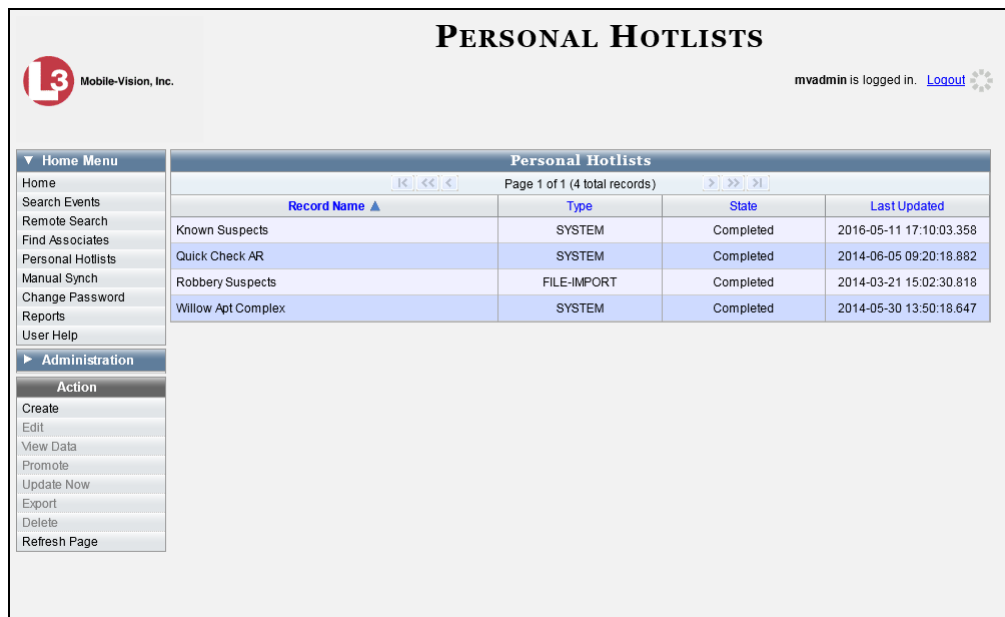
There are two ways in which you can create a new personal hotlist:

❐ Manually import an existing plate list from a file, as described in "Manually Importing a Personal Hotlist," on the next page
❐ Select event records that are currently in the system, as described in "Creating a Personal Hotlist from Existing Events," on page 98.

L3 Mobile-Vision, Inc.

Manually Importing a Personal Hotlist

This section describes how to create a new personal hotlist by importing a list of license plates in a selected format.

1 Go to ▼ Home Menu and click **Personal Hotlists**. The Personal Hotlists page displays.

The columns on this page are described below.

Personal Hotlists	
Column	**Description**
Record Name	The name of this personal hotlist. This is how the hotlist will appear throughout the application.
Type	The manner in which this hotlist was created: ▪ *FILE-IMPORT*. This hotlist was manually imported from a file. ▪ *SYSTEM*. This hotlist was created from a list of existing events.
State	The current creation status of this hotlist: ▪ *Completed*. The system has successfully imported this hotlist *or* created it from an events list. ▪ *Queued*. The system is in the process of importing this hotlist from a file.

(Continued)

Chapter 3: Hotlists
Creating Hotlists

Personal Hotlists (cont'd)	
Column	**Description**
State (cont'd)	▪ *Updating*. The system is in the process of reimporting this hotlist from a file. ▪ *Failed*. The system was unable to update this hotlist, possibly because the hotlist's format did not match the selected value in the *Format* field.
Last Updated	The date and time at which this hotlist was last updated.
Available Actions	
If an action is "grayed out" (i.e., unavailable), it indicates that you must select a hotlist record before you can perform that action.	
Action	**Description**
Create	Create a new hotlist by manually importing a file containing a list of license plates.
Edit	Change a hotlist's name or notification status.
View Data	View a hotlist's license plates and metadata.
Promote	Convert a *personal* hotlist to a *system* hotlist.
Update Now	Reimport a hotlist's source file.
Export	Copy a hotlist's license plates to a .csv spreadsheet file.
Delete	Permanently remove a hotlist from the server.
Refresh Page	Redisplay the current webpage to reflect any recent updates, such as a change in the value of the *State* column.

2   Go to the Action column and click **Create**. The Import Manual Hotlist popup displays.
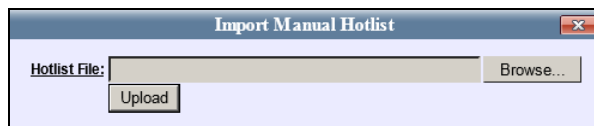
3   Click the **Browse** button. The Choose File to Upload popup displays.

4   Navigate to the disk drive location where the import file resides.

5   Double-click on the import file. The selected file name displays in the *Hotlist File* field.

L3 Mobile-Vision, Inc.
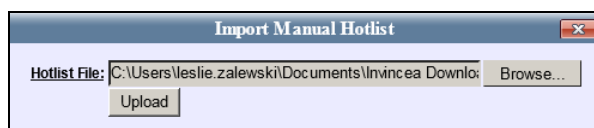
6 Click **Upload**. After a momentary delay, the Hotlist Properties popup displays.

Hotlist Properties

Name:	
Format:	CSV
Header:	☐
Footer:	☐
Notify Me:	☐

Save   Cancel
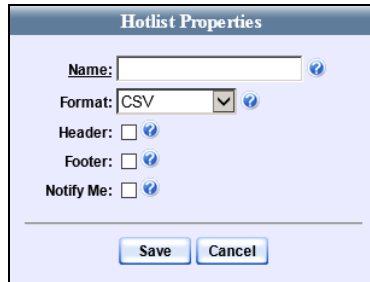
7 Enter a descriptive name for this hotlist in the *Name* field.

8 Select the import file's format from the *Format* drop-down list. This list includes some or all of the following formats, as well as any additional hotlist formats defined by your agency.

AR NLETS .... Arkansas National Law Enforcement Telecommunication System
CLEW SVS .... California Law Enforcement Web Stolen Vehicle Systems
CSV .... Comma separated text file
FCIC .... Florida Crime Information Center
MD MVA .... Maryland Motor Vehicle Administration
NCIC .... National Crime Information Center
TXLETS .... Texas Law Enforcement Telecommunication System

9 If the import file includes a header, select the *Header* checkbox. Otherwise proceed to the next step.

10 If the import file includes a footer, select the *Footer* checkbox. Otherwise proceed to the next step.

11 To receive a system alert whenever any AlertVU unit captures an event that matches a license plate on this hotlist, select the *Notify Me* checkbox. Otherwise proceed to the next step.

12 Click the **Save** button. A confirmation message displays.
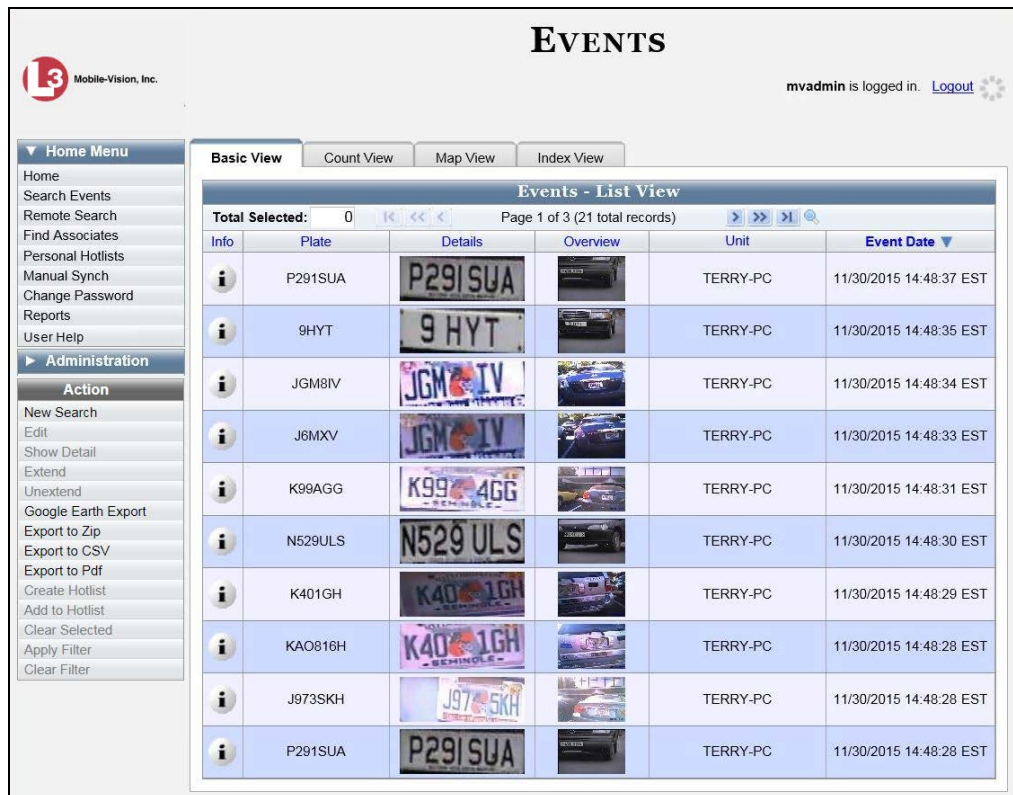
> The Hotlist named Morris County successfully saved and is queued for import. When import is complete, a message will be sent to your Inbox.

Creating a Personal Hotlist from Existing Events

This section describes how to create a new personal hotlist from event records that currently reside on either the local server or selected remote server(s).

For a definition of personal hotlists and how they're used, see "Creating Hotlists" on page 94.

1   Search for the events you wish to incorporate into your new hotlist. (If necessary, review "Searching for Events" in chapter 2.)

2   Select the events you wish to incorporate into your new hotlist:

To select *all* events on your search results list, click the **Index View** tab, then click the **Select All** button at the top of the page.

– OR –

To select *some* events on your search results list, click on the appropriate event record(s) to highlight them. If necessary, use the navigation arrows at the top of the page to scroll through the full list.

3   Once the desired event records are selected, go to the Action column and click **Create Hotlist**. The Create Hotlist popup displays.

4 Enter a descriptive name for this hotlist in the *Hotlist Name* field.

5 To receive a system alert whenever any AlertVU unit captures an event that matches a license plate on this hotlist, select the *Notify Me* checkbox. Otherwise proceed to the next step.

6 Click **Save**. A confirmation message displays.

Hotlist Morris County successfully created.

Creating a System Hotlist

This section describes how to create a system hotlist. For a definition of system hotlists and how they're used, see "Creating Hotlists" on page 94.

There are five ways in which you can create a new system hotlist:

❐ Manually import an existing plate list from a file.
❐ Automatically import a hotlist from a specified source, such as an agency server or website. The system will automatically update this type of hotlist according to a set of predefined rules.
❐ Convert or "promote" a *personal* hotlist to a *system* hotlist
❐ Create a one plate "Amber Alert" style hotlist that you can immediately transmit to all your AlertVU units.
❐ Create a hotlist from a subset of another, larger, hotlist. This is referred to as a *derivative* hotlist.
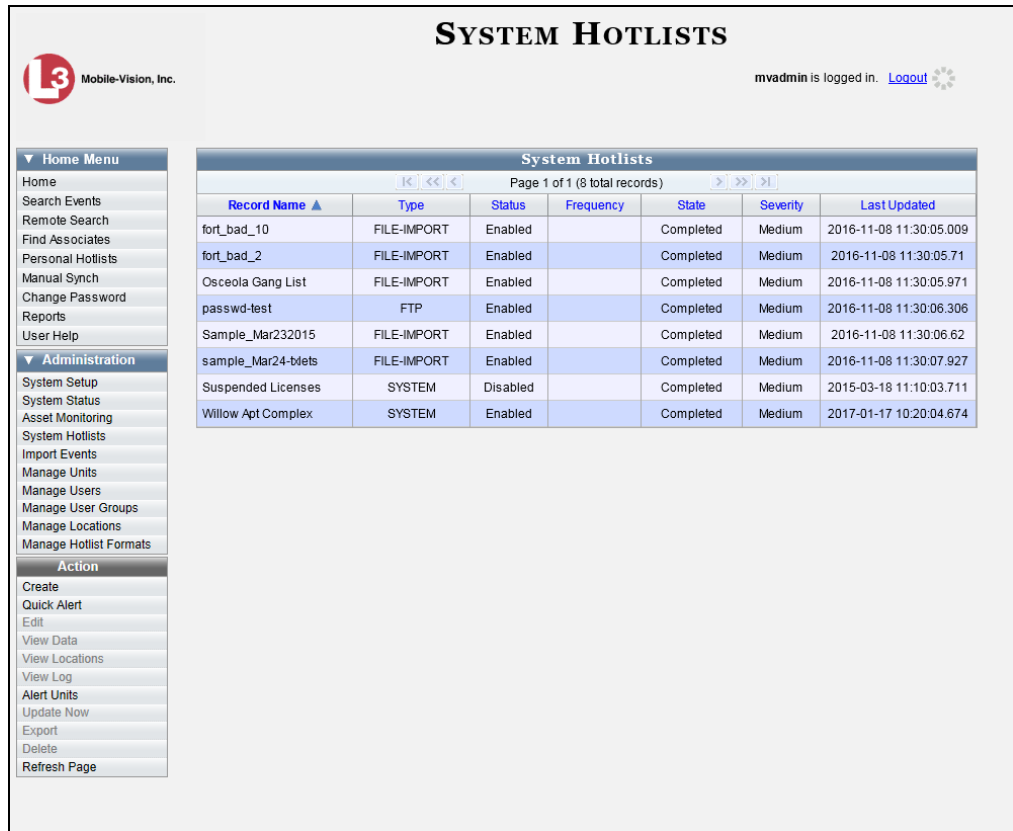
For specific instructions, see:

❐ Manually Importing a System Hotlist, next page
❐ Automatically Importing a System Hotlist, page 109
❐ Promoting a Personal Hotlist to a System Hotlist, page 130
❐ Creating a Quick Alert Hotlist, page 132
❐ Creating a Derivative Hotlist, page 135.

Manually Importing a System Hotlist

This section describes how to manually import a system hotlist that's in a predefined format. For a definition of system hotlists and how they're used, see "Creating Hotlists" on page 94.

1 Go to ▼ Administration and click **System Hotlists**. The System Hotlists page displays.

The components on this page are described in the following table.

L3 Mobile-Vision, Inc.

System Hotlists	
Column	**Description**
Record Name	The name of this system hotlist.
Type	The manner in which this hotlist was created: ▪ FILE-IMPORT. This hotlist was manually imported from a file. ▪ SYSTEM. This hotlist was promoted from a *personal* hotlist to a *system* hotlist. ▪ QUICK. This hotlist was manually input via the New Quick Alert screen. ▪ DERIVATIVE. This hotlist was manually created from a subset of another hotlist. ▪ POP3. This hotlist was automatically imported from a mail server. ▪ FTP. This hotlist was automatically imported from an FTP server. ▪ SFTP. This hotlist was automatically imported from a secure FTP server. ▪ HTTP. This hotlist was automatically imported from a web address. ▪ FILE-SHARE (PUBLIC). This hotlist was automatically imported from a public file share path. ▪ FILE-SHARE (PRIVATE). This hotlist was automatically imported from a password-protected file share path. ▪ TXLETS. This hotlist was automatically imported from the Texas Law Enforcement Telecommunication System.
Status	The current status of this hotlist: ▪ *Enabled*. This hotlist is *active*. It can receive automatic updates from the server, generate alerts for incoming hits, and appear on mobile units' list of active hotlists. ▪ *Disabled*. This hotlist is *inactive*. It *cannot* receive automatic updates from the server, generate alerts for incoming hits, or appear on mobile units' list of active hotlists.
Frequency *(Auto-import hotlists only)*	The number of times per day or week that the system will check for updates to this hotlist. This is an optional feature that applies to auto-import system hotlists only.
State	The current creation status of this hotlist: ▪ *Completed*. The system has successfully created this hotlist either by importing it, converting it from a personal hotlist, or deriving (i.e., excerpting) it from an existing hotlist. ▪ *Queued*. The system is getting ready to import or update this hotlist. ▪ *Updating*. The system is in the process of reimporting this hotlist's source file.

(Continued)

System Hotlists (cont'd)	
Column	**Description**
State (cont'd)	▪ *Failed*. The system was unable to update this hotlist, possibly because the hotlist's format did not match the selected value in the *Format* field.
Severity	The importance of this hotlist: *critical*, *high*, *medium* (default), or *low*.
Last Updated	The date and time at which this hotlist was last updated.
Available Actions	
If an action is "grayed out" (i.e., unavailable), it indicates that you must select a hotlist record before you can perform that action.	
Action	**Description**
Create	Define a new system hotlist.
Quick Alert	Create a one plate "Amber Alert" style hotlist by manually typing a license plate number onto a popup screen.
Edit	Change a hotlist's properties *or* add user(s) to a hotlist's *Notifications* list.
View Data	View a hotlist's license plates and metadata.
View Log	View the logs which document the success or failure of previous hotlist retrievals.
View Locations	View the predefined Locations that are currently linked to this hotlist.
Alert Units	Manually push all system hotlists out to all AlertVU units that need them. Any unit that is missing a particular hotlist or has an outdated version of a hotlist will receive the appropriate update(s).
Update Now	Reimport a hotlist's source file.
Export	Copy a hotlist's license plates and metadata to a .csv spreadsheet file.
Delete	Permanently remove a hotlist from the server.
Refresh Page	Redisplay the current webpage to reflect any recent updates, such as a change in the value of the *State* column.

2 Go to the Action column and click **Create**. The New Hotlist popup displays.

L3 Mobile-Vision, Inc.

3 Select **Create Manual Hotlist**.

4 Click **OK**. The Import Manual Hotlist popup displays.
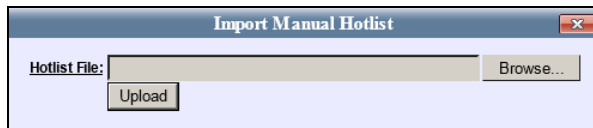
5 Click the **Browse** button. The Choose File to Upload popup displays.

6 Navigate to the disk drive location where the hotlist file resides.

7 Double-click on the hotlist file. The selected file name displays in the *Hotlist File* field.

8 Click **Upload**. After a delay of 10 – 20 seconds, the Hotlist Properties popup displays.
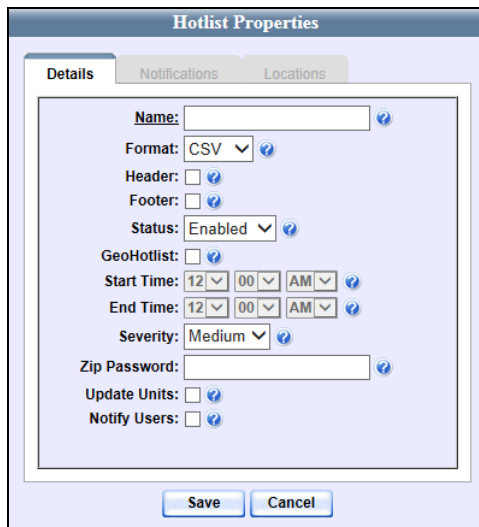
9   Enter a descriptive name for this hotlist in the *Name* field.

10 Select the import file's format from the *Format* drop-down list. This list includes some or all of the following formats, as well as any additional hotlist formats defined by your agency.

AR NLETS .... Arkansas National Law Enforcement Telecommunication System
CLEW SVS .... California Law Enforcement Web Stolen Vehicle Systems
CSV .... Comma separated text file
FCIC .... Florida Crime Information Center
MD MVA .... Maryland Motor Vehicle Administration Maryland Motor Vehicle
NCIC .... National Crime Information Center Administration
TXLETS .... Texas Law Enforcement Telecommunication System

11 If the import file includes a header, select the *Header* checkbox. Otherwise proceed to the next step.

12 If the import file includes a footer, select the *Footer* checkbox. Otherwise proceed to the next step.

13 To limit this hotlist to a certain geographic region, such as a school zone, proceed to the next step. Otherwise skip to step 17.

14 Select the *GeoHotlist* checkbox.
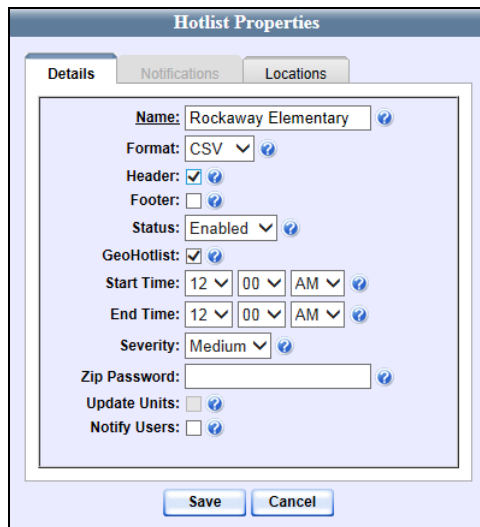
15 Using the *Start Time* drop-down lists, enter the beginning of the daily time range in which the Location parameter will be active for this hotlist. For example, if your Location is a school zone, you might specify a *Start Time* of 8:00 a.m.

16 Using the *End Time* drop-down lists, enter the end of the daily time range in which the Location parameter will be active for this hotlist. For example, if your Location is a school zone, you might specify an *End Time* of 3:30 p.m.

17 To set this hotlist's severity level to **Medium** (default), proceed to the next step.

– OR –

To assign a different severity level to this hotlist, select a new value from the *Severity* drop-down list.

18 If this hotlist will be transmitted to the AlertVU server via an encrypted zip file, enter the required password in the *Zip Password* field. Otherwise proceed to the next step.
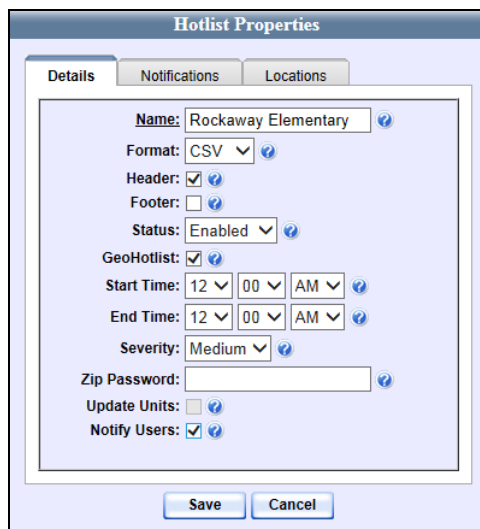
19 If you want the system to automatically push an update out to all AlertVU units whenever a change is made to this hotlist, select the *Update Units* checkbox. Otherwise proceed to the next step.

20 If you want the system to send an alert to selected users whenever any AlertVU unit captures a license plate that's on this hotlist, proceed to the next step.

– OR –

If you do *not* want the system to send alerts to any users, skip to step 25.

21 Select the *Notify Users* checkbox.

22 Click the **Notifications** tab. A list of system users displays.

(Continued)
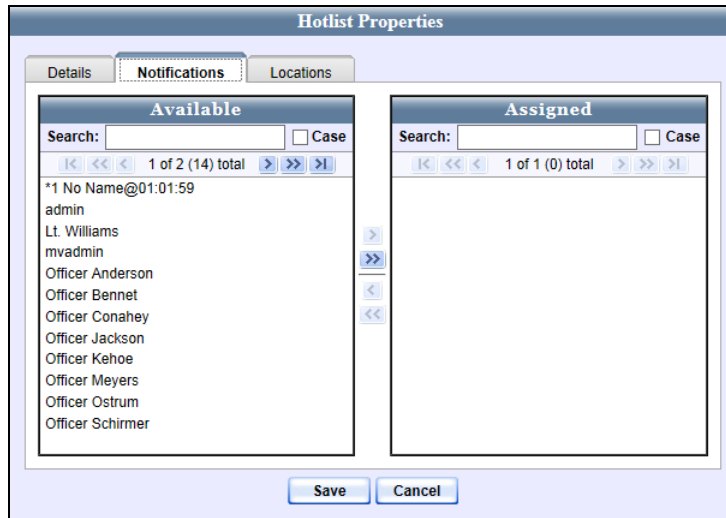
23 Go to the left column (Available) and click on the users you wish to notify whenever an AlertVU unit captures a plate on this hotlist. If the user you're looking for does not appear onscreen, use the navigation arrows at the top of the column to scroll through the user list.

24 Once you've highlighted the desired users, click the ▶ icon located between the two columns. The selected users display in the right column (Assigned).
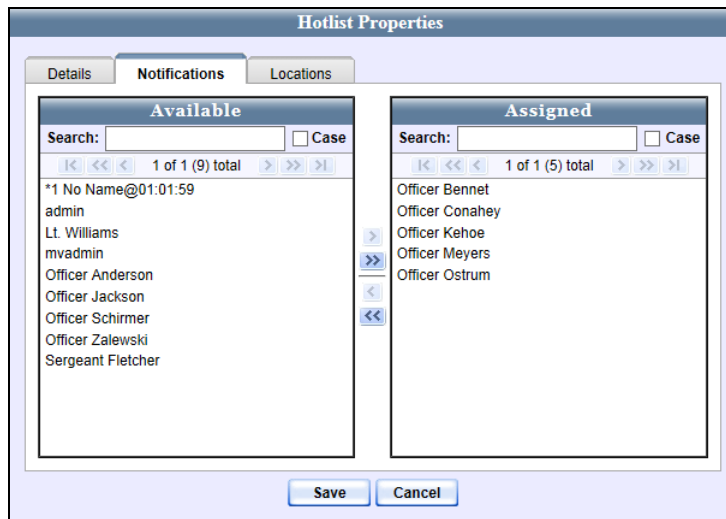
25 If the **Locations** tab is available, proceed to the next step.

– OR –

If the **Locations** tab is *not* available, skip to step 34.

26 Click the **Locations** tab.
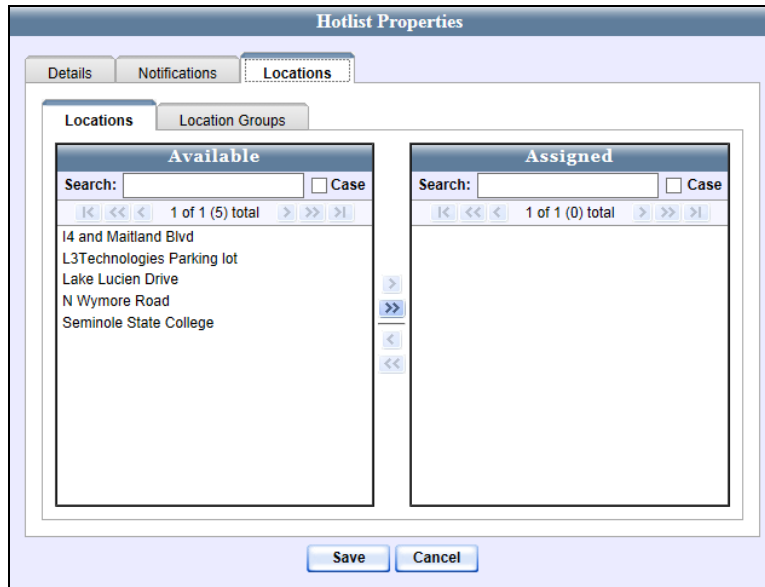
27 To assign one or more *Locations* to this hotlist, proceed to the next step.

– OR –

To assign a *Location Group* to this hotlist, skip to step 31.

28 Go to the *Available* column and click on the Location(s) you wish to assign to this hotlist.

29 Click the ➤ icon located between the two columns. The selected Location(s) display in the *Assigned* column.
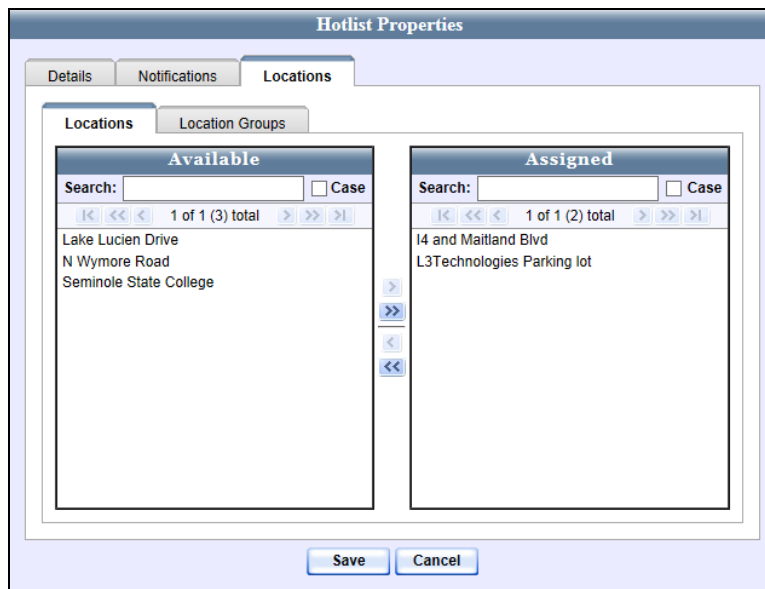
30 If you also wish to add a Location Group to this hotlist, proceed to the next step. Otherwise skip to step 34.

31   Click the **Location Groups** tab.
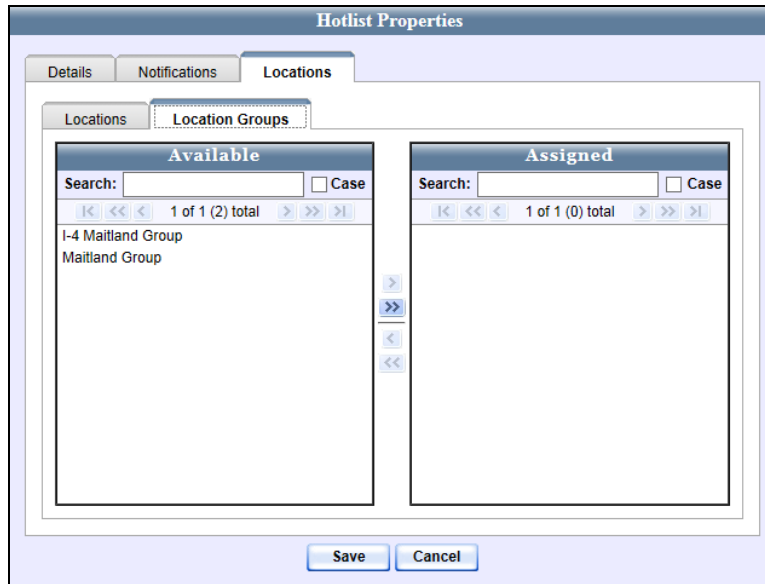
32   Go to the *Available* column and click on the Location Group you wish to assign to this hotlist.

33   Click the ▶ icon located between the two columns. The selected Location Group displays in the *Assigned* column.
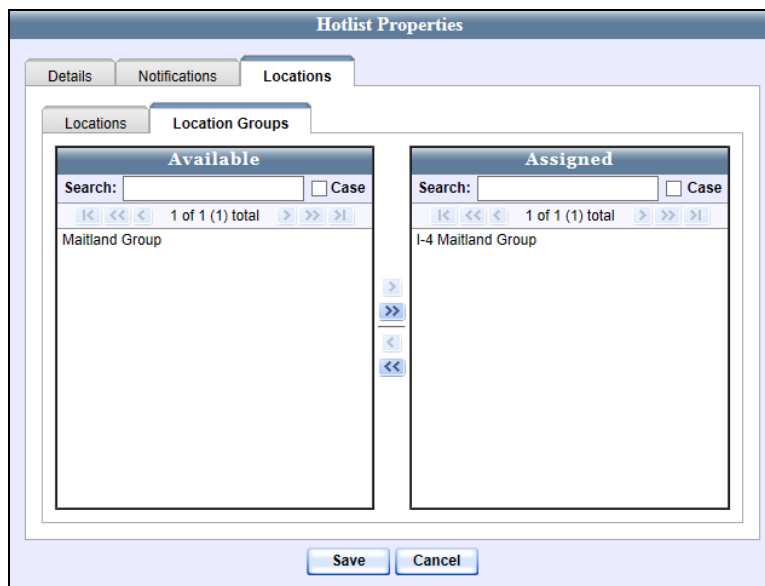
34   Click **Save**. A confirmation message displays.

> The Hotlist named **National BOLOs** successfully saved and is queued for import. When import is complete, a message will be sent to your Inbox.
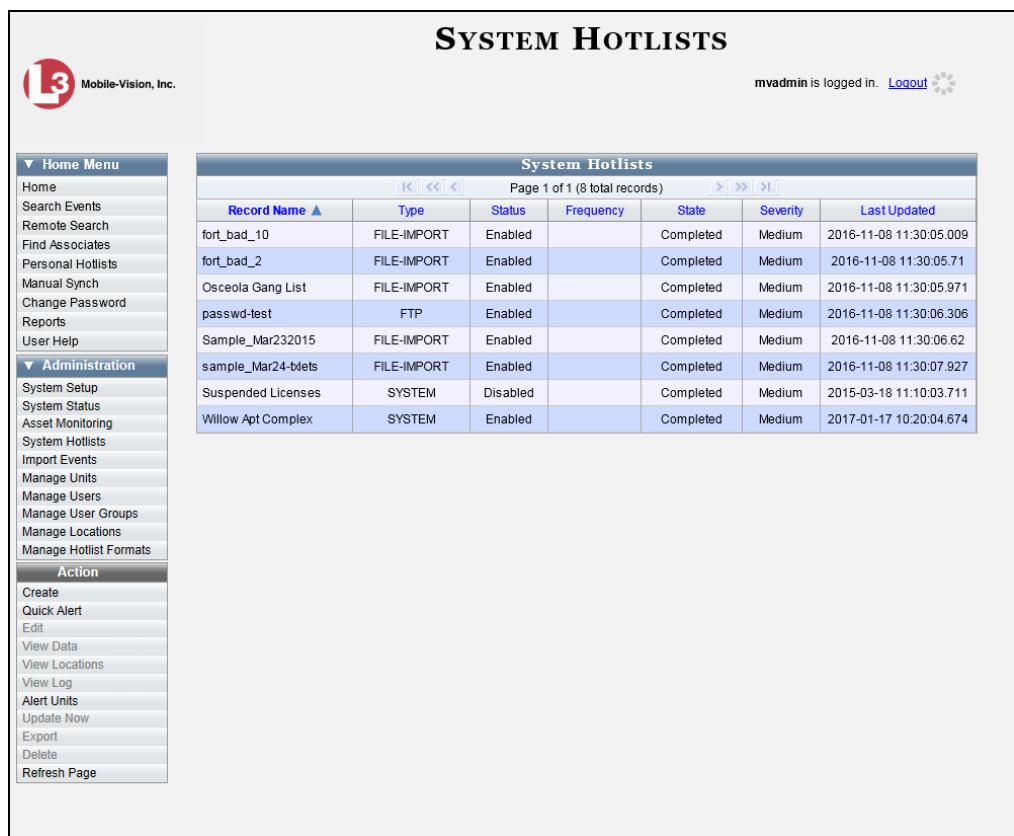
Automatically Importing a System Hotlist

This section describes how to create a new hotlist that the system will automatically import and update on a schedule. This is the "set it and forget it" approach to using hotlists.

For a definition of system hotlists and how they're used, see "Creating Hotlists" on page 94.

Part 1: Details

1 Go to ▼ Administration and click **System Hotlists**. The System Hotlists page displays.

The components on this page are described in the table on page 101.

2 Go to the Action column and click **Create**. The New Hotlist popup displays.

3 Make sure **Create Automatic Hotlist** is selected, then click **OK**. The New Hotlist form displays.

The fields on this popup are described below.

New Hotlist	
Column	**Description**
Name	The name of this system hotlist.
Type	The retrieval method that the system will use to import this hotlist. Select this value from the drop-down list.
	▪ POP3. Import the hotlist from an email attachment sent to you or another System Administrator. A specific word or word(s) in the subject line will identify the exact hotlist to the system.
	▪ FTP. Import the hotlist from an FTP server.
	▪ SFTP. Import the hotlist from a secure FTP server.
	▪ HTTP. Import the hotlist from a web address.
	▪ FILE SHARE (PUBLIC). Import the hotlist from a public file share path.
	▪ FILE SHARE (PRIVATE). Import the hotlist from a password-secured file share path.
	▪ TXLETS. Import the hotlist from the Texas Law Enforcement Telecommunication System.
Format	The format for this hotlist, which includes some or all of the following formats, as well as any additional hotlist formats defined by your agency.
	(Continued)

L3 Mobile-Vision, Inc.
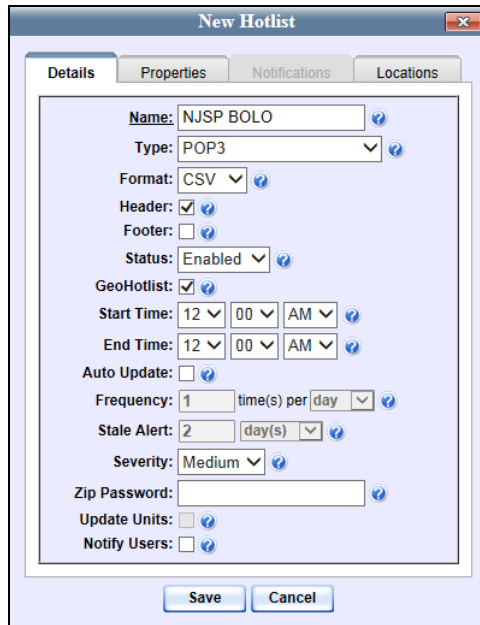
New Hotlist (cont'd)	
Column	**Description**
Format (cont'd)	▪ AR NLETS. Arkansas National Law Enforcement Telecommunication System ▪ CLEW SVS. California Law Enforcement Web Stolen Vehicle Systems ▪ CSV. Comma separated text file ▪ FCIC. Florida Crime Information Center ▪ MD MVA. Maryland Motor Vehicle Administration ▪ NCIC. National Crime Information Center ▪ TXLETS. Texas Law Enforcement Telecommunication System *Select this value from the drop-down list.*
Header	A checkbox used to indicate whether or not the hotlist file contains a header. A header is the optional first line of text that contains column descriptions but doesn't contain any valid plate information. ☑ The file contains a header. ☐ The file does *not* contain a header.
Footer	A checkbox used to indicate whether or not the hotlist file contains a footer. A footer is the optional last line of text that contains column descriptions but doesn't contain any valid plate information. ☑ The file contains a footer. ☐ The file does *not* contain a footer.
Status	The current status of this hotlist: ▪ *Enabled.* This hotlist is *active*. It can receive automatic updates from the server, generate alerts for incoming hits, and appear on mobile units' list of active hotlists. ▪ *Disabled.* This hotlist is *inactive*. It *cannot* receive automatic updates from the server, generate alerts for incoming hits, or appear on mobile units' list of active hotlists.
GeoHotlist	A checklist that enables you to limit this hotlist to a certain geographic region, such as a school zone. If you select this option, you will have an opportunity to add a predefined *Location* or *Location Group* to the Hotlist. For more information on this topic, see "Maintaining Locations" on page 192. ☑ Limit this hotlist to a specified geographic region ☐ Do *not* Limit this hotlist to a specified geographic region If you select this checkbox, you are required to enter an associated time range (see *Start Time* and *End Time* fields).

(Continued)

New Hotlist (cont'd)	
Column	**Description**
Start Time	The beginning of the daily time range in which the Location parameter will be active for this hotlist. For example, if your Location is a school zone, you might specify a *Start Time* of 8:00 a.m. *Select a value from the drop-down lists provided.*
End Time	The end of the daily time range in which the Location parameter will be active for this hotlist. For example, if your Location is a school zone, you might specify an *End Time* of 3:30 p.m. *Select a value from the drop-down lists provided.*
Auto Update	A checkbox used to indicate whether or not you want the system to automatically check for updates to this hotlist's source file. If the system finds that the hotlist's source file has changed since the last import, it will automatically reimport the file. This field must be used in combination with the *Frequency* field to specify the number of times per day or week that the system will check the source file for updates. ☑ Automatically check hotlist source file for changes. ☐ Do *not* check hotlist source file for changes.
Frequency	The number of times per day or week that the system will check for changes to this hotlist's source file. Used in combination with the *Auto Update* field described above. System defaults to *one time per day*.
Stale Alert	An automatic alert for System Administrators. If you complete this field, then if the system is unable to update this hotlist in **X** number of hours, days, or weeks, it will automatically send an alert to the System Administrator's *Inbox Messages* list. System default is **2 days**. *Enter a number in the first field segment and select either* **hours(s)**, **day(s)**, *or* **week(s)** *from the second field segment.* Stale Alert: 1 week(s) ▼ ❷ In the example above, if the system has been unable to update a hotlist for one full week, it will automatically send an alert message to the System Administrator's *Inbox Messages* list.
Severity	The importance of this list: *critical*, *high*, *medium* (default), or *low*. *Select this value from the drop-down list.*
Zip Password	The password for the encrypted zip file, if applicable. Some, but not all, hotlist uploads require a password.

L3 Mobile-Vision, Inc.

New Hotlist (cont'd)	
Column	**Description**
Update Units	A checkbox used to indicate whether or not you want the system to automatically push an update out to all AlertVU units whenever a change is made to this hotlist. ☑ Automatically notify all AlertVU units whenever this hotlist changes. ☐ Do *not* automatically notify all AlertVU units whenever this hotlist changes.
Notify Users	A checkbox used to indicate whether or not you want the system to send an alert to all users on the hotlist's *Notifications* list whenever an AlertVU unit captures a license plate that's on this hotlist. ☑ Send an alert to all users on the hotlist's *Notifications* list whenever any AlertVU unit receives a hit on this hotlist. ☐ Do *not* send an alert to all users on the hotlist's *Notifications* list whenever any AlertVU unit receives a hit on this hotlist.

4 Enter a unique name for this hotlist in the *Name* field.

5 Select a file retrieval method for this hotlist from the *Type* drop-down list.

6 Select a format for this hotlist from the *Format* drop-down list. This list includes some or all of the following formats, as well as any additional hotlist formats defined by your agency.

AR NLETS .... Arkansas National Law Enforcement Telecommunication System
CLEW SVS .... California Law Enforcement Web Stolen Vehicle Systems
CSV .... Comma separated text file
FCIC .... Florida Crime Information Center
MD MVA .... Maryland Motor Vehicle Administration
NCIC .... National Crime Information Center
TXLETS .... Texas Law Enforcement Telecommunication System

7 If the hotlist file includes a header, select the *Header* checkbox. Otherwise proceed to the next step.

8 If the hotlist file includes a footer, select the *Footer* checkbox. Otherwise proceed to the next step.

9 To limit this hotlist to a certain geographic region, such as a school zone, proceed to the next step. Otherwise skip to step 13.

10 Select the *GeoHotlist* checkbox.

11 Using the *Start Time* drop-down lists, enter the beginning of the daily time range in which the Location parameter will be active for this hotlist. For example, if your Location is a school zone, you might specify a *Start Time* of 8:00 a.m.

12 Using the *End Time* drop-down lists, enter the end of the daily time range in which the Location parameter will be active for this hotlist. For example, if your Location is a school zone, you might specify an *End Time* of 3:30 p.m.

13 If you want the system to automatically check for updates to the hotlist source file **X** number of times per day or week, select the *Auto Update* checkbox. Proceed to the next step.

– OR –

If you do *not* want the system to automatically reimport the hotlist source file **X** number of times per day or week, skip to step 19.

14 Enter a number in the *Frequency* field to indicate how many times per day or week you want the system to automatically reimport the hotlist file.

15 Select a time interval (i.e., **day** or **week**) from the *time(s) per* drop-down list.

16 If you want the system to notify you if it's unable to reimport the hotlist file after **X** number of days or weeks, proceed to the next step. Otherwise skip to step 19.

17 Enter a number in the *Stale Alert* field to indicate how many days, weeks, or hours should go by without an update before the system notifies you.

18 Select an appropriate time interval—**hour(s)**, **day(s)**, or **week(s)**—from the *Stale Alert* drop-down list.

19 To set this hotlist's severity level to **Medium** (default), proceed to the next step.

– OR –

To assign a different severity level to this hotlist, select a new value from the *Severity* drop-down list.

20 If this hotlist will be transmitted to the AlertVU server via an encrypted zip file, enter the required password in the *Zip Password* field. Otherwise proceed to the next step.

21 If you want the system to automatically push an update out to all AlertVU units whenever a change is made to this hotlist, select the *Update Units* checkbox. Otherwise proceed to the next step.

22 If you want the system to send an alert to selected users whenever any AlertVU unit captures a license plate that's on this hotlist, select the *Notify Users* checkbox. Otherwise proceed to the next step.

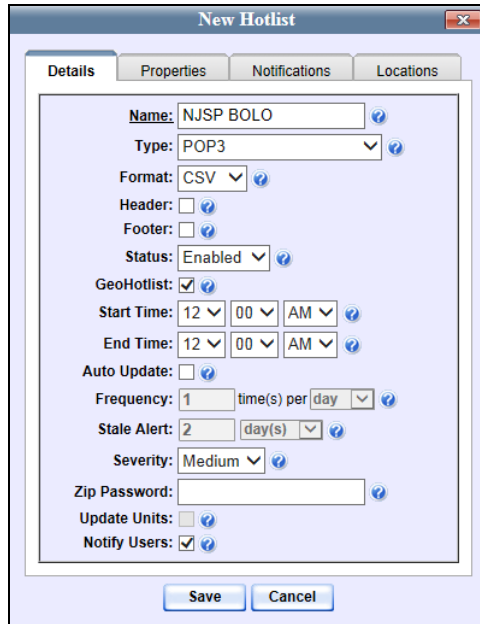**23** Note the value in the *Type* field. Your next few steps will vary depending on this value.

Proceed to "Part II: Properties" below.

Part II: Properties

Proceed to the appropriate page for further instructions:

If you selected this Type…	Proceed to this page…
POP3	116
FTP	117
SFTP	119
HTTP	120
FILE SHARE (PUBLIC)	122
FILE SHARE (PRIVATE)	123
TXLETS	125

POP3
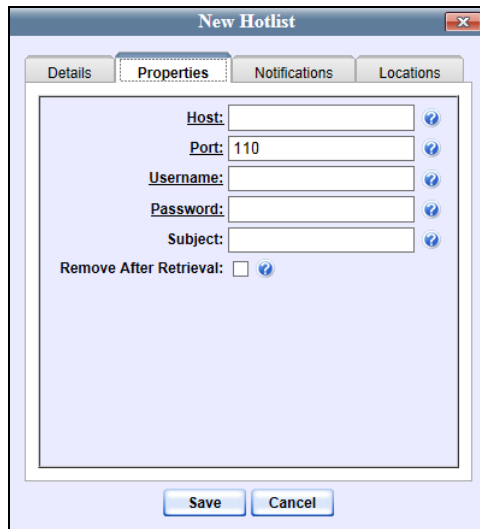
1 Click the **Properties** tab.

Host **2** Enter the mail server host. This may be either a resolvable DNS name or an IP address.

Port **3** To use port **110** to access this mail server (default), proceed to the next step. Otherwise enter a different value in the *Port* field.

Username **4** Enter the username that the system should use to access this server.

Password **5** Enter the password for the *Username* you just entered.

L3 Mobile-Vision, Inc.

6 If the system will need to search for specific text in the subject line of the user's *Inbox*, proceed to the next step. Otherwise skip to step 8.

Subject **7** Enter the subject line text to search for, as described in step 6.

Remove after Retrieval **8** If you want the system to delete the email message after its contents have been ingested into the hotlist, select the *Remove After Retrieval* checkbox. Otherwise proceed to the next step.

9 If the **Notifications** tab is available, proceed to "Part III: Notifications" on page 126 for further instructions.

– OR –

If the **Notifications** tab is *not* available (i.e., grayed-out), proceed to the next step.

10 If the **Locations** tab is available, proceed to Part IV: Locations on page 128.
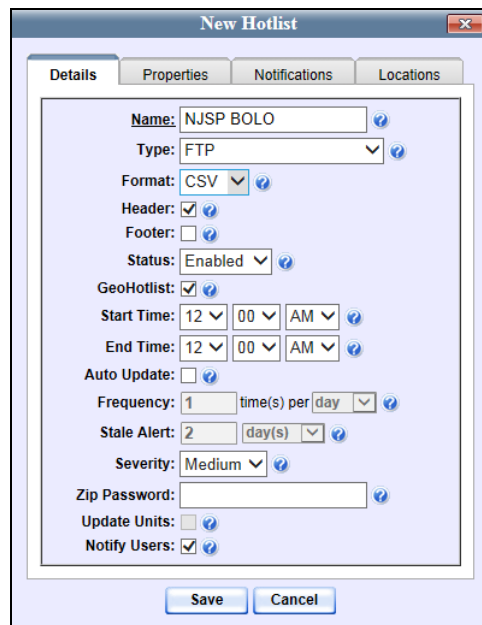
– OR –

If the **Locations** tab is *not* available (i.e., grayed-out), proceed to the next step.

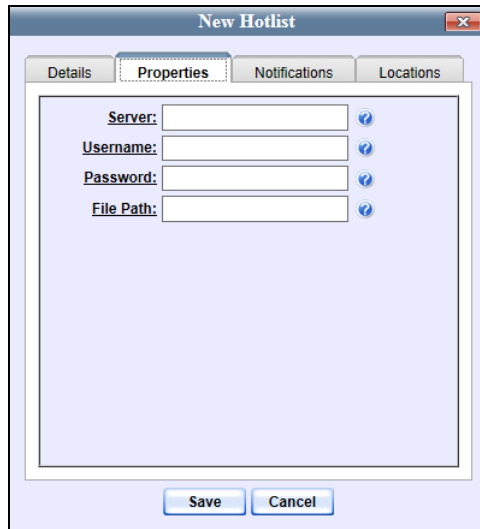**11** click **Save**. A confirmation message displays.

> The Hotlist named **National BOLOs** **successfully saved and is queued for import. When import is complete, a message will be sent to your Inbox.**

End of Procedure.
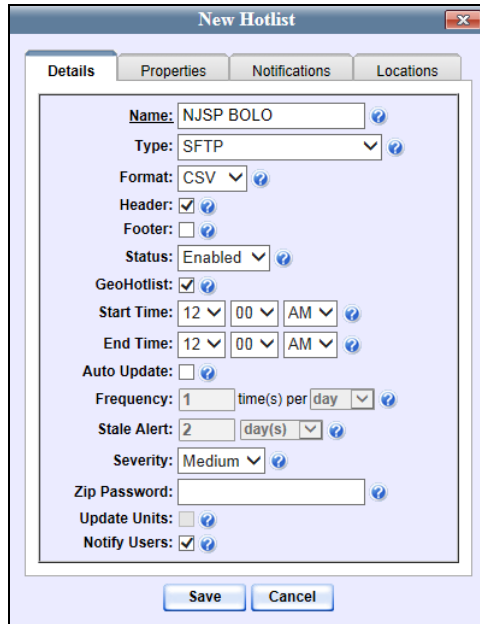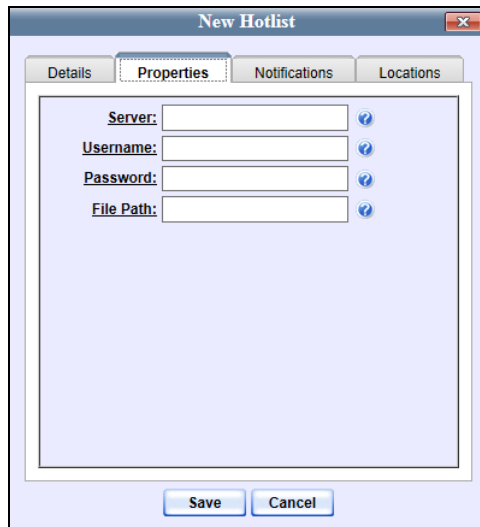
FTP

1 Click the **Properties** tab.

Server	**2**	Enter the name or IP address of the FTP server.
Username	**3**	Enter the username that the system should use to access this server.
Password	**4**	Enter the password for the *Username* above.
File Path	**5**	Enter the path to the FTP file.

6 If the **Notifications** tab is available, proceed to "Part III: Notifications" on page 126 for further instructions.

– OR –

If the **Notifications** tab is *not* available (i.e., grayed-out), proceed to the next step.

7 If the **Locations** tab is available, proceed to Part IV: Locations on page 128.

– OR –

If the **Locations** tab is *not* available (i.e., grayed-out), proceed to the next step.

8 Click **Save**. A confirmation message displays.

> The Hotlist named **National BOLOs** successfully saved and is queued for import. When import is complete, a message will be sent to your Inbox.

End of Procedure.

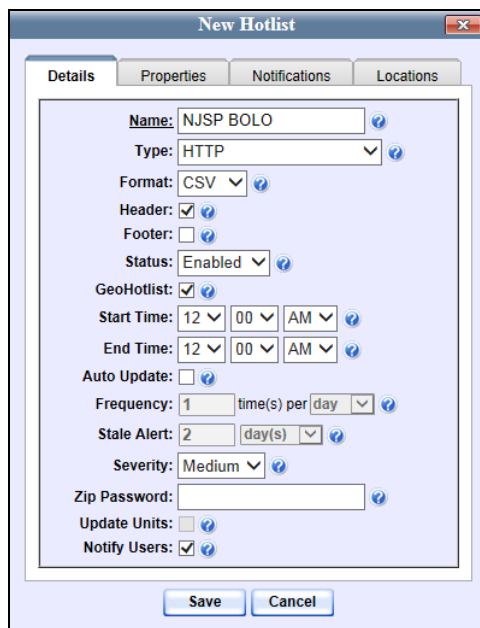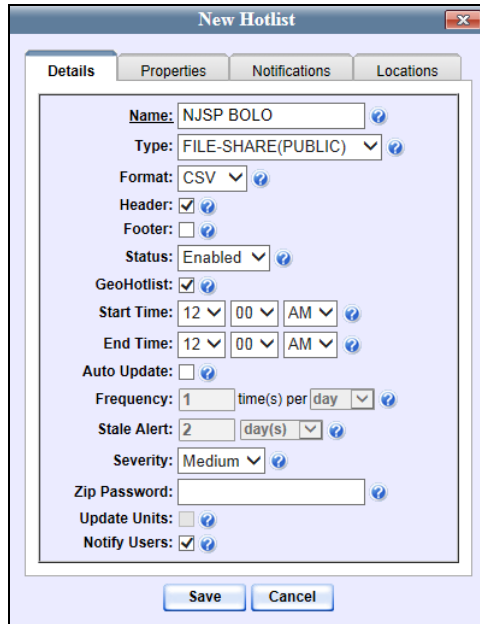**SFTP**

1   Click the **Properties** tab.

Server   2   Enter the name or IP address of the secure FTP server.

Username   3   Enter the username that the system should use to access this server.

Password   4   Enter the password for the *Username* above.

File Path   5   Enter the path to the SFTP file.

6 If the **Notifications** tab is available, proceed to "Part III: Notifications" on page 126 for further instructions.

– OR –

If the **Notifications** tab is *not* available (i.e., grayed-out), proceed to the next step.

7 If the **Locations** tab is available, proceed to Part IV: Locations on page 128.

– OR –

If the **Locations** tab is *not* available (i.e., grayed-out), proceed to the next step.

8 Click **Save**. A confirmation message displays.

> The Hotlist named **National BOLOs** successfully saved and is queued for import. When import is complete, a message will be sent to your Inbox.

End of Procedure.
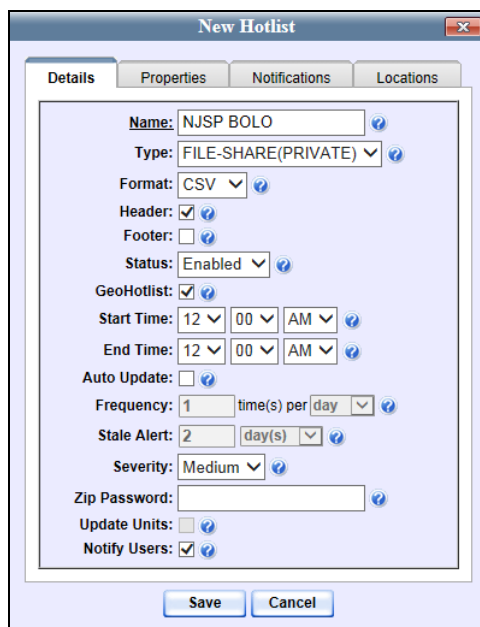
HTTP

1 Click the **Properties** tab.

L3 Mobile-Vision, Inc.
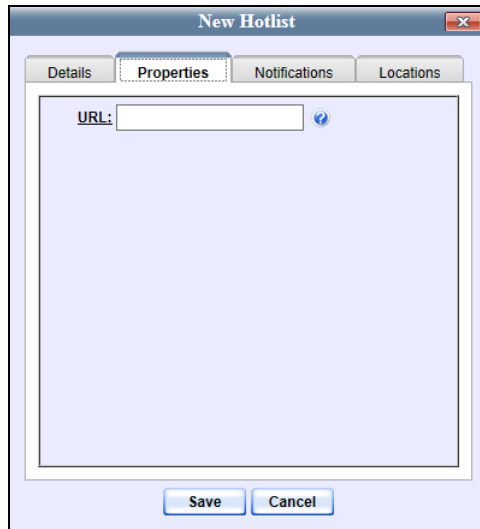
2 Enter the web address from which the hotlist file will be retrieved.

3 If the **Notifications** tab is available, proceed to "Part III: Notifications" on page 126 for further instructions.

– OR –

If the **Notifications** tab is *not* available (i.e., grayed-out), proceed to the next step.

4 If the **Locations** tab is available, proceed to Part IV: Locations on page 128.

– OR –

If the **Locations** tab is *not* available (i.e., grayed-out), proceed to the next step.

5 Click **Save**. A confirmation message displays.

> The Hotlist named National BOLOs successfully saved and is queued for import. When import is complete, a message will be sent to your Inbox.
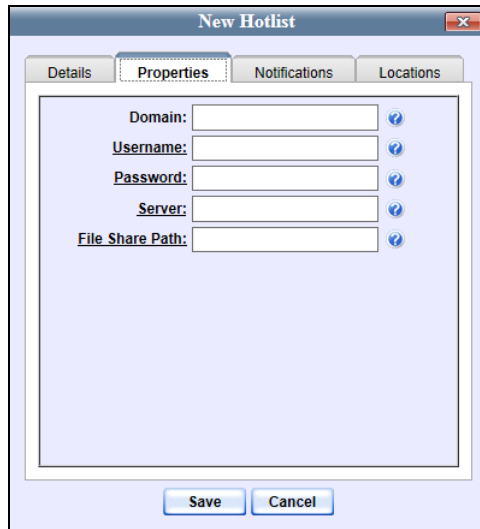
End of Procedure.

FILE SHARE (PUBLIC)

1   Click the **Properties** tab.

2   Enter the path to the shared file, including the name or IP address of the host server or Windows machine.

3   If the **Notifications** tab is available, proceed to "Part III: Notifications" on page 126 for further instructions.

– OR –

If the **Notifications** tab is *not* available (i.e., grayed-out), proceed to the next step.

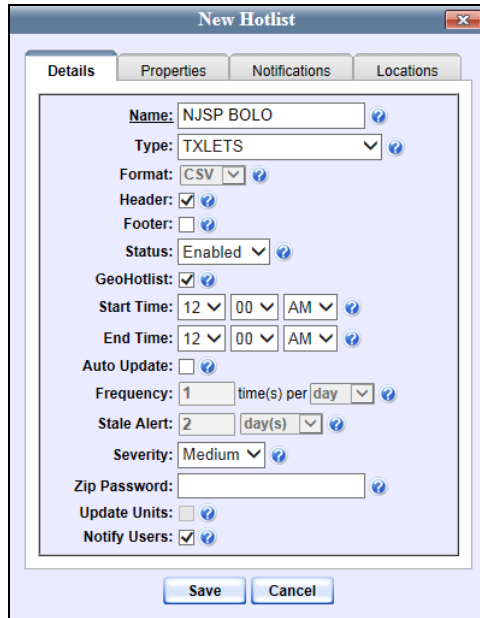**4** If the **Locations** tab is available, proceed to Part IV: Locations on page 128.

– OR –

If the **Locations** tab is *not* available (i.e., grayed-out), proceed to the next step.

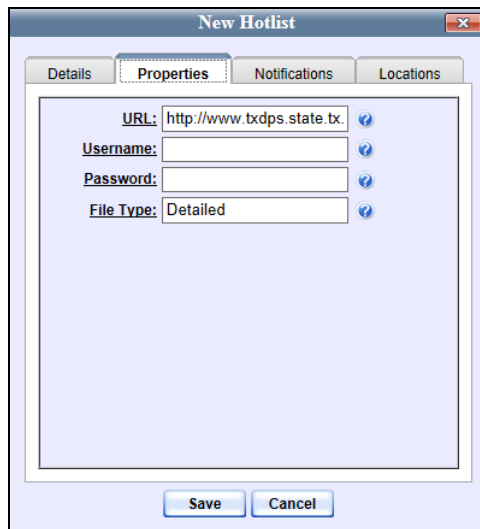**5** Click **Save**. A confirmation message displays.

> The Hotlist named **National BOLOs** successfully saved and is queued for import. When import is complete, a message will be sent to your Inbox.

End of Procedure.

FILE SHARE (PRIVATE)

1 Click the **Properties** tab.

(Continued)

Domain **2** Enter the domain of the user being authenticated, if applicable.

Username **3** Enter the username that the system should use to access this server.

Password **4** Enter the password for the *Username* above.

Server **5** Enter the name or IP address of the server/windows machine.

File Share Path **6** Enter the path to the share file, omitting leading forward slashes (//).

7 If the **Notifications** tab is available, proceed to "Part III: Notifications" on page 126 for further instructions.

– OR –

If the **Notifications** tab is *not* available (i.e., grayed-out), proceed to the next step.

8 If the **Locations** tab is available, proceed to Part IV: Locations on page 128.

– OR –

If the **Locations** tab is *not* available (i.e., grayed-out), proceed to the next step.

9 Click **Save**. A confirmation message displays.

> The Hotlist named **National BOLOs** successfully saved and is queued for import. When import is complete, a message will be sent to your Inbox.

End of Procedure.

TXLETS

1 Click the **Properties** tab.

URL 2 Verify that the URL displayed at the top of this form points to the Texas Department of Public Safety's stolen license plate file.

Username 3 Enter the username for the account that the system should use to access the Texas Department of Public Safety's website.

Password 4 Enter the password for the *Username* above.

File Type **5** To retrieve a *Detailed* file type (default), proceed to the next step.

– OR –

To retrieve a *Standard* file type, enter **Standard** in the *File Type* field.

6 If the **Notifications** tab is available, proceed to "Part III: Notifications" below for further instructions.

– OR –

If the **Notifications** tab is *not* available (i.e., grayed-out), proceed to the next step.

7 If the **Locations** tab is available, proceed to Part IV: Locations on page 128.

– OR –

If the **Locations** tab is *not* available (i.e., grayed-out), proceed to the next step.

8 Click **Save**. A confirmation message displays.

> The Hotlist named **National BOLOs** successfully saved and is queued for import. When import is complete, a message will be sent to your Inbox.

End of Procedure.

**Part III: Notifications**

1 Click the **Notifications** tab. A list of system users displays.
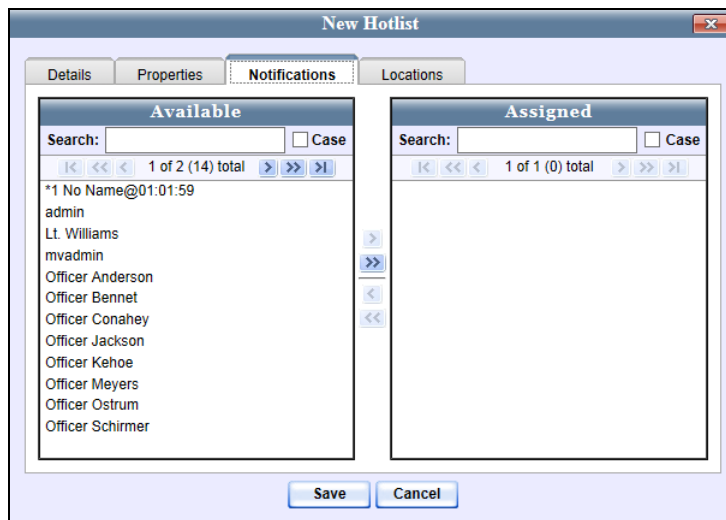
2 Go to the left column (Available) and click on the users you wish to notify whenever an AlertVU unit captures a plate on this hotlist. If the user you're looking for does not appear onscreen, use the navigation arrows at the top of the column to scroll through the user list.

3 Once you've highlighted the desired users, click the ▶ icon located between the two columns. The selected users display in the right column (Assigned).
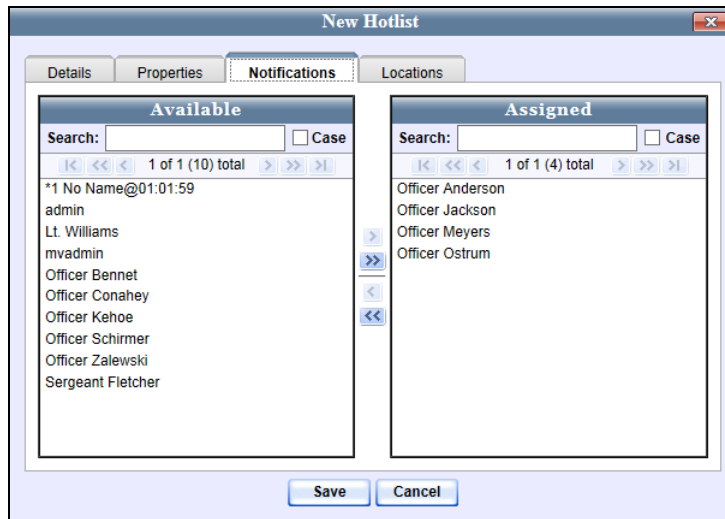
4 If the **Locations** tab is available, skip to "Part IV: Locations" on the next page.

– OR –

If the **Locations** tab is *not* available (i.e., grayed-out), proceed to the next step.

5 Click **Save**. A confirmation message displays.

> The Hotlist named **National BOLOs** successfully saved and is queued for import. When import is complete, a message will be sent to your Inbox.

End of Procedure.

Part IV: Locations

1 Click the **Locations** tab.
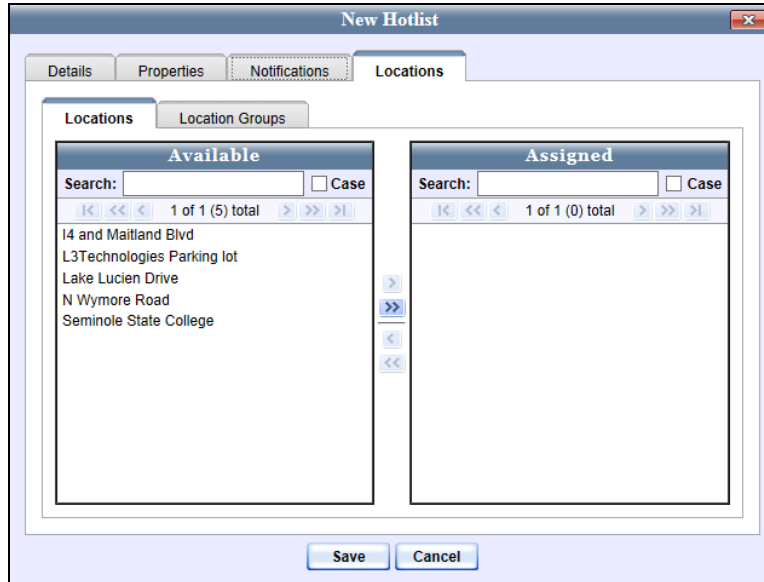
2 To assign one or more *Locations* to this hotlist, proceed to the next step.

– OR –

To assign a *Location Group* to this hotlist, skip to step 6.

3 Go to the *Available* column and click on the Location(s) you wish to assign to this hotlist.

4 Click the ▶ icon located between the two columns. The selected Location(s) display in the *Assigned* column.

L3 Mobile-Vision, Inc.
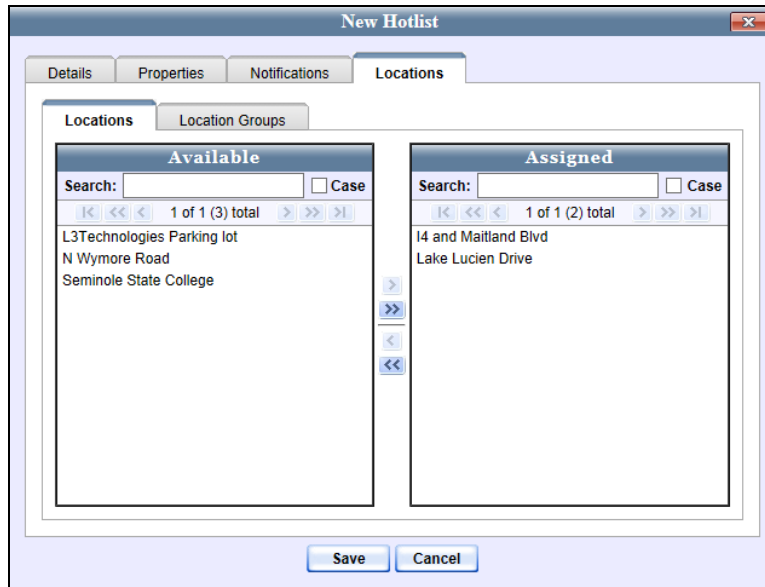
5 If you also wish to add a Location Group to this hotlist, proceed to the next step. Otherwise skip to step 9.

6 Click the **Location Groups** tab.
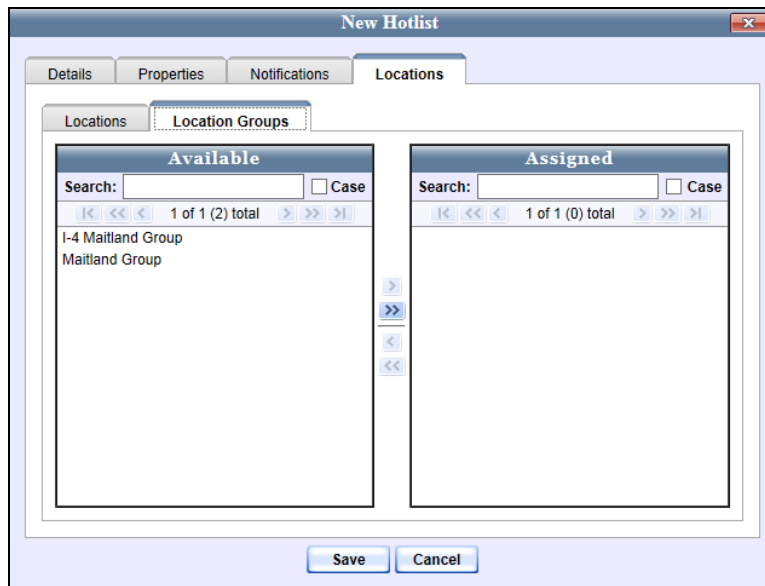
7 Go to the *Available* column and click on the Location Group you wish to assign to this hotlist.

8 Click the ▶ icon located between the two columns. The selected Location Group displays in the *Assigned* column.
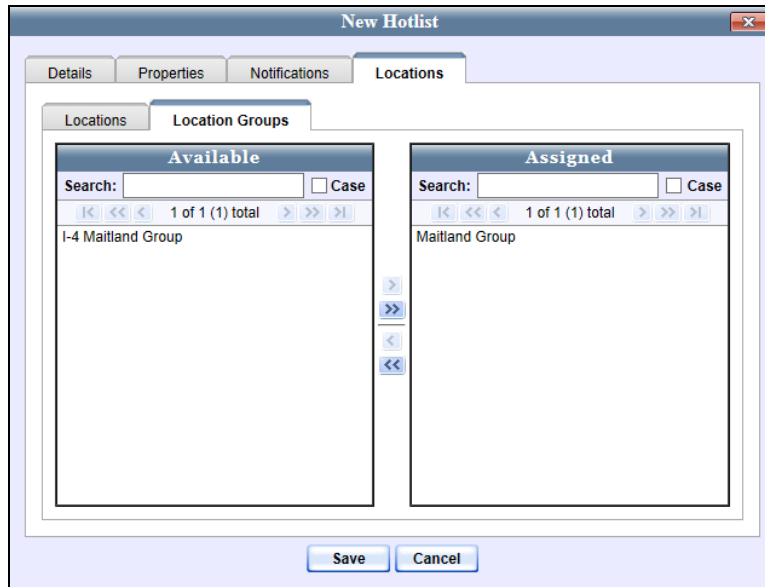
9 Click **Save**. A confirmation message displays.

> The Hotlist named **National BOLOs** successfully saved and is queued for import. When import is complete, a message will be sent to your Inbox.

Promoting a Personal Hotlist to a System Hotlist

This section describes how to create a new system hotlist by converting or "promoting" an existing *personal* hotlist to a *system* hotlist. After you do so, the hotlist can then be pushed out to your AlertVU units.

For a definition of personal vs. system hotlists, see "Creating Hotlists" on page 94.

1 Go to ▼ Home Menu and click **Personal Hotlists**. The Personal Hotlists page displays.
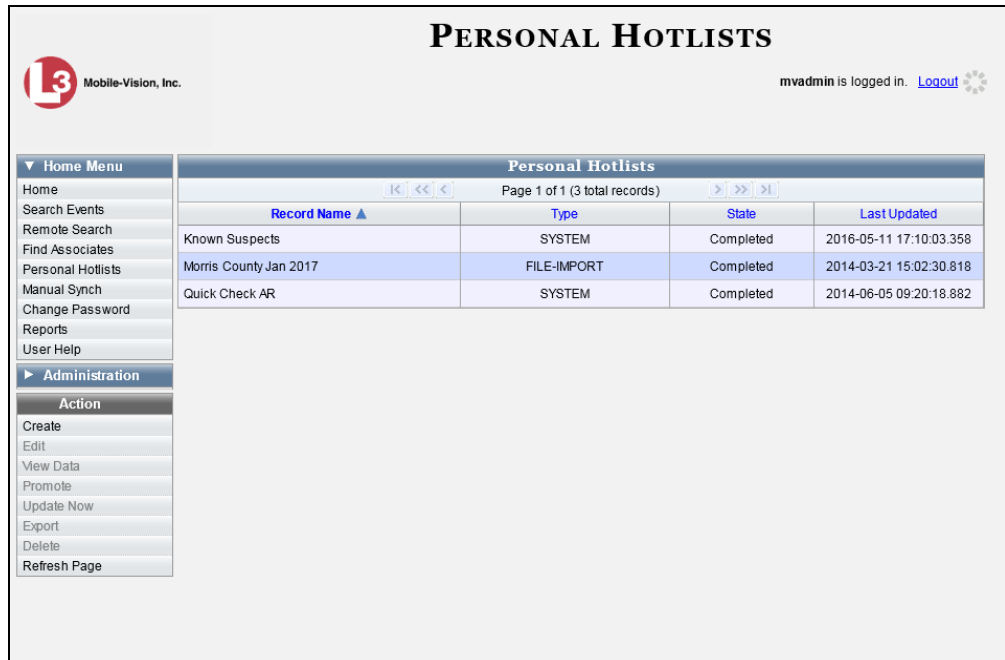
2 Click on the hotlist you wish to promote.

3 Go to the Action column and click **Promote**. The Promote Hotlist popup displays.

4 To change the hotlist's name, enter a new value in the *Name* field. Otherwise proceed to the next step.

5 To set this alert's severity level to **Medium** (default), proceed to the next step.

– OR –

To assign a different severity level to this hotlist, select a new value from the *Severity* drop-down list.

6 Click **Save**. A confirmation message displays.

The hotlist named Morris County Jan 2017 successfully saved.

Note that the word "**Promoting…**" displays in the *State* column. When the promotion process is complete, the value of this field will change to **Completed**.

Creating a Quick Alert Hotlist

This section describes how to create a one plate "Amber Alert" style hotlist which you can immediately transmit to all your AlertVU units.

1 Go to ▼ Administration and click **System Hotlists**. The System Hotlists page displays.

The components on this page are described in the table on page 101.

2   Go to the Action column and click **Quick Alert**. The New Quick Alert popup displays.

3   Enter a name for the Quick Alert in the *Record Name* field.

4   Enter the full license plate number in the *Tag* field.

5   Enter a brief description of this Quick Alert in the *Description* field (e.g., *Amber Alert*).

6   To set this hotlist's severity level to **Critical** (default), proceed to the next step.

     – OR –

     To assign a lower severity level to this hotlist, select a new value from the *Severity* drop-down list.

7   If you want this alert to remain in effect for two days (default), proceed to the next step.

     – OR –

     If you want this alert to remain in effect for more than or fewer than two days, go to the *Expiration* field and enter a number between 1 and 999.

8   If you want the system to automatically push an update out to all AlertVU units whenever a change is made to this hotlist (default), proceed to the next step.

     – OR –

     If you do *not* want the system to automatically push an update out to all AlertVU units whenever a change is made to this hotlist, deselect the *Update Units* checkbox.

9   If you want the system to send an alert to selected users whenever an AlertVU unit captures this license plate, proceed to the next step.

     – OR –

     If you do *not* want the system to send an alert to any users whenever an AlertVU unit captures this license plate, skip to step 14.

10   Select the *Notifications* checkbox.

11   Click the **Notifications** tab. A list of system users displays.
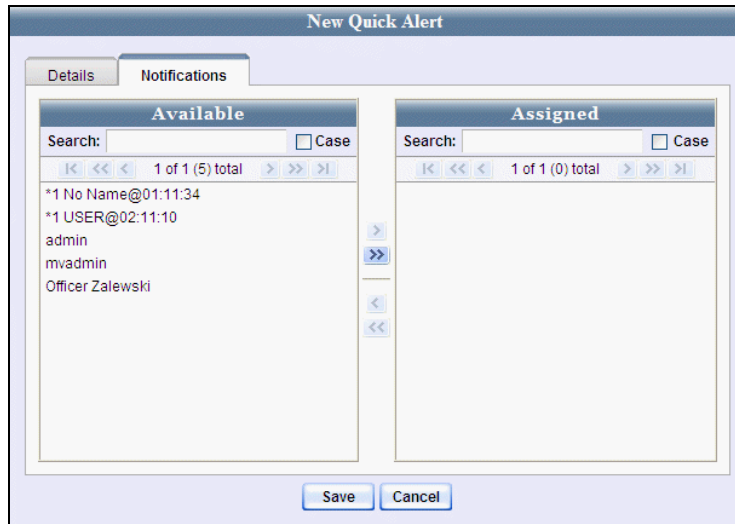
L3 Mobile-Vision, Inc.

New Quick Alert

Details   Notifications

Available

Search: ☐ Case

|◄ ◄◄ ◄   1 of 1 (5) total   ► ►► ►|

*1 No Name@01:11:34
*1 USER@02:11:10
admin
mvadmin
Officer Zalewski

Assigned

Search: ☐ Case

|◄ ◄◄ ◄   1 of 1 (0) total   ► ►► ►|

Save   Cancel

12 Go to the left column (Available) and click on the users you wish to notify whenever an AlertVU unit captures this Quick Alert plate. If the user you're looking for does not appear onscreen, use the navigation arrows at the top of the column to scroll through the user list.

|◄ ◄◄ ◄   ► ►► ►|

13 Once you've highlighted the desired users, click the ► icon located between the two columns. The selected users display in the right column (Assigned).

14 Click **Save**. A confirmation message displays.

> **The Hotlist named Amber Alert successfully saved.**

Note that the *Type* designation for the new hotlist is **QUICK**, indicating that it is a Quick Alert.

Creating a Derivative Hotlist

This section describes how to create a derivation hotlist, which is a subset of a larger hotlist.

1 Go to ▼ Administration and click **System Hotlists**. The System Hotlists page displays.

(Continued)

2 Go to the Action column and click **Create**. The New Hotlist popup displays.

3 Select **Create Derivative Hotlist**.

4 Click **OK**. The New Derivative Hotlist popup displays.

L3 Mobile-Vision, Inc.

The fields on this popup are described below.

| New Derivative Hotlist	
Field	**Description**
Name	The name of the derivative hotlist.
Type	The type of hotlist: DERIVATIVE. *System-generated field*.
Status	The current status of this hotlist: ▪ *Enabled*. This hotlist is *active*. It can receive automatic updates from the server, generate alerts for incoming hits, and appear on mobile units' list of active hotlists. ▪ *Disabled*. This hotlist is *inactive*. It *cannot* receive automatic updates from the server, generate alerts for incoming hits, or appear on mobile units' list of active hotlists.
GeoHotlist	A checklist that enables you to limit this hotlist to a certain geographic region, such as a school zone. If you select this option, you will have an opportunity to add a predefined *Location* or *Location Group* to the Hotlist. For more information on this topic, see "Maintaining Locations" on page 192. ☑ Limit this hotlist to a specified geographic region ☐ Do *not* Limit this hotlist to a specified geographic region If you select this checkbox, you are required to enter an associated time range (see *Start Time* and *End Time* fields).
Start Time	The beginning of the daily time range in which the Location parameter will be active for this hotlist. For example, if your Location is a school zone, you might specify a *Start Time* of 8:00 a.m. *Select a value from the drop-down lists provided.*

(Continued)

New Derivative Hotlist (cont'd)	
Field	**Description**
End Time	The end of the daily time range in which the Location parameter will be active for this hotlist. For example, if your Location is a school zone, you might specify an *End Time* of 3:30 p.m. *Select a value from the drop-down lists provided.*
Severity	The importance of this hotlist: *critical*, *high*, *medium* (default), or *low*.
Update Units	A checkbox used to indicate whether or not you want the system to automatically push an update out to all AlertVU units whenever a change is made to this hotlist. ☑ Automatically notify all AlertVU units whenever this hotlist changes. ☐ Do *not* automatically notify all AlertVU units whenever this hotlist changes.
Notify Users	A checkbox used to indicate whether or not you want the system to send an alert to all users on the hotlist's *Notifications* list whenever an AlertVU unit captures a license plate that's on this hotlist. ☑ Send an alert to all users on the hotlist's *Notifications* list whenever any AlertVU unit receives a hit on this hotlist. ☐ Do *not* send an alert to all users on the hotlist's *Notifications* list whenever any AlertVU unit receives a hit on this hotlist.
Derived From	The existing hotlist you wish to use to create the new hotlist, also referred to as the *source* hotlist. *Select a value from the drop-down lists provided.*

5 Enter a name for the new hotlist in the *Name* field.

6 To limit this hotlist to a certain geographic region, such as a school zone, proceed to the next step. Otherwise skip to step 10.

7 Select the *GeoHotlist* checkbox.

L3 Mobile-Vision, Inc.

New Derivative Hotlist

Details | Filters | Notifications | Locations

Name: NJSP BOLO
Type: DERIVATIVE
Status: Enabled
GeoHotlist: ☑
Start Time: 12 : 00 AM
End Time: 12 : 00 AM
Severity: Medium
Update Units: ☐
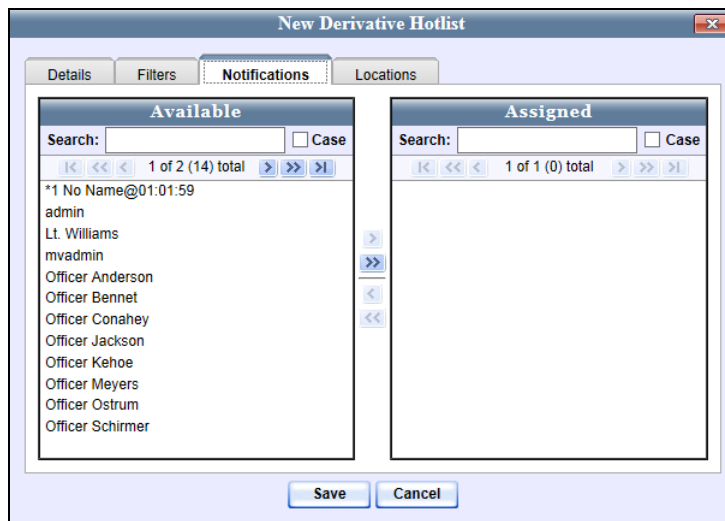Notify Users: ☐
Derived From: manualList

Save   Cancel
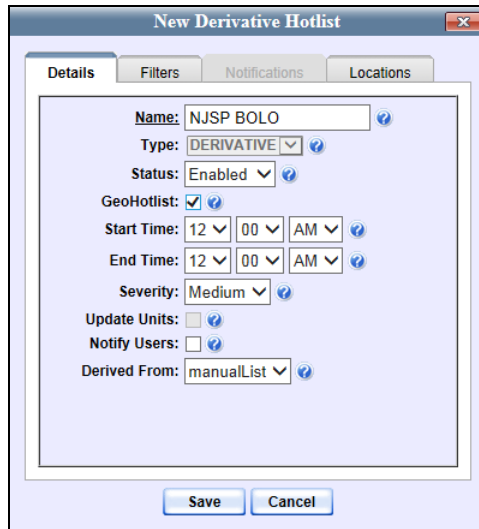
8   Using the *Start Time* drop-down lists, enter the beginning of the daily time range in which the Location parameter will be active for this hotlist. For example, if your Location is a school zone, you might specify a *Start Time* of 8:00 a.m.

9   Using the *End Time* drop-down lists, enter the end of the daily time range in which the Location parameter will be active for this hotlist. For example, if your Location is a school zone, you might specify an *End Time* of 3:30 p.m.

10   To set this alert's severity level to **Medium** (default), proceed to the next step.

– OR –

To assign a different severity level to this hotlist, select a new value from the *Severity* drop-down list.

11   If you want the system to automatically push an update out to all AlertVU units whenever a change is made to this hotlist, select the *Update Units* checkbox. Otherwise proceed to the next step.

12   If you want the system to send an alert to selected users whenever any AlertVU unit captures a license plate that's on this hotlist, proceed to the next step.

– OR –

If you do *not* want the system to send alerts to any users, skip to step 17.

13   Select the *Notify Users* checkbox.

(Continued)
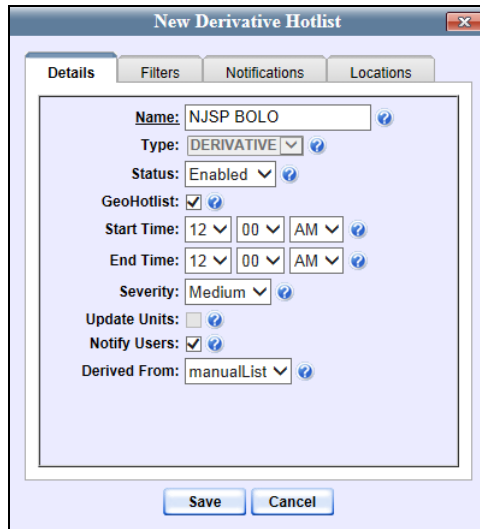
14 Click the **Notifications** tab. A list of system users displays.

15 Go to the left column (Available) and click on the users you wish to notify whenever an AlertVU unit captures a plate on this hotlist. If the user you're looking for does not appear onscreen, use the navigation arrows at the top of the column to scroll through the user list.
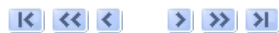
16 Once you've highlighted the desired users, click the ⟩ icon located between the two columns. The selected users display in the right column (Assigned) then click on the "Details" tab.

New Derivative Hotlist — Notifications tab
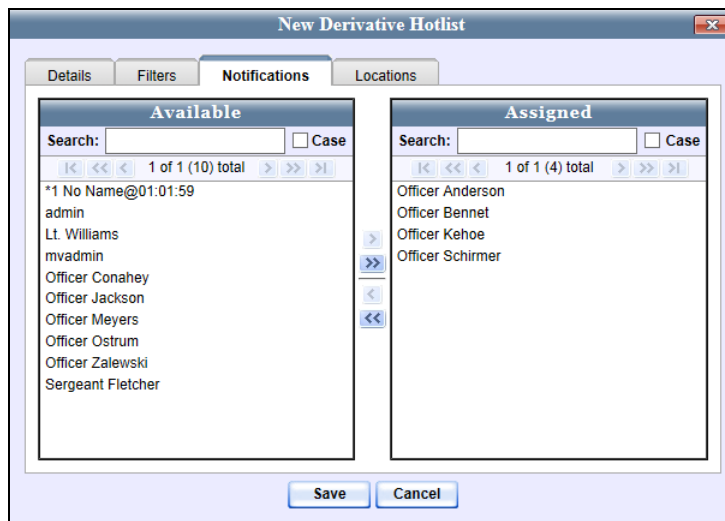
17 Select a hotlist from the *Derived From* drop-down list.

18 Click the **Filters** tab.

New Derivative Hotlist — Filters tab
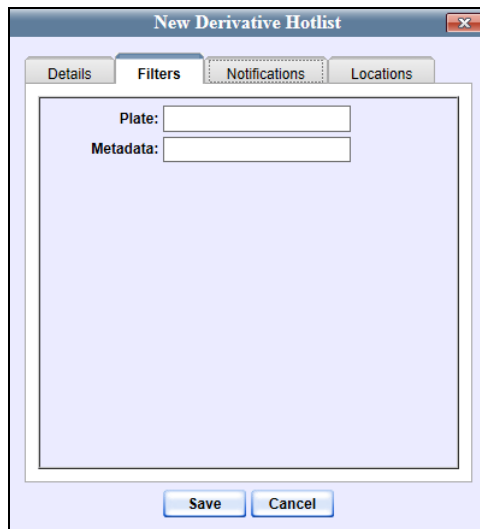
The current column headers for the source hotlist display.

19 Using the blank fields provided, enter the value(s) you wish to include in the new hotlist. To enter multiple values in one field, separate each value with a comma (no spaces). For example, if the source hotlist is a national BOLO and you want the new derivative hotlist to include NJ and NY plates only, enter **NJ,NY** in the *Plate* field.

20 If the **Locations** tab is available, proceed to the next step.

– OR –

If the **Locations** tab is *not* available (i.e., grayed-out), skip to step 29.

21 Click the **Locations** tab.
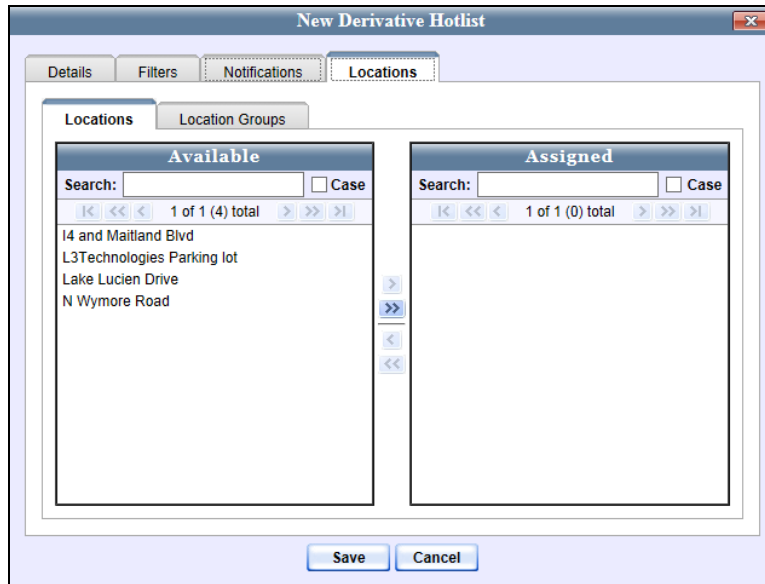
22 To assign one or more *Locations* to this hotlist, proceed to the next step.

– OR –

To assign a *Location Group* to this hotlist, skip to step 26.

23 Go to the *Available* column and click on the Location(s) you wish to assign to this hotlist.

24 Click the ⊳ icon located between the two columns. The selected Location(s) display in the *Assigned* column.
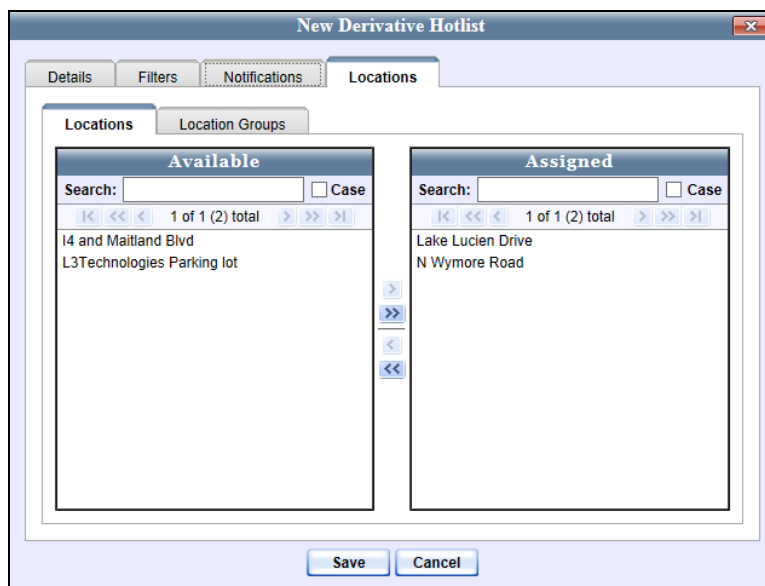
25 If you also wish to add a Location Group to this hotlist, proceed to the next step. Otherwise skip to step 29.

26 Click the **Location Groups** tab.
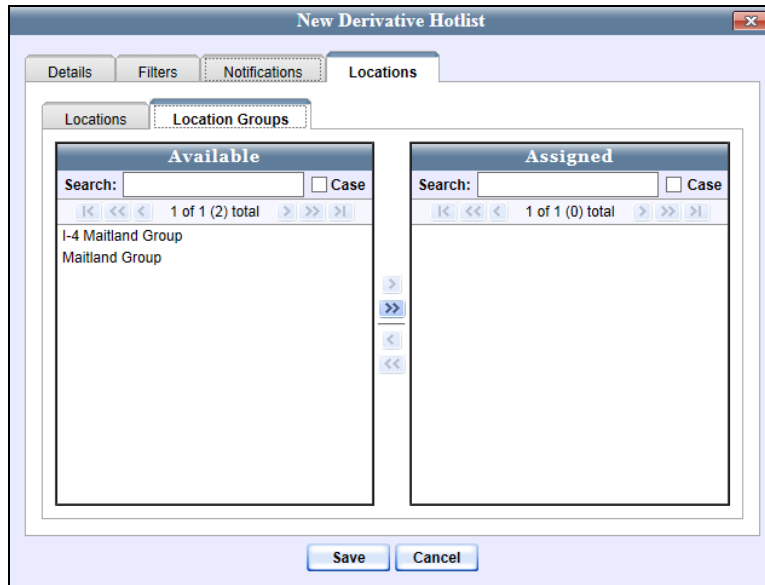
27 Go to the *Available* column and click on the Location Group you wish to assign to this hotlist.

28 Click the ▶ icon located between the two columns. The selected Location Group displays in the *Assigned* column.
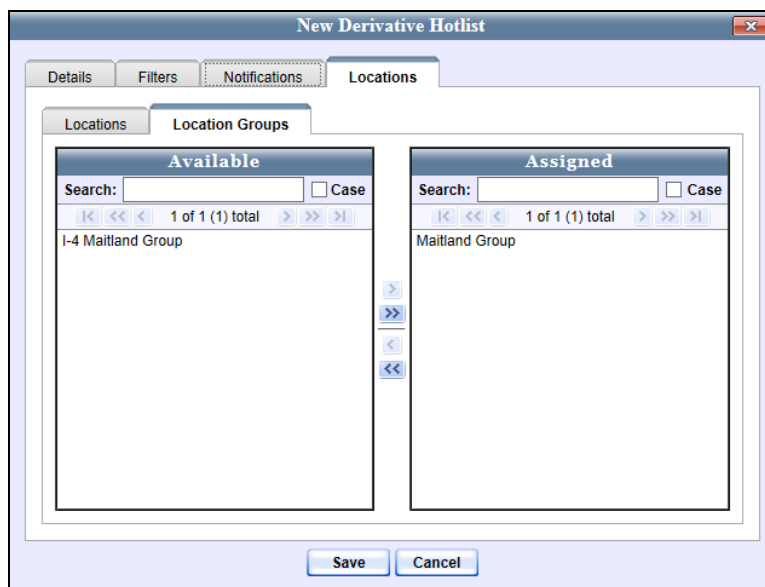
29 Click **Save**. A confirmation message displays.

> **The Hotlist named NJ BOLOs successfully saved and is queued for import. When import is complete, a message will be sent to your Inbox.**

Maintaining Hotlists

This section describes how to update and maintain your personal and system hotlists. For specific instructions, see:

❒ Adding Events to an Existing Hotlist, below
❒ Adding Users to a System Hotlist's Notifications List, page 145
❒ Manually Reimporting a Hotlist, page 148
❒ Changing the Attributes of a Personal Hotlist, page 150
❒ Changing the Attributes of a System Hotlist, page 151
❒ Copying the Most Up-to-Date Hotlists to Your AlertVU Units, page 153.

Adding Events to an Existing Hotlist

This section describes how to add selected event records to an existing personal or system hotlist. The events can reside on either a local server or selected remote server(s).

1 Search for the events you wish to add to an existing hotlist. (If necessary, review "Searching for Events" in chapter 2.)

2 Select the events you wish to incorporate into the existing hotlist:

To select *all* events on your search results list, click the **Index View** tab, then click the **Select All** button at the top of the page.

– OR –

To select *some* events on your search results list, click on the appropriate event(s) to highlight them. If necessary, use the navigation arrows at the top of the page to scroll through the full list.

3 Once the desired event records are selected, go to the Action column and click **Add to Hotlist**. The Add to Hotlist popup displays.

4 Select a hotlist from the *Hotlist* drop-down list.

5 Click **Save**. A confirmation message displays.

> **Hotlist Morris County** **successfully updated. 4 plates added.**

Adding Users to a System Hotlist's Notifications List

This section describes how to add user(s) to a system hotlist's *Notifications* list. Users on the *Notifications* list will receive an Inbox, email, or real-time "popup" alert whenever an AlertVU unit captures a plate that's on the system hotlist.

For more information on alerts and how they are used in the system, see "Alerts" on page 90.

1 Go to ▼ Administration and click **System Hotlists**. The System Hotlists page displays.

(Continued)

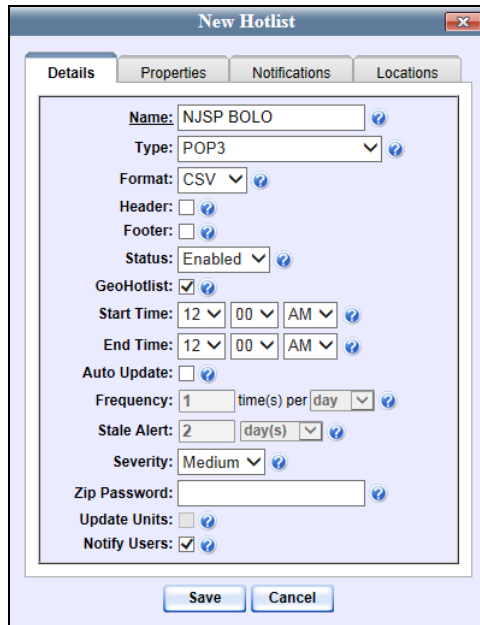The components on this page are described in the table on page 101.

2 Click on the hotlist you wish to update.

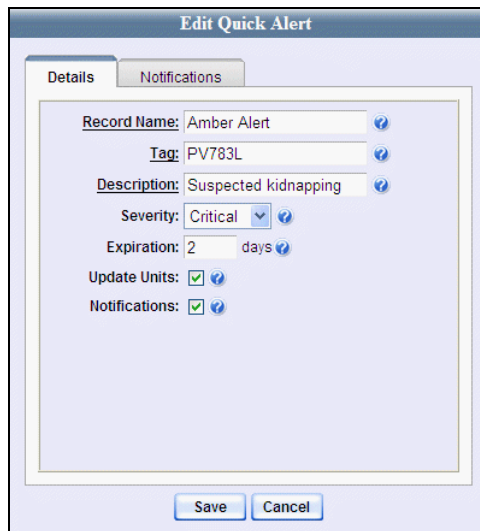**3** Go to the Action column and click **Edit**.

– OR –

Right-click on the record and select **Edit** from the popup menu.

The Hotlist Properties popup displays. This screen may appear slightly different depending on whether this is a *regular* system hotlist or a *Quick Alert* system hotlist.

**Regular
System Hotlist**

**Quick Alert
System Hotlist**

4   Click the **Notifications** tab. A list of system users displays.

   NOTE: If the *Notifications* tab is unavailable (i.e., "grayed-out"), it indicates that the proper checkbox is not selected. Go to the bottom of the form and select either *Notify Users* (regular system hotlist) or *Notifications* (Quick Alert system hotlist).

(Continued)
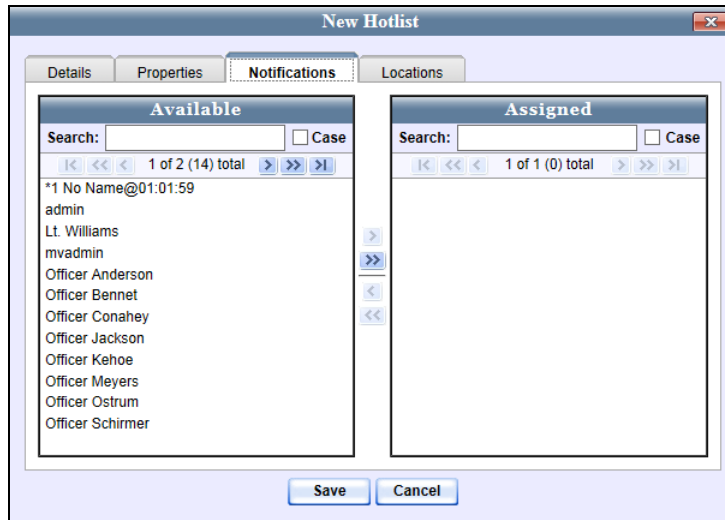
5   Go to the left column (Available) and click on the users you wish to add. If the user you're looking for does not appear onscreen, use the navigation arrows at the top of the column to scroll through the user list.
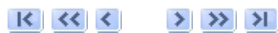
6   Once you've highlighted the desired user(s), click the ⟩ icon located between the two columns. The selected users display in the right column (Assigned).

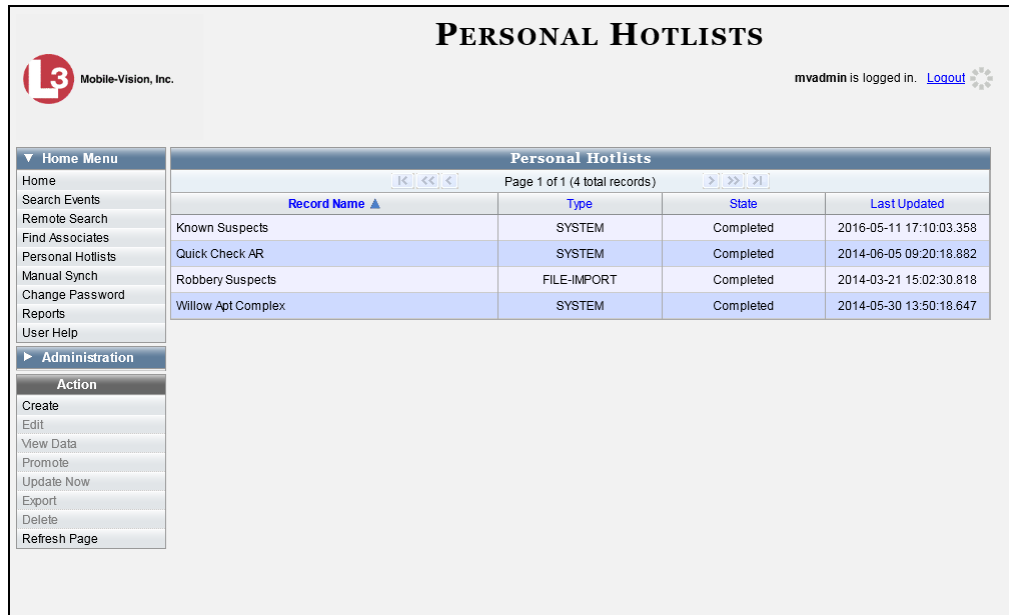7   Click **Save**. A confirmation message displays.

The Hotlist named National BOLO successfully saved.

Manually Reimporting a Hotlist

This section describes how to manually reimport a personal or system hotlist that you previously created using one of the manual import procedures. For more information on these procedures, see "Manually Importing a Personal Hotlist" on page 95 and/or "Manually Importing a System Hotlist" on page 100.

1   To reimport a *personal* hotlist, go to ▼ Home Menu and click **Personal Hotlists**. The Personal Hotlists page displays, as pictured on the next page.
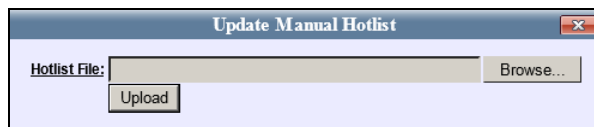
    – OR –

    To reimport a *system* hotlist, go to ▼ Administration and click **System Hotlists**. The System Hotlists page displays (not pictured).

2 Click on the hotlist you wish to reimport. All files that were previously imported will have a *Type* value of **FILE-IMPORT**.

3 Go to the [Action] column and click **Update Now**. The Update Manual Hotlist popup displays.

4 Click the **Browse** button. The Choose File to Upload popup displays.

5 Navigate to the disk drive location where the import file resides.

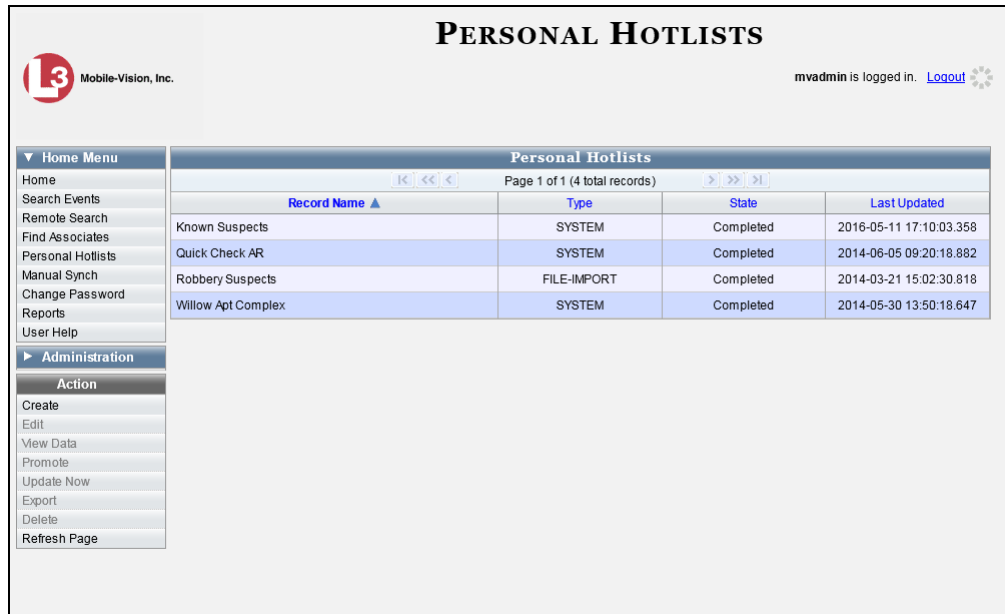**6** Double-click on the import file. The selected file name displays in the *Hotlist File* field.
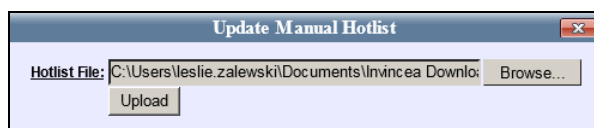
7 Click **Upload**. The system begins reimporting the selected file. While the update is in progress, the word **Updating** will display in the *State* column. When the update is complete, the word **Completed** will display.

Changing the Attributes of a Personal Hotlist

This section describes how to change the *name* or *notification status* of one of your personal hotlists.

1 Go to ▼ Home Menu and click **Personal Hotlists**. The Personal Hotlists page displays.

The columns on this page are described in the table on page 95.

2 Click on the hotlist you wish to update.

3 Go to the Action column and click **Edit**.

– OR –

Right-click on the record and select **Edit** from the popup menu.

The Hotlist Properties popup displays.

4 To change the hotlist's *name*, enter a new value in the *Name* field. Otherwise proceed to the next step.

5 To change the hotlist's *notification status*, proceed to the next step. Otherwise skip to step 7.

6 If you wish to receive a system alert whenever any AlertVU unit captures an event that matches a license plate on this hotlist, select the *Notify Me* checkbox.

– OR –

If you do *not* wish to receive any system alerts for this hotlist, deselect the *Notify Me* checkbox.

7 Click **Save**. A confirmation message displays.

> The Hotlist Morris County Jan 2017 successfully saved.

Changing the Attributes of a System Hotlist

This section describes how to change the general attributes of a system hotlist (i.e., name, type, format, status, etc.) If you're only interested in updating a hotlist's *Notifications* list, see "Adding Users to a System Hotlist's Notifications List" on page 145 instead.

1 Go to **▼ Administration** and click **System Hotlists**. The System Hotlists page displays.

SYSTEM HOTLISTS

mvadmin is logged in. Logout

▼ Home Menu
Home
Search Events
Remote Search
Find Associates
Personal Hotlists
Manual Synch
Change Password
Reports
User Help

▼ Administration
System Setup
System Status
Asset Monitoring
System Hotlists
Import Events
Manage Units
Manage Users
Manage User Groups
Manage Locations
Manage Hotlist Formats

Action
Create
Quick Alert
Edit
View Data
View Locations
View Log
Alert Units
Update Now
Export
Delete
Refresh Page

System Hotlists

Page 1 of 1 (8 total records)

Record Name ▲	Type	Status	Frequency	State	Severity	Last Updated
fort_bad_10	FILE-IMPORT	Enabled		Completed	Medium	2016-11-08 11:30:05.009
fort_bad_2	FILE-IMPORT	Enabled		Completed	Medium	2016-11-08 11:30:05.71
Osceola Gang List	FILE-IMPORT	Enabled		Completed	Medium	2016-11-08 11:30:05.971
passwd-test	FTP	Enabled		Completed	Medium	2016-11-08 11:30:06.306
Sample_Mar232015	FILE-IMPORT	Enabled		Completed	Medium	2016-11-08 11:30:06.62
sample_Mar24-blets	FILE-IMPORT	Enabled		Completed	Medium	2016-11-08 11:30:07.927
Suspended Licenses	SYSTEM	Disabled		Completed	Medium	2015-03-18 11:10:03.711
Willow Apt Complex	SYSTEM	Enabled		Completed	Medium	2017-01-17 10:20:04.674

The components on this page are described in the table on page 101.

2 Click on the hotlist you wish to update.

3 Go to the Action column and click **Edit**.

– OR –

Right-click on the record and select **Edit** from the popup menu.

The Hotlist Properties popup displays. This screen may appear slightly different depending on whether this is a *regular* system hotlist or a *Quick Alert* system hotlist.

Regular
system hotlist

Quick Alert
system hotlist

L3 Mobile-Vision, Inc.

4   Enter/select your changes in the appropriate field(s). For a detailed description of these fields, see page 110.

5   Click **Save**. A confirmation message displays.

> The Hotlist named **NJ & FL BOLO** successfully saved.

Copying the Most Up-to-Date Hotlists to Your AlertVU Units

This section describes how to manually push all system hotlists out to all AlertVU units. When you do so, any unit that is missing a particular hotlist or has an outdated version of a hotlist will receive the appropriate update(s).

NOTE: When a hotlist's *Update Units* checkbox is selected, the system will automatically push hotlist updates out to your AlertVU units without any action on your part. You only need to use this manual update procedure when the automatic update feature is not in effect for some or all of your hotlists.

1   Go to **▼ Administration** and click **System Hotlists**. The System Hotlists page displays.

The components on this page are described in the table on page 101.

2   Go to the `Action` column and click **Alert Units**. A confirmation message displays.

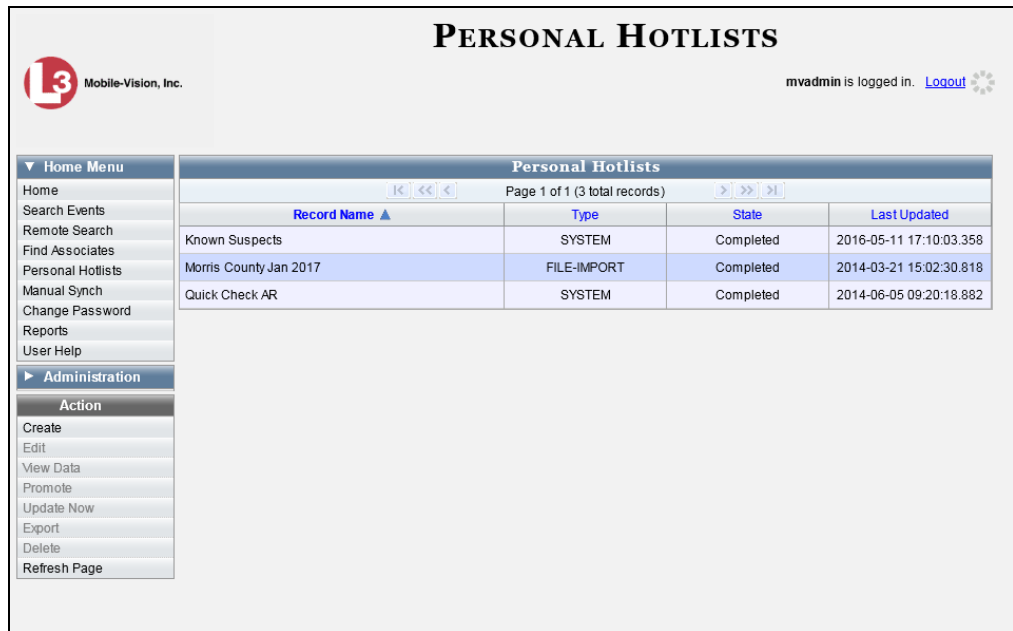> **Successfully alerted all units of the hotlist update.**

Viewing a Hotlist's Plates

This section describes how to view the license plates associated with a *personal* or *system* hotlist.

1   To view the plates for a *personal* hotlist, go to `▼ Home Menu` and click **Personal Hotlists**. The Personal Hotlists page displays, as pictured below.

– OR –

To view the plates for a *system* hotlist, go to `▼ Administration` and click **System Hotlists**. The System Hotlists page displays (not pictured).

2   Click on the hotlist you wish to view.

3   Go to the `Action` column and click **View Data**. The hotlist's license plates display.

4 If necessary, use the navigation arrows at the top of the page to scroll through the full list.

5 When you're finished viewing the plate list, click the ⊗ in the upper right corner of the popup.

Viewing the Locations Attached to a System Hotlist

This section describes how to view the predefined Locations that are currently linked to a System hotlist.

1 Go to ▼ Administration and click **System Hotlists**. The System Hotlists page displays.

2 Click on the hotlist record you wish to view.

3 Go to the Action column and click **View Locations**. The Hotlist Locations popup displays.

4 To view the map associated with a location, click on the icon in the *Map* column.

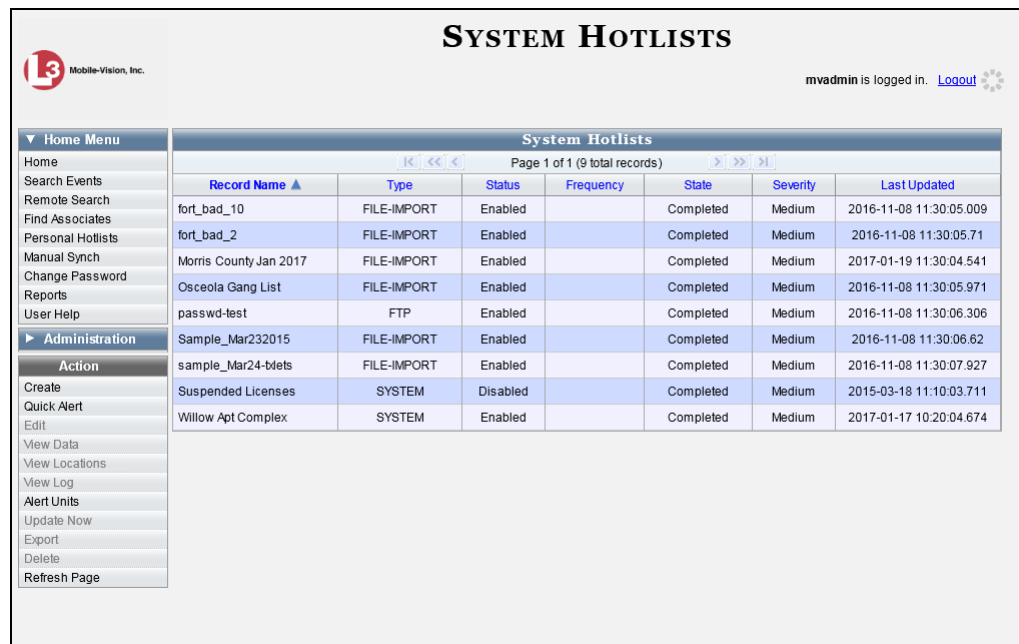**5** To exit, click the ✕ in the upper right corner of the popup(s).

L3 Mobile-Vision, Inc.

Exporting a Hotlist

This section describes how to export a personal or system hotlist to a .csv spreadsheet.

1   To export a *personal* hotlist, go to ▼ Home Menu and click **Personal Hotlists**. The Personal Hotlists page displays (not pictured).

– OR –

To export a *system* hotlist, go to ▼ Administration and click **System Hotlists**. The System Hotlists page displays.
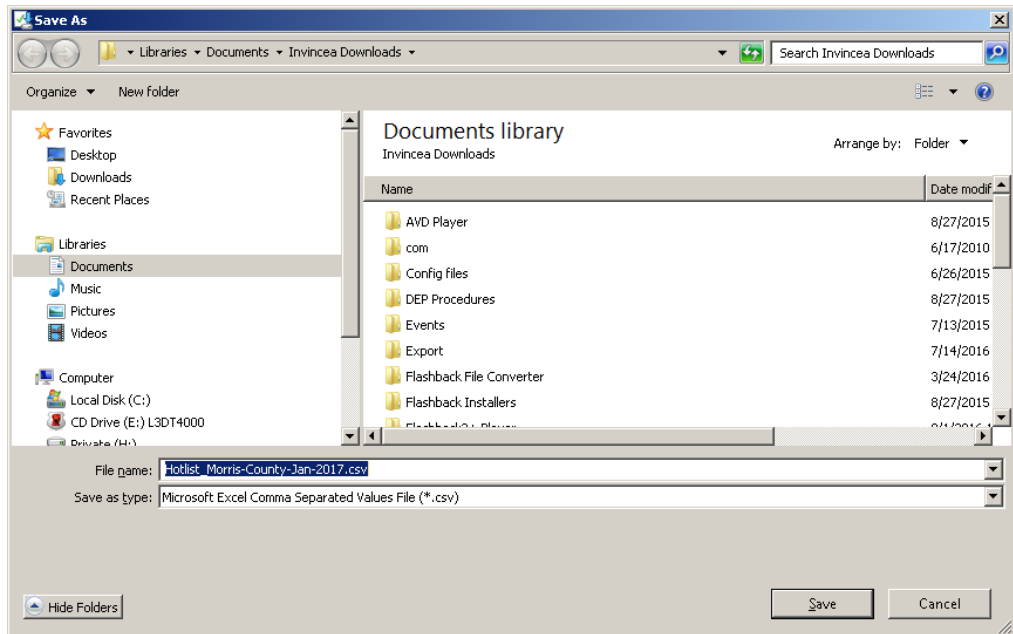

2   Click on the hotlist you wish to export.

3   Go to the Action column and click **Export**. A Windows prompt displays.
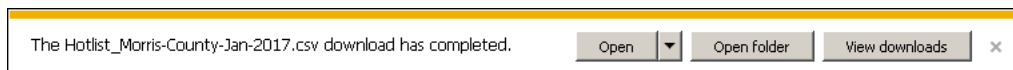

4   Select **Save As** from the *Save* drop-down list. The Save As popup displays.

(Continued)

5 Navigate to the disk drive location where you wish to save the .csv file.

6 Click **Save**. A confirmation message displays.
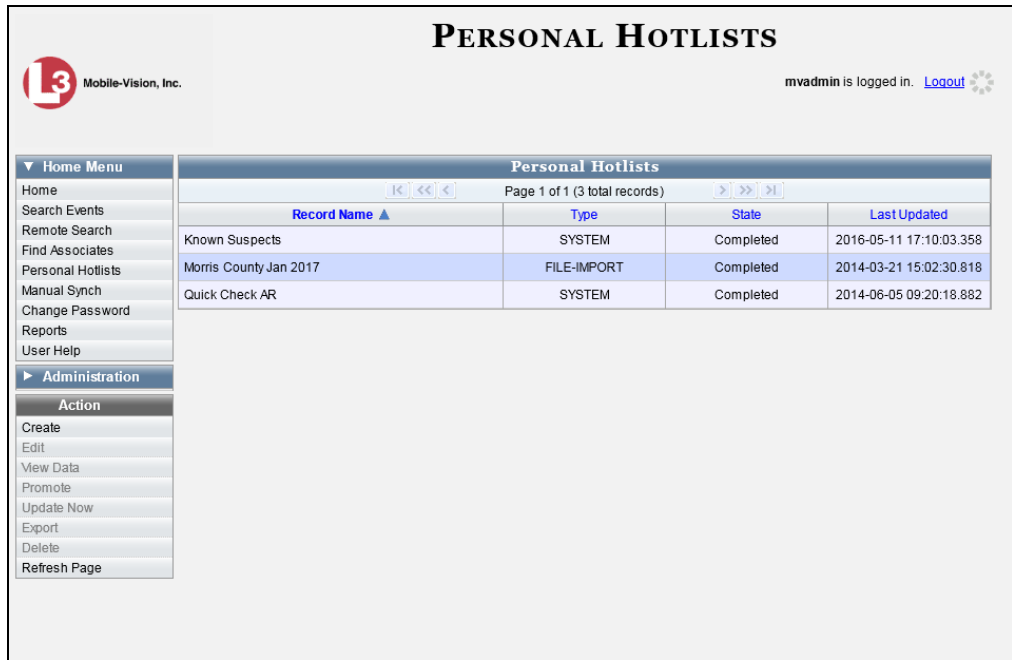

7 To open the spreadsheet right now, click **Open**. Otherwise click ⊠.

Deleting a Hotlist

This section describes how to delete a personal or system hotlist. You can delete any *personal* hotlists that you created. You can delete *system* hotlists if you have the proper permissions to do so. For more on permissions, see chapter 7, Security.

1 To delete a *personal* hotlist, go to ▼ Home Menu and click **Personal Hotlists**. The Personal Hotlists page displays, as pictured on the next page.

– OR –

To delete a *system* hotlist, go to ▼ Administration and click **System Hotlists**. The System Hotlists page displays (not pictured).

2 Click on the hotlist you wish to delete.

3 Go to the Action column and click **Delete**.

– OR –

Right-click on the record and select **Delete** from the popup menu.

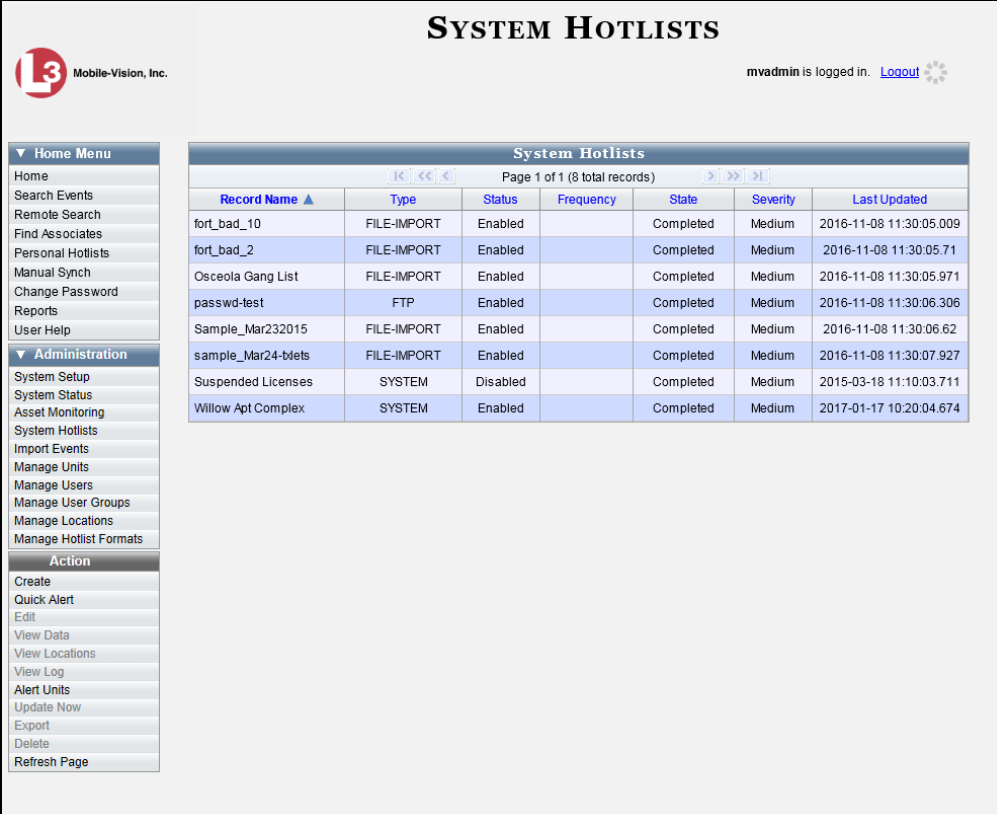A confirmation message displays.

4 Click **Yes**. The selected hotlist is removed from the list.

Enabling/Disabling a Hotlist

This section describes how to enable or disable a system hotlist.

❒ When a hotlist is **Enabled**, it indicates that the hotlist is *active*. It can receive automatic updates from the server, generate alerts for incoming hits, and appear on mobile units' list of active hotlists.

❒ When a hotlist is **Disabled**, it indicates that the hotlist is *inactive*. It *cannot* receive automatic updates from the server, generate alerts for incoming hits, or appear on mobile units' list of active hotlists. A disabled hotlist can, however, be viewed, exported, and/or manually updated.

1 Go to ▼ Administration and click **System Hotlists**. The System Hotlists page displays.
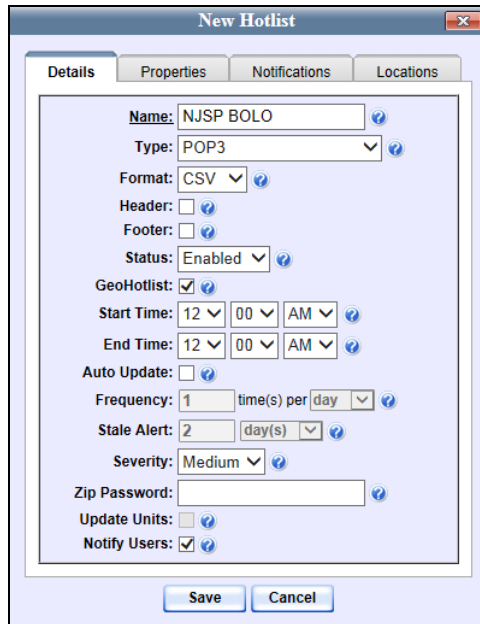

The components on this page are described in the table on page 101.

2 Click on the hotlist you wish to update.

3 Go to the Action column and click **Edit**.

– OR –

Right-click on the record and select **Edit** from the popup menu.

This document consists of general capabilities information that is not defined as controlled technical data under ITAR part 120.10 or EAR

The Hotlist Properties popup displays.

4 Go to the *Status* field and select **Enabled** or **Disabled** from the drop-down list.

5 Click **Save**. A confirmation message displays.

> The Hotlist named Osceola Gang List successfully saved.

Using the Live Alert Facility

This section describes how to use the optional Live Alert facility, which allows you to display real-time alerts whenever an AlertVU unit receives a hit on a license plate that's on a system hotlist for which you have Notification rights. For more on this topic, see "Alerts" on page 90.

For more information, see:

❒ Activating Live Alert, next page
❒ Turning Live Alert Passive Mode On/Off, page 166
❒ Testing Live Alert, page 168.

Activating Live Alert

This section describes how to activate the Live Alert software, also referred to as "Notification Client". Perform this action whenever you login to the AlertVU Back Office application.

For more on Live Alerts, see "Alerts" on page 90.

1 Go to ▼ Home Menu and click **Home**. The Home Page displays.

2 Go to the Action column and click **Launch Client**. A processing message displays, followed by the Login Information popup.
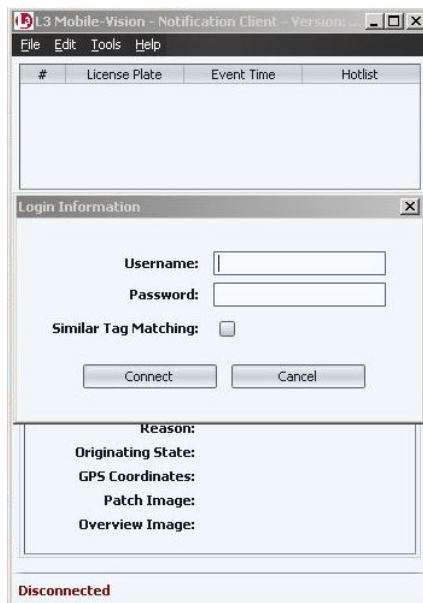
3 Enter your AlertVU Back Office User ID in the *Username* field.

L3 Mobile-Vision, Inc.

4 Enter your AlertVU Back Office password in the *Password* field.

5 If you wish to receive alerts on plate reads that are an exact match to plates on your AlertVU hotlists (default), proceed to the next step.

– OR –

If you wish to receive alerts on plate reads that are either an exact match OR similar but not identical to plates on your AlertVU hotlists, select the *Similar Tag Matching* checkbox.

6 Click **Connect**.

⇒ If the word *Connected* displays in the lower left corner of the popup (see next page), it indicates that the Live Alert Utility is now activated. Skip to step 10.

⇒ If the Authentication Code popup displays (pictured below), it indicates that your agency is using the two-factor authentication feature. This feature requires that you enter an additional code whenever you log into AlertVU Back Office. As soon as you click the **Login** button, the system will automatically generate an Authentication Code and send it to the email address saved in your user record. *Proceed to the next step*.
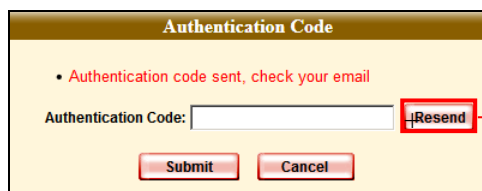
If your Authentication Code expires before you have a chance to click **Submit**, click here to have a new code emailed to you

7 Check your email for a message with the subject line "User Notification." Highlight the Authentication Code contained in this email message, then copy it to your clipboard (**Ctrl + C**).

8 Return to the AlertVU application. Position your cursor in the *Authentication Code* field, then press **Ctrl + V**.

9 Click **Submit**. the word *Connected* displays in the lower left corner of the popup, indicating that the Live Alert Utility is now activated.
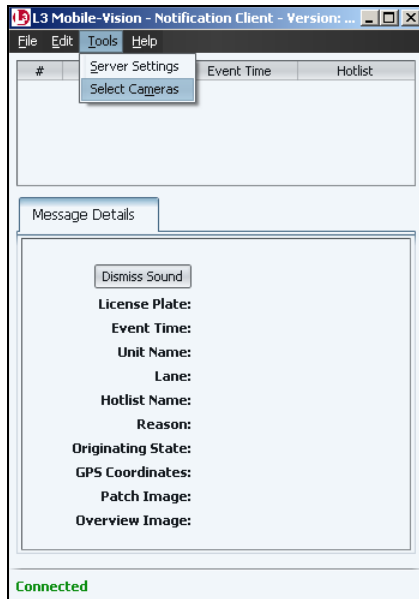
(Continued)
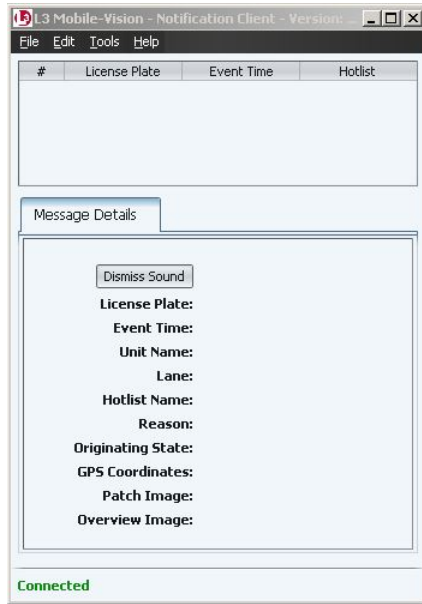
10 If you wish to receive live alerts on hits that come from *all* of your AlertVU cameras (default), skip to step 14.
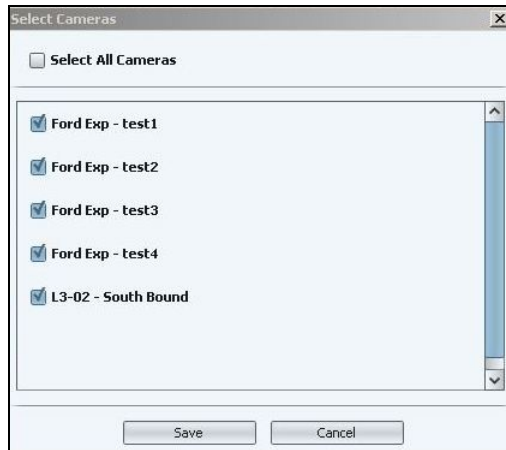
– OR –

If you wish to receive live alerts on hits that come from *some*, but not all, of your AlertVU cameras, proceed to the next step.

11 Select **Tools➜ Select Cameras** from the menubar.

The Select Cameras popup displays.

L3 Mobile-Vision, Inc.

12 Deselect those camera(s) for which you do not wish to receive alerts.

13 Click **Save**.

14 Click the ▣ icon to minimize the popup.

Any time an AlertVU unit receives a hit on a license plate that's 1) on a system hotlist for which you have Notification rights and 2) was captured from a camera on your selection list, the Notification Client popup will automatically display with detailed information on the hit. If audio is activated on your PC, an alarm will sound as well.
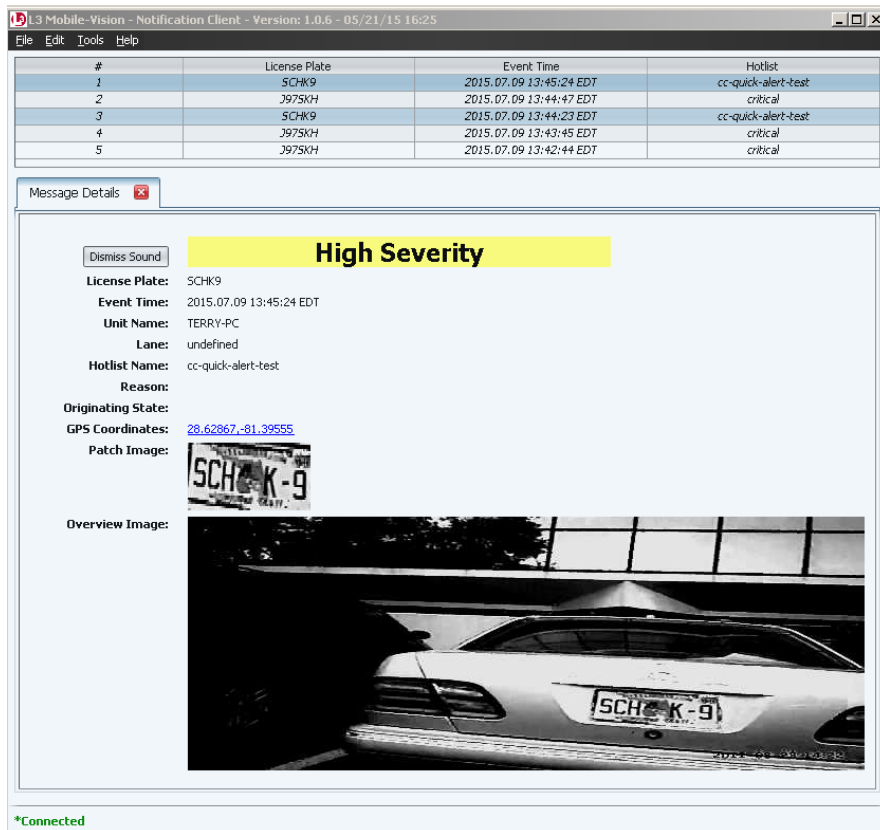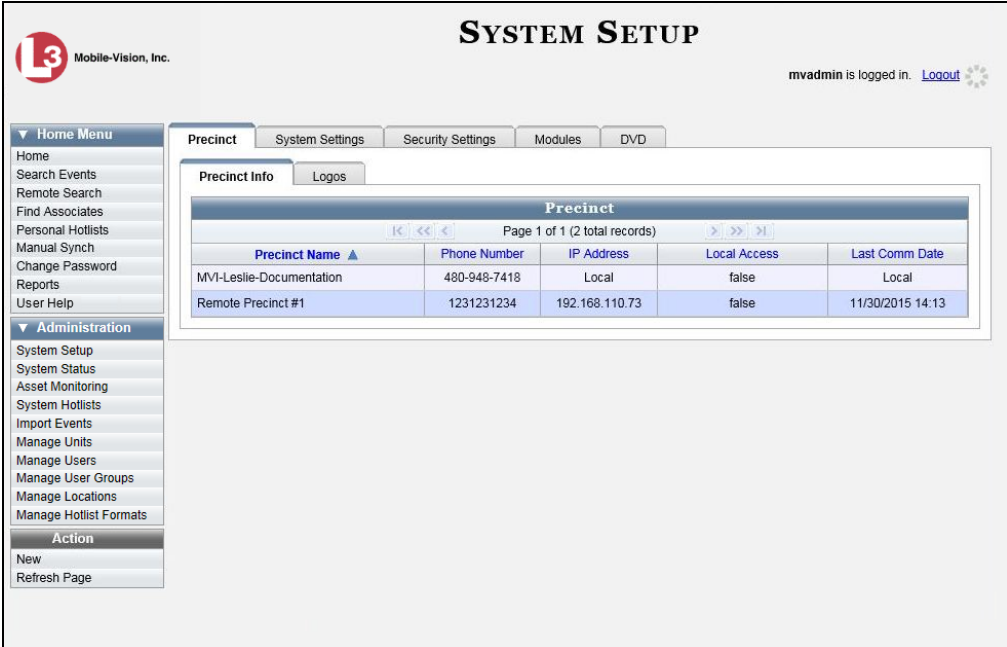
Turning Live Alert Passive Mode On/Off

The Live Alert Passive Mode setting was added to AlertVU in release 3.1.4 to work around firewall issues that can arise when using the Live Alert feature. When *passive mode* is in effect (checkbox selected), it forces Live Alert Client to actively poll the server for live alert messages, thus eliminating the need to change firewall rules. Conversely, when *active mode* is in effect (checkbox deselected), the server pushes messages to Live Alert. The *advantage* of active mode is that it reduces network traffic. The *disadvantage* of active mode is that it may require you to change firewall rules.

The system defaults to *passive mode* (checkbox selected).

Only perform this task when instructed to do so by your agency Network Specialist or an L3 Mobile-Vision Support professional.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 Click the **System Settings** tab.

3 Click the **System Options** tab.

4 Go to the Action column and click **Edit**. The System Options popup displays.

(Continued)

5 To select Live Alert *passive* mode, select the *Enable Live Alert Passive Mode* checkbox.

– OR –

To select Live Alert *active* mode, deselect the *Enable Live Alert Passive Mode* checkbox.

6 Click **Save**.

WARNING: If you selected *active* mode, your agency's Network Specialist will have to reevaluate, and possibly change, your firewall rules.

Testing Live Alert

This section describes how to perform a test of the Live Alert facility. This test will check to make sure that every AlertVU camera that's connected to the server is able to successfully transmit a Live Alert message. When you perform this test, all connected cameras will send a "dummy" Live Alert to all users who are logged into the notification client software. Perform this test when you are unsure if one or more of your AlertVU cameras are transmitting Live Alerts to the server.

HINT: Before you begin a Live Alert test, make a list of all your AlertVU units and associated cameras so that you can check each one off the list as their Live Alert Test popups display. That way you will be able to identify, by process of elimination, which cameras are having communication problems (if any).
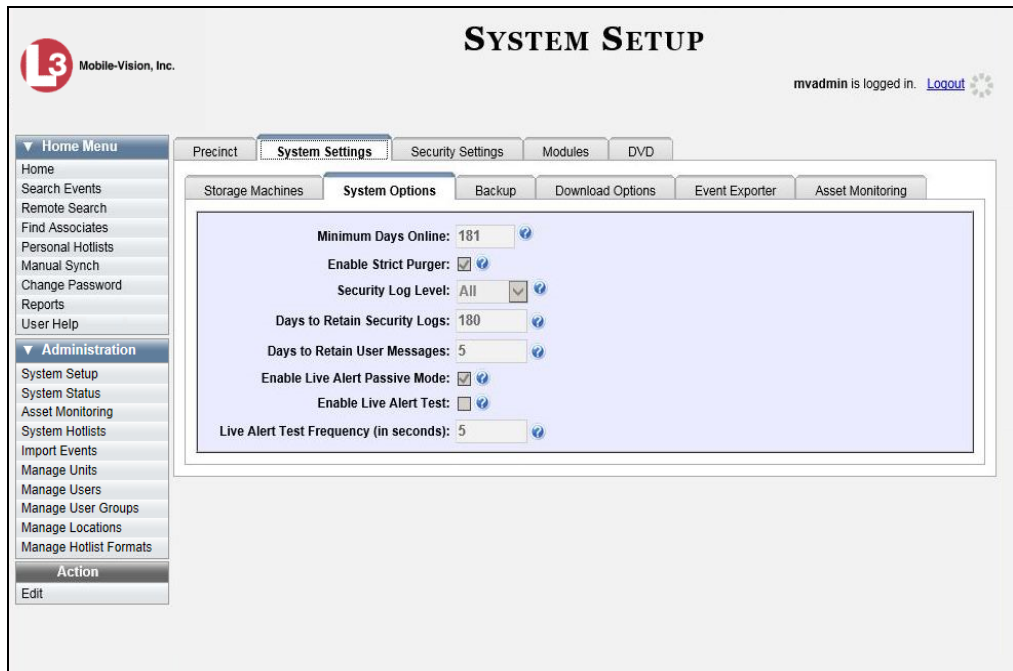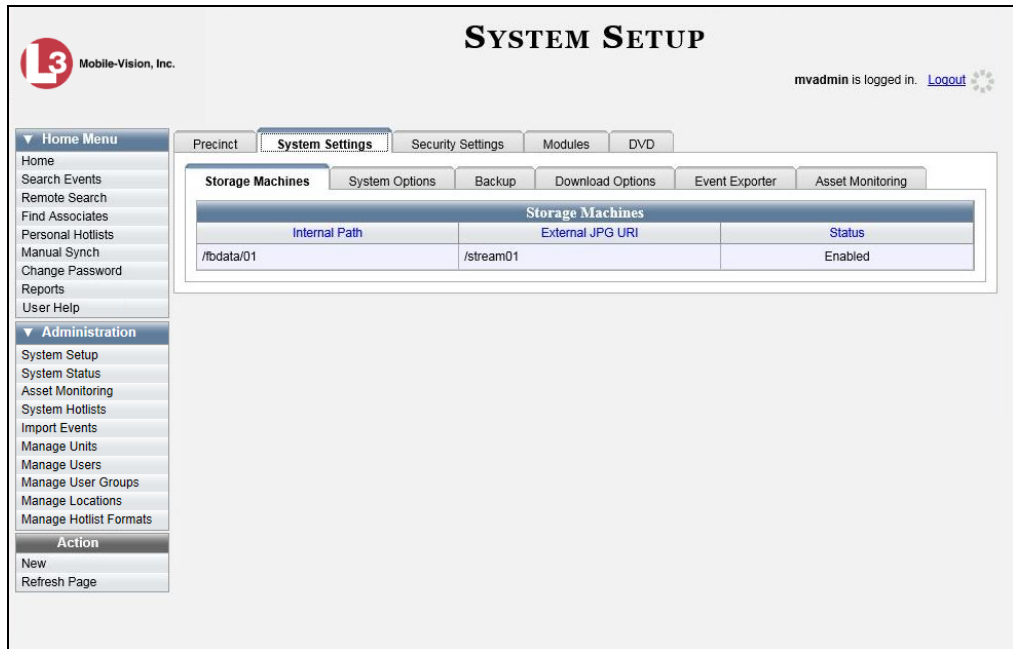
Live Alert Test
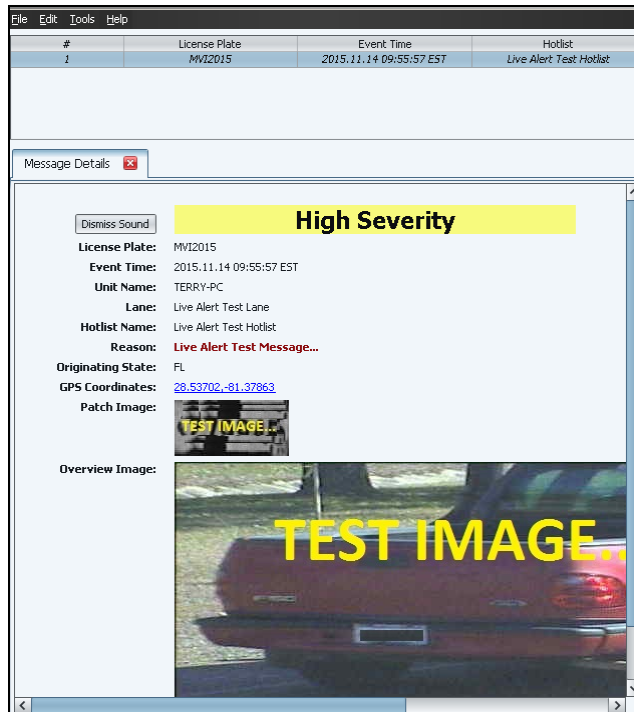
1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.
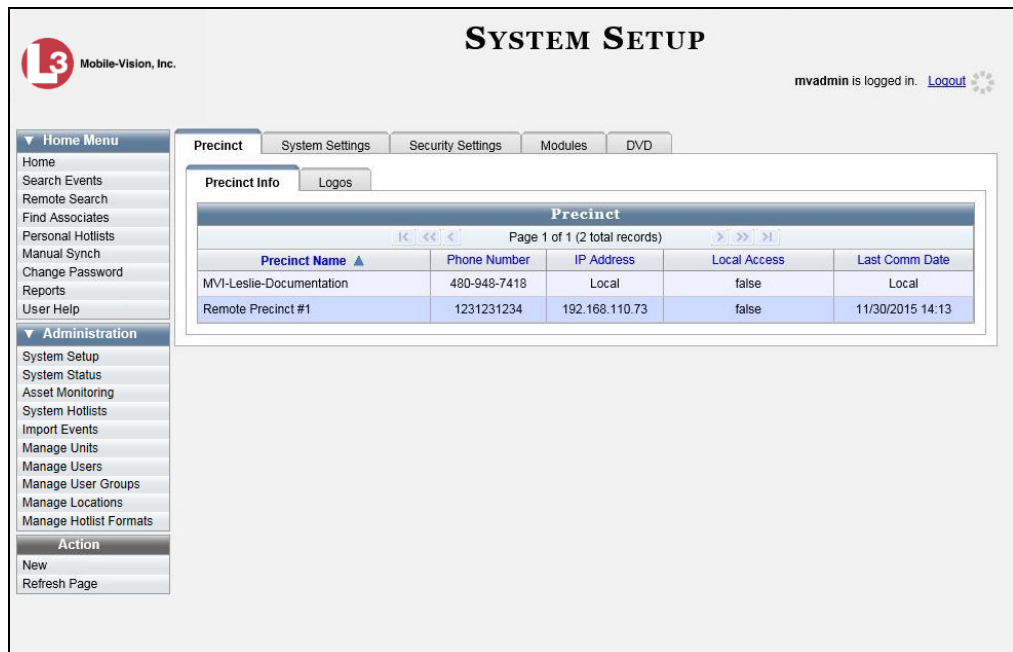
2 Click the **System Settings** tab.

3 Click the **System Options** tab.

4 Go to the Action column and click **Edit**. The System Options popup displays.

5 Select the *Enable Live Alert Test* checkbox.

6 Click **Save**. The cameras will begin sending the Live Alert Test popups. Once the test is complete, proceed to the next step.

7 Go to the Action column and click **Edit**. The System Options popup redisplays.

8 Deselect the *Enable Live Alert Test* checkbox.

9 Click **Save**.

Maintaining Hotlist Formats

Because outside hotlists come from a variety of law enforcement agencies, they also come in many different formats. Each hotlist that you import into AlertVU must have a corresponding *hotlist format* record entered in the system. Hotlist format records contain the information that AlertVU needs to parse, or divide and analyze, the data that's contained in each hotlist type. For example, if the XYZ hotlist consists of five columns and the second column contains the license plate number, the system needs to know that.

In AlertVU, there are two types of hotlist formats: *system-defined* and *custom*, as described below.

❐ **System-defined hotlist formats** are the predefined formats that *cannot be changed*. These include CSV (Comma separated text file) and NCIC (National Crime Information Center).

❐ **Custom hotlist formats** are the *predefined* and *user-defined* formats that can be changed. If you are an existing customer, the *predefined* formats may include:

AR NLETS .... Arkansas National Law Enforcement Telecommunication
CLEW SVS............ California Law Enforcement Web Stolen Vehicle Systems
FCIC .... Florida Crime Information Center System
MD MVA............... Maryland Motor Vehicle Administration
TXLETS .... Texas Law Enforcement Telecommunication System

User-defined custom hotlist formats are created by you, the user. Typically, your System Implementation Specialist (SIS) will assist you with this task at system startup. Thereafter, you only need to add a custom hotlist format when your agency plans to begin importing a new hotlist that does not have a corresponding hotlist format record in AlertVU.

For more information, see:

❐ Adding a Custom Hotlist Format, below
❐ Viewing a Hotlist Format, page 184
❐ Changing a Custom Hotlist Format, page 185
❐ Deleting a Custom Hotlist Format, page 190
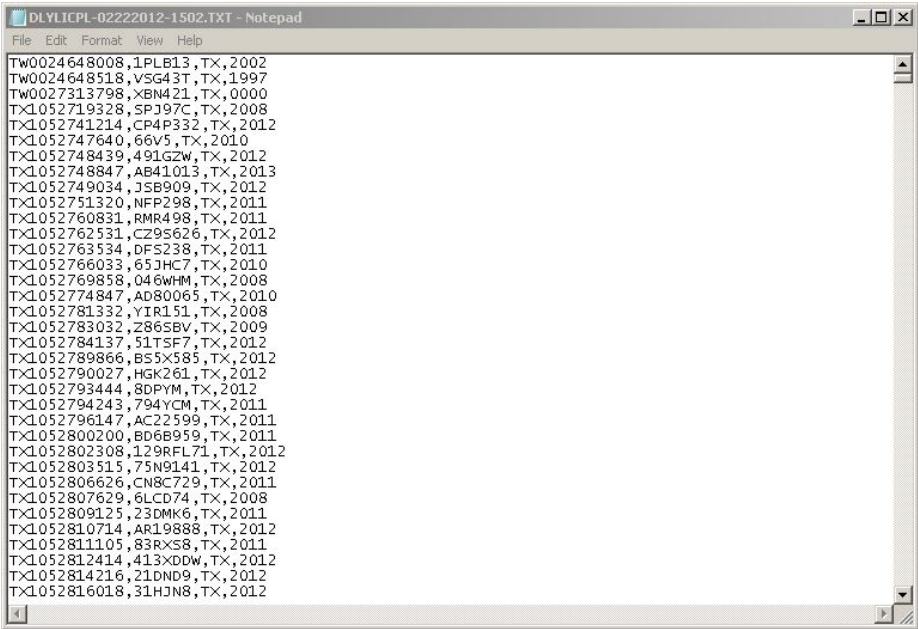
Adding a Custom Hotlist Format

This section describes how to add a new custom hotlist format to AlertVU. For a definition of custom hotlist formats, see the previous section.

There are two custom hotlist formats: *delimited* and *fixed field*. See samples below and on the next page.

Because this procedure is somewhat technical, you may wish to enlist the assistance of an L3 Mobile-Vision Technical Support Engineer to walk you through it.

Figure 1: Sample hotlist in 'delimited' format, which separates each piece of data with a comma, semi-colon, or space

Header ──────→

```
05/27/2011 05:30
VAF      MD SUSPENDED  2002 JEEP   VAF
ATAP2    MD MSP PICKUP 1999 GMC    ATAP2
AXMEN    MD SUSPENDED  2001 HARL   AXMEN
KLUTZ    MD VEIP       2002 ACUR   KLUTZ
ASPEED   MD VEIP       2000 FORD A SPEED
AWAP3    MD VEIP       2003 CHEV A WAP3
AAB85B   MD VEIP       1989 FORD
AAC768   MD VEIP       2003 HOND
AAD020   MD VEIP       1996 CADI
AAE124   MD SUSPENDED  2004 CHEV
AAE88B   MD SUSPENDED  1988 CHEV
AAF22K   MD VEIP       1986 TOYT
AAF42G   MD VEIP       2006 TOYT
AAF97J   MD VEIP       2004 MAZD
AAG17C   MD VEIP       1991 JEEP
AAG92T   MD VEIP       2006 CHRY
AAG974   MD MSP PICKUP 2001 TOYT
AAH82S   MD VEIP       1989 CHEV
AAH95T   MD VEIP       1998 FORD
AAK54G   MD VEIP       2001 FORD
AAL588   MD VEIP       2006 HYUN
AAL824   MD VEIP       2001 TOYT
AAM15S   MD VEIP       1999 CHEV
AAM59W   MD SUSPENDED  2000 FORD
AAM59Z   MD VEIP       1984 CHEV
AANDSZ   MD SUSPENDED  2006 NISS AANDS Z
AAP56L   MD VEIP       1993 CHRY
AAR76C   MD VEIP       2001 CHRY
AAR86J   MD VEIP       2000 DODG
AATAF    MD SUSPENDED  1997 HOND
AAT087   MD SUSPENDED  2009 CHEV
```

Figure 2: Sample hotlist in 'fixed field' format, which lists each data element in a column of a specific width

NOTE: When viewing a hotlist's text file, as in the examples above, it's recommended that you use WordPad rather than Notepad.

Before you begin creating a custom hotlist format, you will need a hotlist containing sample data. The source agency can provide you with this file. Once you obtain the sample hotlist file, open it in WordPad and either print the file or jot down the relevant information required to design your new hotlist format. Specifically, you'll need to be able to answer the following questions:

Hotlist format questions

❐ Does the file have a header?
❐ Is the file in *delimiter* or *fixed field* format? (Review Figure 1 on the previous page and Figure 2 above.)
❐ If the file is in *delimiter* format, what character separates each data segment? (comma, semi-colon, etc.)
❐ If the file is in *fixed field* format, how many columns does it have? And how wide is each column, including the blank space(s) at the end of the column?
❐ What types of data are in the file? (e.g., tag number, state in which tag was issued, vehicle make, vehicle model, reason tag was captured, etc.). If you can't identify something, you will have to speak with someone from the source agency.
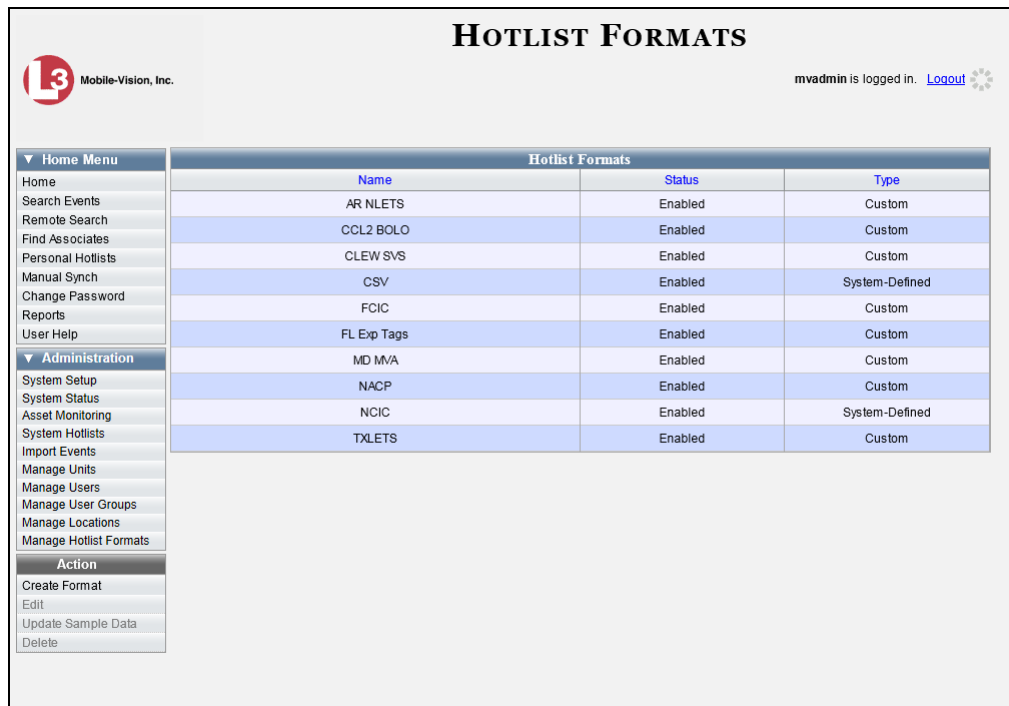
For specific instructions, see:

❐ Adding a 'Delimited' Hotlist Format, next page
❐ Adding a 'Fixed Field' Hotlist Format, page 179

Adding a 'Delimited' Hotlist Format

This section describes how to add a new custom hotlist format that is in *delimited* format. *Delimited* format separates each piece of data with a comma, semicolon, or space. To view a sample, see Figure 1 on page 172.

Before performing this procedure, review the previous section, "Adding a Custom Hotlist Format."

1   If you have not done so already, obtain answers to the *hotlist format questions* listed at the top of this page.

2   Go to ▼ Administration and click **Manage Hotlist Formats**. The Hotlist Formats page displays.

3   Go to the Action column and click **Create Format**. The Import Sample Data popup displays.

4   Click **Browse**. The Choose File to Upload popup displays.

5   Navigate to the disk drive location where the hotlist is located (i.e, the sample hotlist provided by the source agency).

6 Double-click on the appropriate hotlist file. The file name displays in the *Hotlist File* field.

7 If this hotlist includes a header, check the *File contains header information* checkbox.

– OR –

If this hotlist does *not* include a header (default), proceed to the next step.

8 Click **Upload**. After a delay of 10 – 20 seconds, the Hotlist Format Properties screen displays.

(Continued)

The fields on this page are described below.

Hotlist Format Properties	
Field	**Description**
Name	The name of the hotlist format.
Enabled	A checkbox used to activate (enable) or deactivate (disable) this hotlist format. ☑ Hotlist format is currently in use (enabled) ☐ Hotlist format is *not* currently in use (disabled). When a hotlist format is *disabled*, it will not appear on any drop-down lists in AlertVU.
Record Format	The manner in which this hotlist format file is organized: ▪ *Delimited*. Each data element in the file is separated by a comma, semicolon, or space. ▪ *Fixed*. Each data element in the file is in a column of a specific width, such as 8 characters.
Delimiter	The type of character used to separate each data element in the file: comma, semi-colon, or space. *Applies to 'delimited' hotlist formats only.*
Number of Columns	The total number of columns in this file. *Applies to 'fixed field' hotlist formats only.*
Label	The column heading. Enter one label for each column, beginning with column 1.

L3 Mobile-Vision, Inc.

Hotlist Format Properties (cont'd)	
Field	**Description**
Type	The type of data that displays in this column: ▪ *Metadata*. Any data that does not fall under the category of *plate*, *reason*, or *state*. ▪ *Plate*. The license plate number. ▪ *Reason*. The reason that the license plate is on this hotlist. ▪ *State*. The 2-position state code associated with the license plate. Select a *Type* for each column, beginning with column 1.
Display	A checkbox used to determine whether or not you wish to include this column's value in your alert displays. ☑ Include this column's value in your alert displays ☐ Do *not* include this column's value in your alert displays Select a *Display* value for each column, beginning with column 1.
Length	The column length in characters, including the extra space(s) at the end of the column. Enter the length for each column, beginning with column 1. Set the last column to zero (0). *Applies to 'fixed field' hotlist formats only.*

9 Enter a unique name for this hotlist in the *Name* field.

10 If the delimiter (i.e., data separator) used in this file is a comma (default), proceed to the next step.

– OR –

If the delimiter used in this file is a semi-colon or space, select the appropriate value from the *Delimiter* drop-down list.

11 Proceed to the *Label* field and enter a descriptive name for this column.

12 Proceed to the *Type* field and select a data type for this column from the drop-down list:

If this column contains license plate numbers, select **Plate**.

– OR –

If this column contains state codes, select **State**.

– OR –

(Continued)

If this column contains reasons why a plate is wanted, select **Reason**.

– OR –

If this column contains information that does not fall under any of the previous categories, select **Metadata**.

13 Proceed to the *Display* checkbox:

If you wish to include this column's value in your alert displays (default), proceed to the next step.

– OR –

If you do *not* wish to include this column's value in your alert displays, deselect the *Display* checkbox.

14 Enter/select information for all the remaining columns, as described in steps 11 – 13.

15 When you're finished entering/selecting column data, click **Generate Preview**. All the labels you just entered will display at the bottom of the page.

16 Review the displayed information to make sure it's correct.

If the display is correct, proceed to the next step.

– OR –

If the display is *not* correct, make any necessary adjustments, then click **Generate Preview** again. Once the display is 100% correct, proceed to the next step.

L3 Mobile-Vision, Inc.

17 Click **Save**. A confirmation message displays.
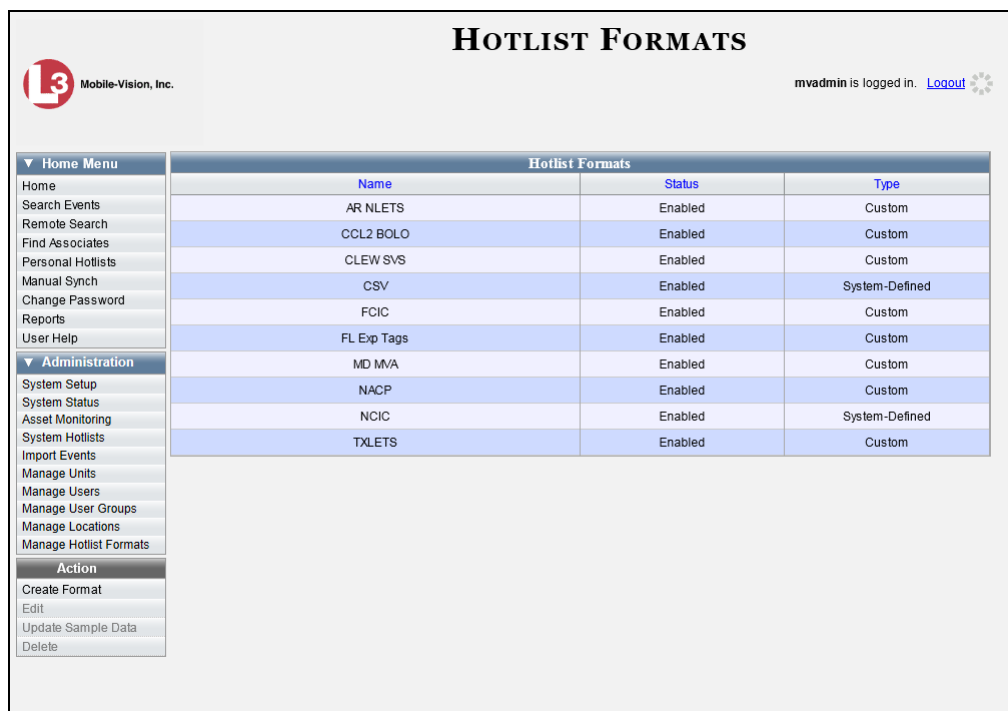
> The Hotlist Format named **NCMC** successfully saved.

Adding a 'Fixed Field' Hotlist Format

This section describes how to add a new custom hotlist format that is in *fixed field* format. *Fixed field* format means that each data element is in a column of a specific length, such as eight characters wide. To view a sample, see Figure 2 on page 172.

Before performing this procedure, review "Adding a Custom Hotlist Format" on page 172.

1 If you have not done so already, obtain answers to the *hotlist format questions* listed at the top of page 176.

2 Go to **▼ Administration** and click **Manage Hotlist Formats**. The Hotlist Formats page displays.

3 Go to the **Action** column and click **Create Format**. The Import Sample Data popup displays.

4 Click **Browse**. The Choose File to Upload popup displays.

5 Navigate to the disk drive location where the hotlist is located (i.e., the sample hotlist provided by the source agency).

6 Double-click on the appropriate hotlist file. The file name displays in the *Hotlist Field* field.

7 If this hotlist includes a header, select the *File contains header information* checkbox.

– OR –

If this hotlist does *not* include a header (default), proceed to the next step.

8 Click **Upload**. After a delay of 10 – 20 seconds, the Hotlist Format Properties screen displays.

The fields on this form are described on page 176.

9 Enter a unique name for this hotlist in the *Name* field.

10 Select **Fixed** from the *Record Format* drop-down list.

11 Proceed to the *Number of Columns* field and enter the total number of columns in this hotlist.

12 Press **Tab**. A blank field displays for each column.

(Continued)
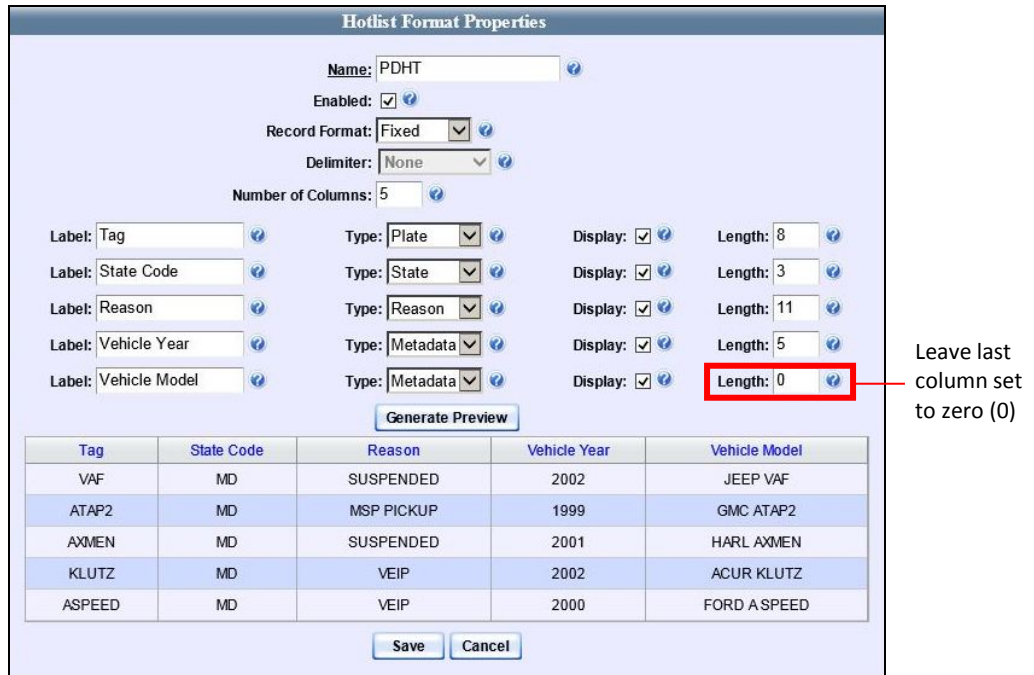
13 Proceed to the *Label* field and enter a heading for this column.

14 Proceed to the *Type* field and select a data type for this column from the drop-down list:

If this column contains license plate numbers, select **Plate**.

– OR –

If this column contains state codes, select **State**.

– OR –

If this column contains reasons why a plate is wanted, select **Reason**.

– OR –

If this column contains other information that does not fall under any of the previous categories, select **Metadata**.

15 Proceed to the *Display* checkbox:

If you wish to include this column's value in your alert displays (default), proceed to the next step.

– OR –

If you do *not* wish to include this column's value in your alert displays, deselect the *Display* checkbox.

16 Proceed to the *Length* field and enter the width of this column. This is the number of characters in that column, including the blank space or spaces at the end of the column.

L3 Mobile-Vision, Inc.

17 Enter/select information for all the remaining columns, as described in steps 13 – 16. Leave the length of the last column set to zero (0), as the system will automatically allocate the remaining space in the row to that column.

18 When you're finished entering/selecting column data, click **Generate Preview**. All the labels you entered will display at the bottom of the page, as pictured below.

Hotlist Format Properties

Name: PDHT
Enabled: ☑
Record Format: Fixed
Delimiter: None
Number of Columns: 5

Label:	Type:	Display:	Length:
Tag	Plate	☑	8
State Code	State	☑	3
Reason	Reason	☑	11
Vehicle Year	Metadata	☑	5
Vehicle Model	Metadata	☑	0

Generate Preview

Leave last column set to zero (0)

Tag	State Code	Reason	Vehicle Year	Vehicle Model
VAF	MD	SUSPENDED	2002	JEEP VAF
ATAP2	MD	MSP PICKUP	1999	GMC ATAP2
AXMEN	MD	SUSPENDED	2001	HARL AXMEN
KLUTZ	MD	VEIP	2002	ACUR KLUTZ
ASPEED	MD	VEIP	2000	FORD A SPEED

Save   Cancel

19 Review the displayed information to make sure it's correct. If the hotlist file has more than five columns, use the scroll bar to scan all the rows.

If the display is correct, proceed to the next step.

– OR –

If the display is *not* correct, make any necessary adjustments, then click **Generate Preview** again. Once the display is 100% correct, proceed to the next step.

20 Click **Save**. A confirmation message displays.

The Hotlist Format named PDHT successfully saved.

Viewing a Hotlist Format

This section describes how to view a system-defined or custom hotlist format. For more on hotlist formats and how they are used in AlertVU, see "Maintaining Hotlist Formats" on page 168.

1 Go to ▼ Administration and click **Manage Hotlist Formats**. The Hotlist Formats page displays.

2 Click on the hotlist format you wish to view.

3 Go to the Action column and click **Edit** or **View**. The Hotlist Format Properties screen displays.

L3 Mobile-Vision, Inc.

The fields on this form are described on page 176.

4 When you're finished viewing the hotlist format, click **Cancel** to exit.

Changing a Custom Hotlist Format

Periodically, you may need to update your custom hotlist formats. For example, if the source organization that supplies you with hotlist XYZ adds a column to that hotlist, you will have to update the associated hotlist format record in AlertVU. This procedure varies slightly depending on whether you are importing sample hotlist data or not. For example, some minor edits, such as changing a column name, do not require the use of sample hotlist data. Other more significant changes require that you import sample hotlist data, as you did when you first created the hotlist.
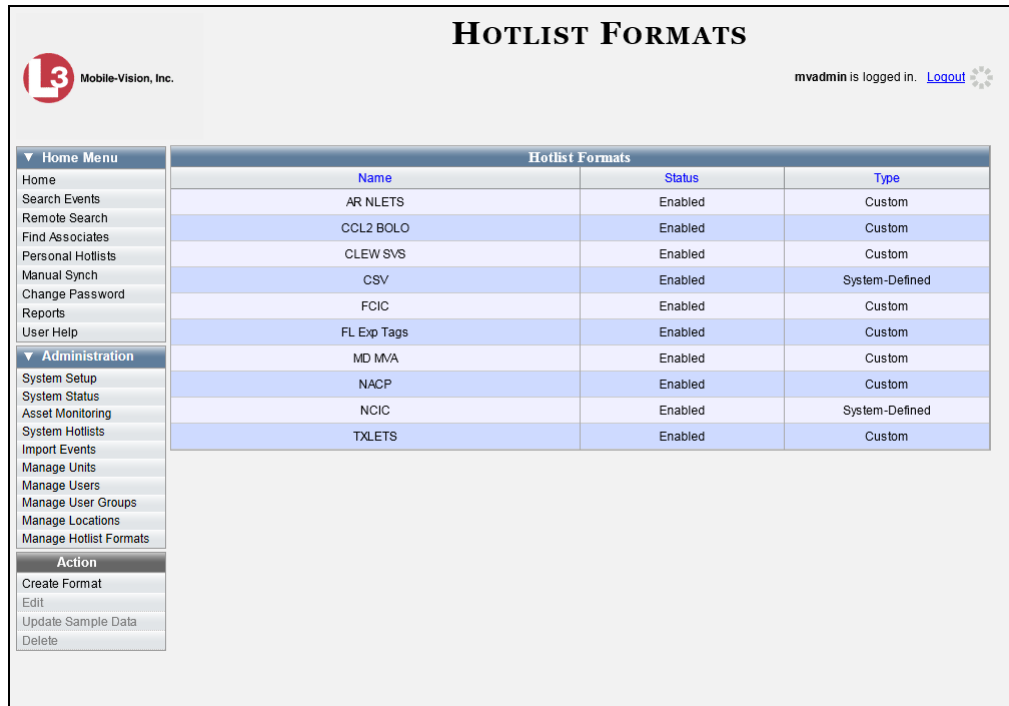
For specific instructions, see:

❐ Procedure 1: Updating a Hotlist Format with Sample Data, next page
❐ Procedure 2: Updating a Hotlist Format Without Sample Data, page 189.

Procedure 1: Updating a Hotlist Format with Sample Data

This section describes how to update a custom hotlist format when there is a sample data file available (i.e., a copy of the updated hotlist file that contains sample data). If there is no sample data file available, see "Procedure 2: Updating a Hotlist Format Without Sample Data" on page 189 instead.

1 Go to ▼ Administration and click **Manage Hotlist Formats**. The Hotlist Formats page displays.

2 Click on the hotlist format you wish to update.

3 Go to the Action column and click **Update Sample Data**. The Update Sample Data popup displays.

4 Click **Browse**. The Choose File to Upload popup displays.

5 Navigate to the disk drive location where the sample hotlist is located.
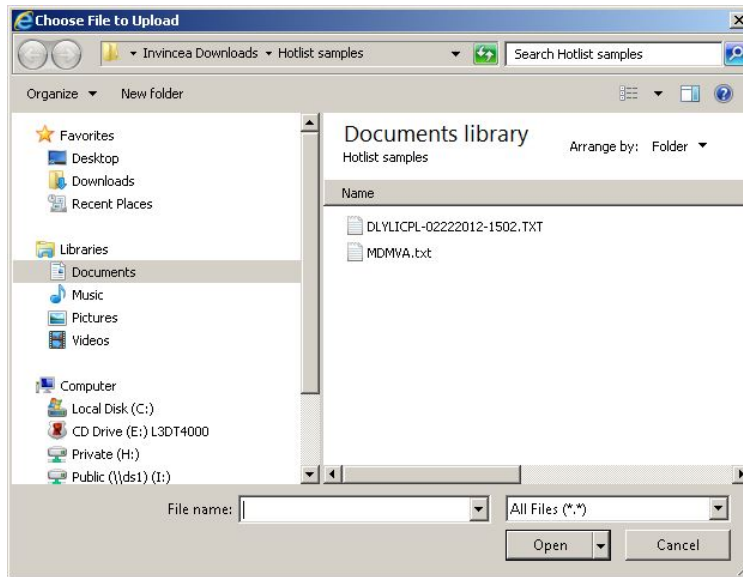
6   Double-click on the appropriate file. The file name displays in the *Hotlist File* field.
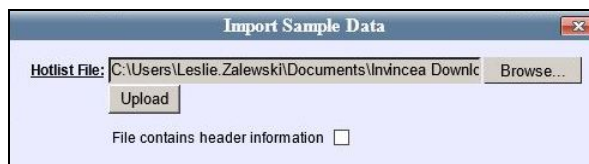
7   If this hotlist includes a header, select the *File contains header information* checkbox.

– OR –

If this hotlist does *not* include a header (default), proceed to the next step.

8   Click **Upload**. After a delay of 10 to 20 seconds, the Hotlist Format Properties screen displays.

(Continued)

The fields on the Hotlist Format Properties form are described on page 176.

9 Enter/select your changes in the appropriate fields.

❐ If this hotlist is in *delimited* format, review steps 9 – 14 of "Adding a 'Delimited' Hotlist Format," beginning on page 177.

❐ If this hotlist is in *fixed field* format, review steps 9 – 17 of "Adding a 'Fixed Field' Hotlist Format," beginning on page 181.

10 When you're finished entering/selecting data, click **Generate Preview**. Your changes will display at the bottom of the page.

11 Review the displayed information to make sure it's correct.

If the display is correct, proceed to the next step.

– OR –

If the display is *not* correct, make any necessary adjustments, then click **Generate Preview** again. Once the display is 100% correct, proceed to the next step.

12 Click **Save**. A confirmation message displays.
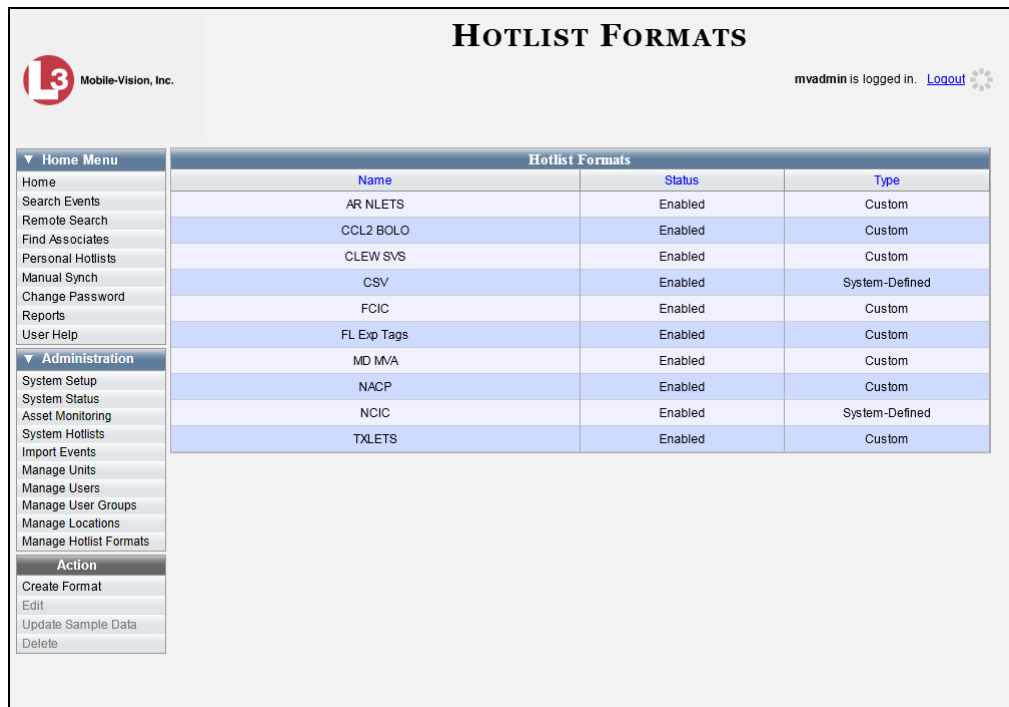
The Hotlist Format named **NACP** successfully saved.

Procedure 2: Updating a Hotlist Format Without Sample Data

This section describes how to update a custom hotlist format when one of the following circumstances applies:

❒ There is no sample data file available, or
❒ You are making a simple change that does not require the use of a sample data file.

1 Go to ▼ Administration and click **Manage Hotlist Formats**. The Hotlist Formats page displays.

2 Click on the hotlist format you wish to update.

3 Go to the Action column and click **Edit**. The Hotlist Format Properties screen displays.

(Continued)

The fields on this form are described on page 176.

4 Enter/select your changes in the appropriate fields.

5 Click **Save**. A confirmation message displays.

> The Hotlist Format named NACP successfully saved.

Deleting a Custom Hotlist Format

This section describes how to delete a custom hotlist format.

1 Go to ▼ Administration and click **Manage Hotlist Formats**. The Hotlist Formats page displays.

L3 Mobile-Vision, Inc.

HOTLIST FORMATS

Mobile-Vision, Inc.

mvadmin is logged in. Logout

▼ Home Menu		Hotlist Formats		
Home		Name	Status	Type
Search Events		AR NLETS	Enabled	Custom
Remote Search		CCL2 BOLO	Enabled	Custom
Find Associates		CLEW SVS	Enabled	Custom
Personal Hotlists		CSV	Enabled	System-Defined
Manual Synch		FCIC	Enabled	Custom
Change Password		FL Exp Tags	Enabled	Custom
Reports		MD MVA	Enabled	Custom
User Help		NACP	Enabled	Custom
▼ Administration		NCIC	Enabled	System-Defined
System Setup		TXLETS	Enabled	Custom
System Status				
Asset Monitoring				
System Hotlists				
Import Events				
Manage Units				
Manage Users				
Manage User Groups				
Manage Locations				
Manage Hotlist Formats				
Action				
Create Format				
Edit				
Update Sample Data				
Delete				

2 Click on the hotlist format you wish to delete. Keep in mind that you *cannot* delete the CSV or NCIC formats, as they are system-defined.

3 Go to the Action column and click **Delete**. A confirmation message displays.

Confirm Delete

Delete this hotlist format? NACP

Yes   No

4 Click **Yes**. The selected hotlist format is removed from the Hotlist Formats list.

Maintaining Locations

Locations A Location is a predefined geographic region that you can apply to a system hotlist. When you assign a Location to a system hotlist, it narrows that hotlist's criteria to plates that are scanned within the Location's region.

Location Groups In addition to Location records, there is also another, similar, feature in AlertVU called *Location Groups*. This type of record simply combines multiple Locations into one group, making it easier to apply multiple locations to a hotlist at the same time.

For more information, see:
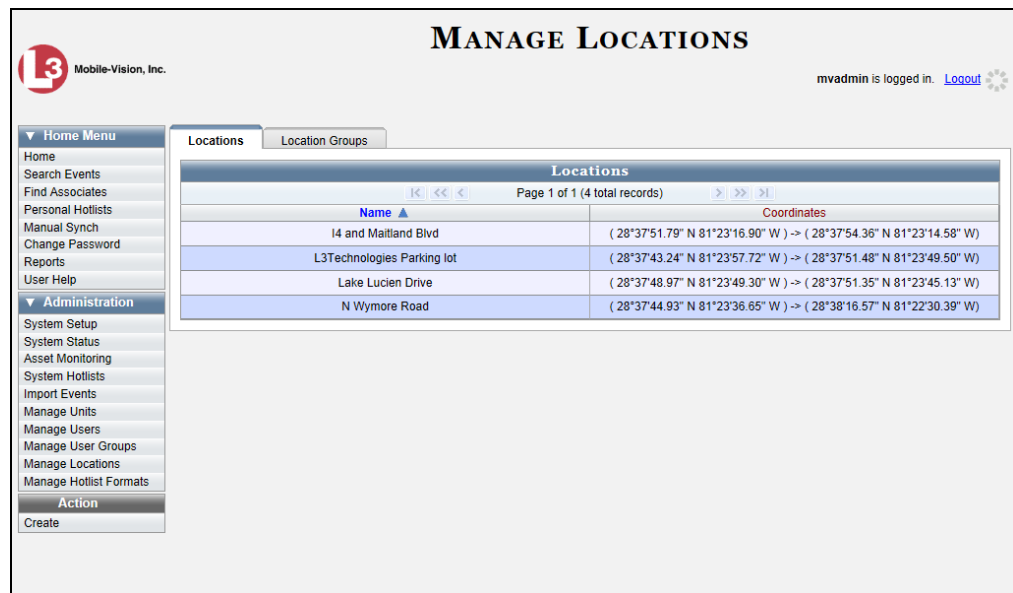
❏ Adding a Location, below
❏ Changing a Location, page 196
❏ Deleting a Location, page 198
❏ Adding a Location Group, page 200
❏ Changing a Location Group, page 202
❏ Deleting a Location Group, page 205.

Adding a Location

This section describes how to create a new Location, which you can, in turn, apply to a new or existing hotlist. For more on Locations and how they are used in AlertVU, see the previous section, "Maintaining Locations."

The *Location Management* permission is required to perform this task.

1 Go to ▼ Administration and click **Manage Locations**. The Manage Locations page displays.

AlertVU Back Office Administrator's Guide
L3 Mobile-Vision • 8.7.2017

2 Go to the Action column and click **Create**. The New Location page displays.
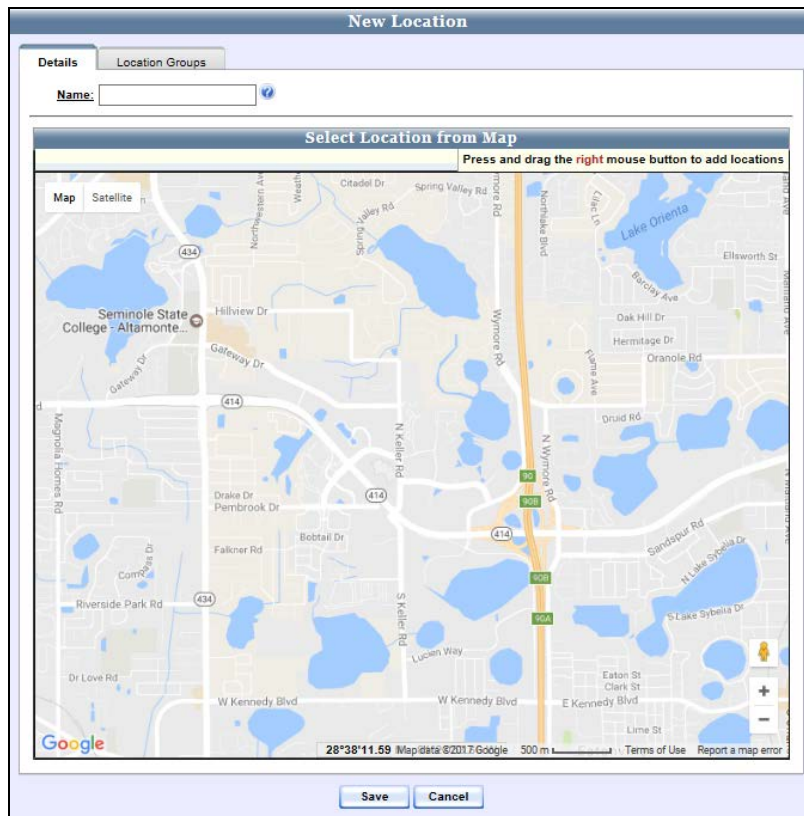
This map defaults to your main precinct location. To update this location, see "Updating Precinct Information" in chapter 6.

3 Enter a unique name for this Location in the *Name* field at the top of the page.

4 Manually reposition the map so that the desired location is visible. To do so, click on the map and drag it into the correct position. If necessary, use the plus (+) or minus (-) icons to zoom the map image in or out, respectively.

5 Click and drag the right mouse button over the desired location. A green box displays in the selected area.

(Continued)
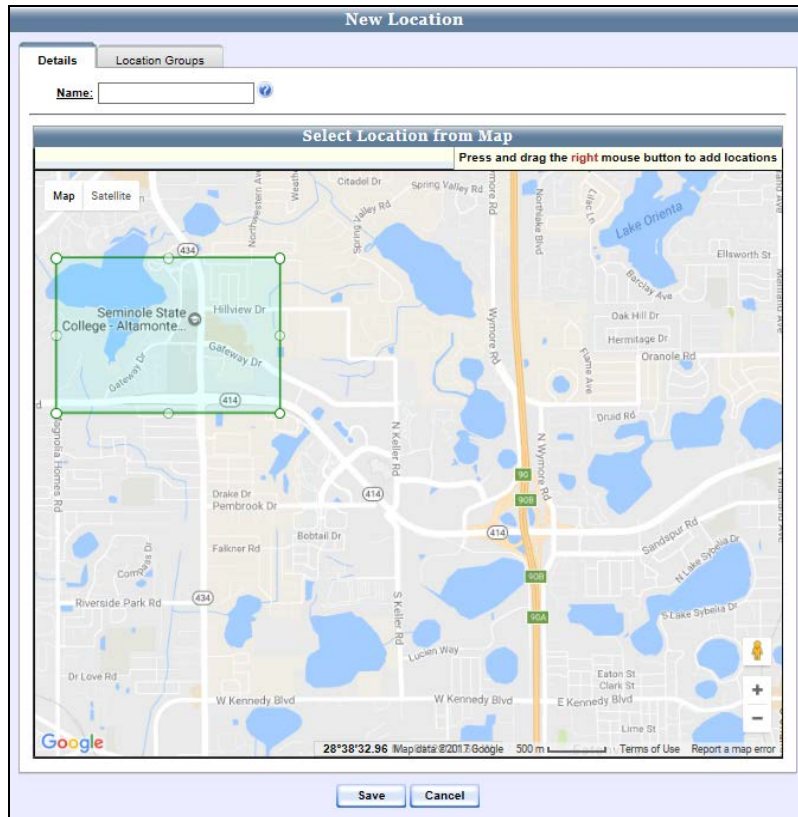
6 If you are satisfied with the box's parameters, skip to step 8.

– OR –

If you are *not* satisfied with the box's parameters, proceed to the next step.

7 Using the small circle icons that surround the box, adjust the box's parameters. To do so, click on one circle at a time and drag that segment of the box in/out, right/left, or up/down. Once you're satisfied with the parameters of your box, proceed to the next step.

8 To add this Location to an existing Location Group(s), proceed to the next step. Otherwise skip to step 12.

9 Click the **Location Groups** tab. A list of your existing Location Groups displays in the *Available* column.
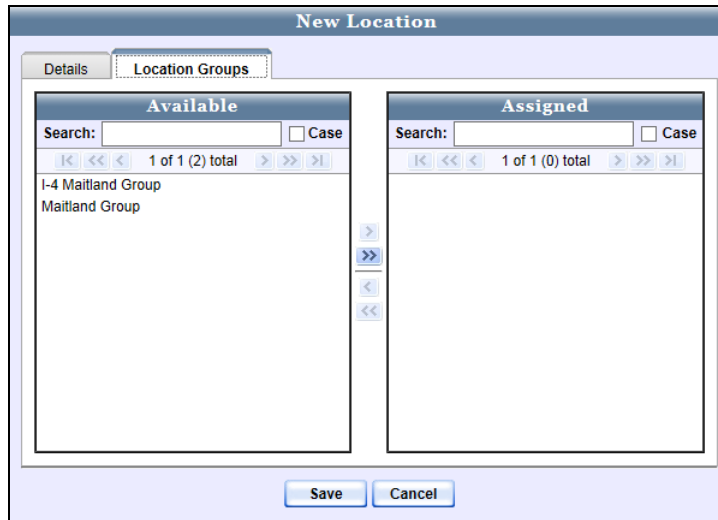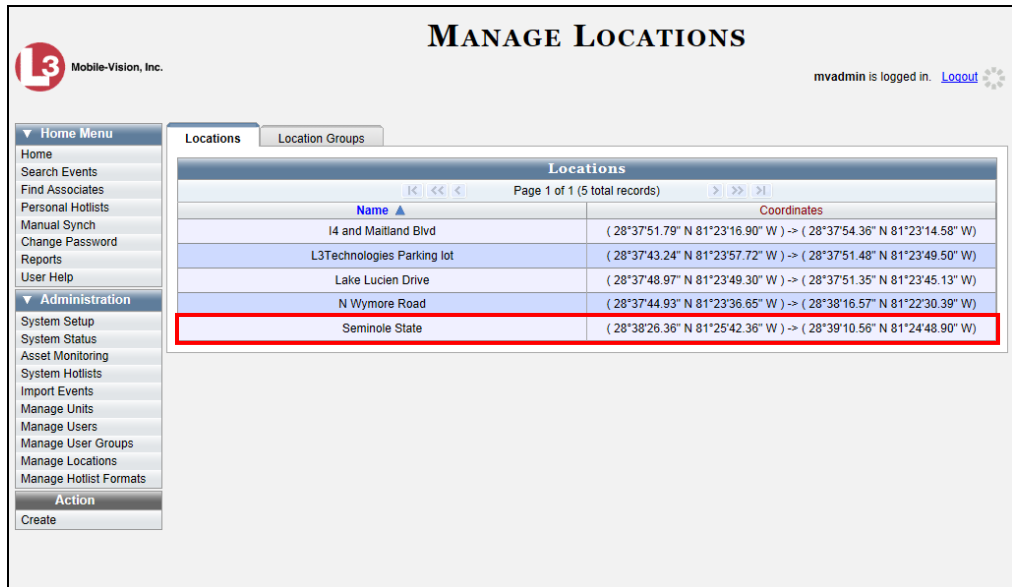
If the *Available* column is blank, it indicates that your agency has not created any Location Groups yet. For more information, see "Adding a Location Group" on page 200.

10 Go to the *Available* column and click on the Location Group(s) you wish to add the new Location to.

11 Click the ▶ icon located between the two columns. The selected Location Group(s) display in the *Assigned* column.
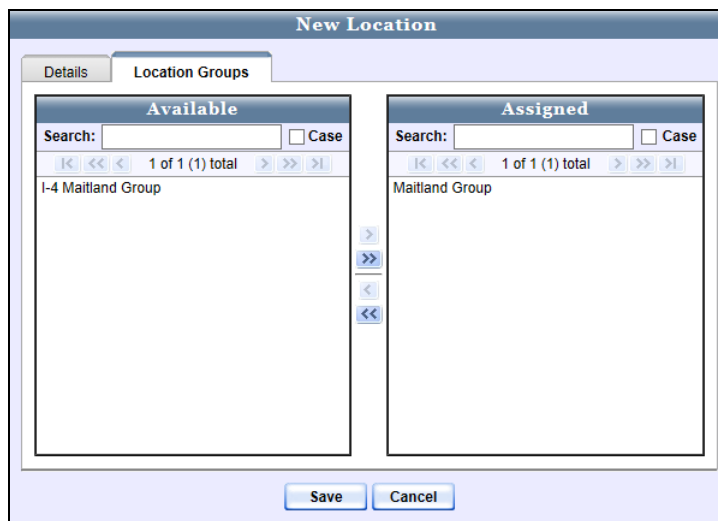
12 Click **Save**. The new Location displays on the Locations list.

(Continued)
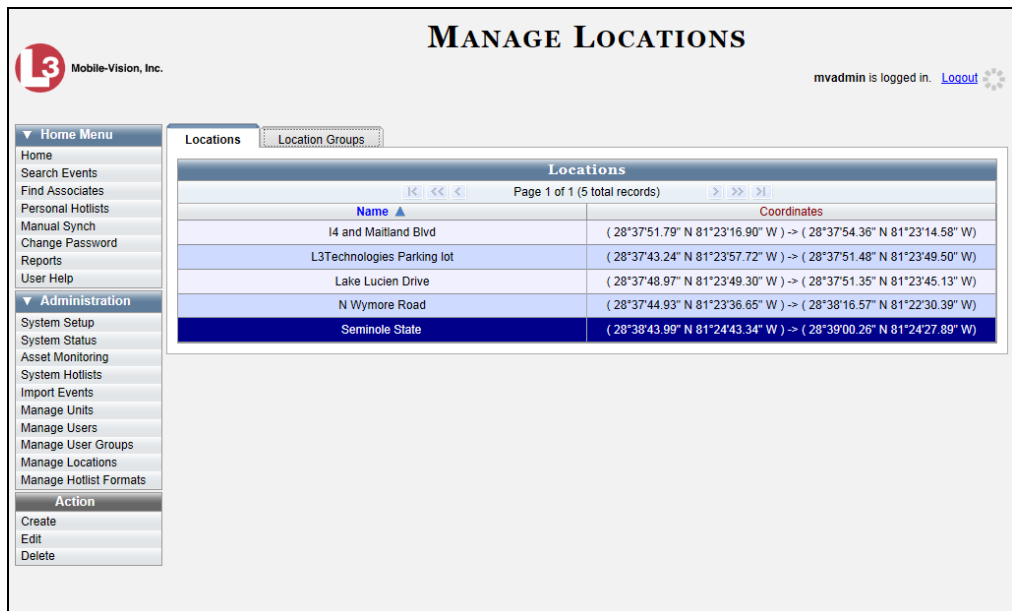
Changing a Location

This section describes how to update an existing Location record. For more on Locations and how they are used in AlertVU, see "Maintaining Locations" on page 192.

The *Location Management* permission is required to perform this task.

1 Go to ▼ Administration and click **Manage Locations**. The Manage Locations page displays, as pictured above.

2 Click on the Location you wish to update.

3 Go to the `Action` column and click **Edit**. The Location Properties page displays.
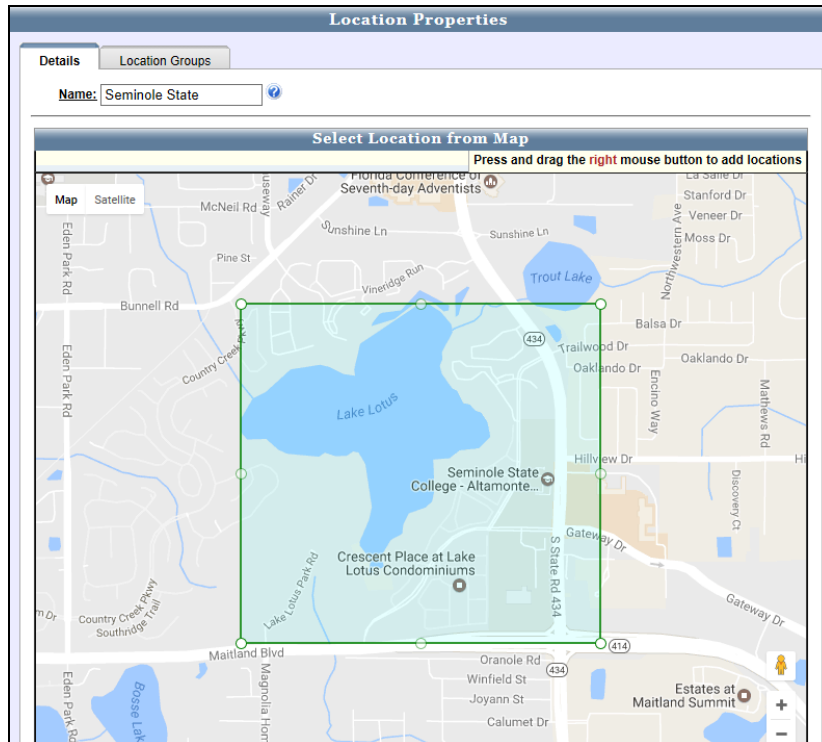
4 To change the name of this Location, enter a new value in the *Name* field. Otherwise proceed to the next step.

5 To change the geographic parameters of this Location, proceed to the next step. Otherwise skip to step 7.

6 Use the circle icons that surround the box to adjust its parameters. To do so, click on the circles one at a time and drag that segment of the box in/out, right/left, or up/down. Once you are satisfied with the parameters of your box, proceed to the next step.

7 To assign this Location to a new Location Group *or* unassign this Location from its current Location Group(s), proceed to the next step. Otherwise skip to step 15.

8 Click the **Location Groups** tab. Your existing Location Group assignment(s) display in the *Assigned* column.

(Continued)
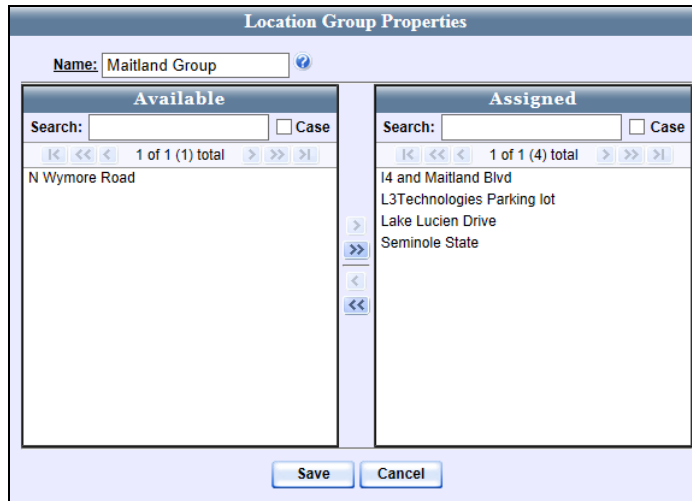
9 To add this Location to a new Location Group, proceed to the next step. Otherwise skip to step 12.

10 Go to the *Available* column and click on the Location Group(s) you wish to add this Location to.

11 Click the ▶ icon located between the two columns. The selected Location Group(s) display in the *Assigned* column.

12 To remove this Location from an assigned Location Group(s), proceed to the next step. Otherwise skip to step 15.

13 Go to the *Assigned* column and click on the Location Group(s) you wish to remove this Location from.

14 Click the ◀ icon located between the two columns. The selected Location Group(s) display in the *Available* column.

15 Click **Save**.

Deleting a Location

This section describes how to delete a Location. For more on Locations and how they are used in AlertVU, see "Maintaining Locations" on page 192.

The *Location Management* permission is required to perform this task.

1 Go to ▼ Administration and click **Manage Locations**. The Manage Locations page displays.
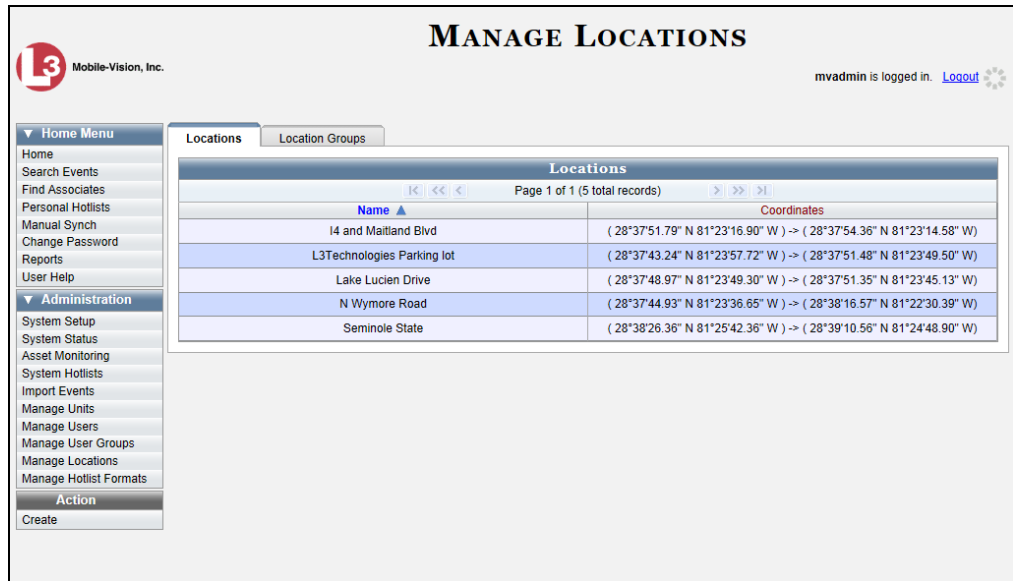
2 Click on the Location you wish to delete.
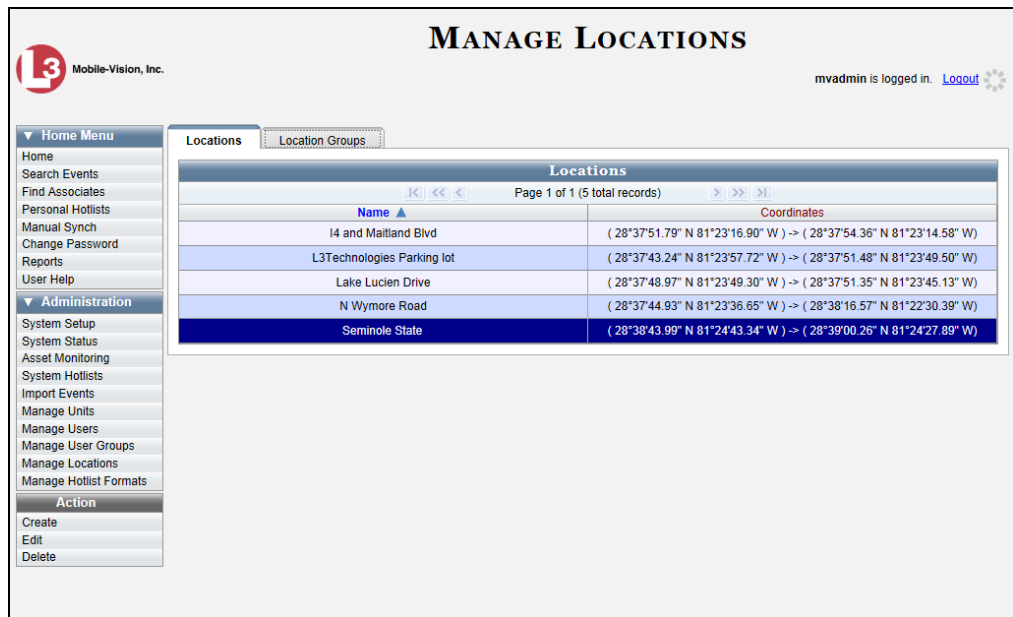
3 Go to the Action column and click **Delete**. A verification message displays.
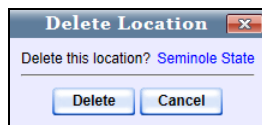
4 Click **Delete**. A confirmation message displays.
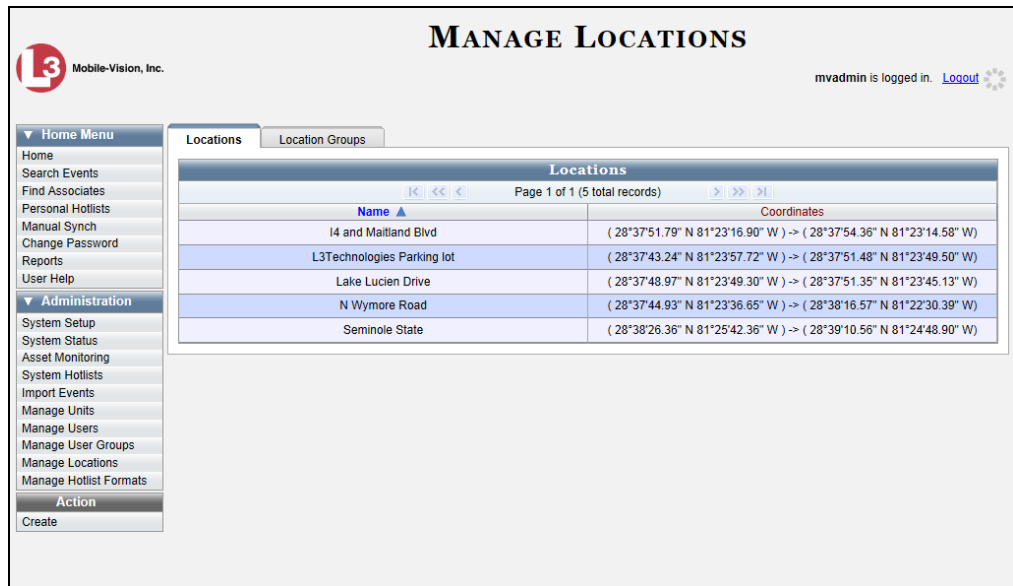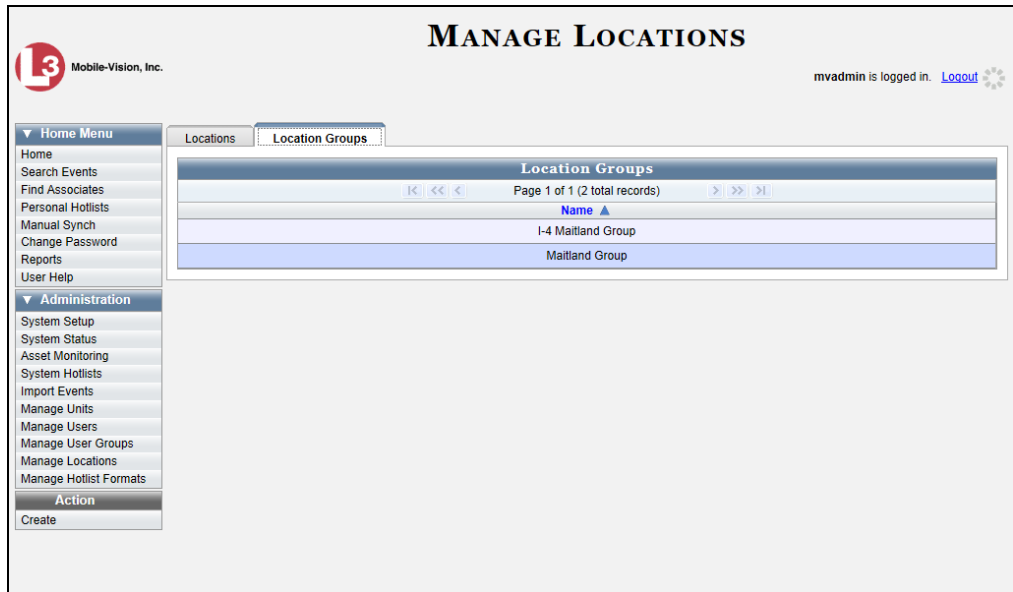
Adding a Location Group

This section describes how to add a new Location Group, which you can, in turn, apply to a new or existing hotlist. A Location Group is simply a record that contains multiple Locations. For more on Location Groups and how they are used in AlertVU, see "Maintaining Locations" on page 192.

The *Location Management* permission is required to perform this task.

NOTE: In order to enter a Location Group, you must first have some Locations. If you haven't created any Location records yet, see "Adding a Location" on page 192.

1   Go to ▼ Administration and click **Manage Locations**. The Manage Locations page displays.

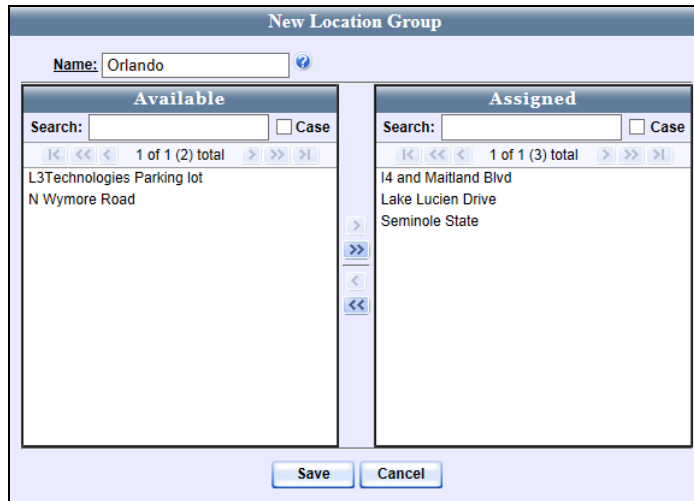2   Click the **Location Groups** tab. A list of existing Location Groups displays (if any).

3 Go to the Action column and click **Create**. The New Location Group form displays.
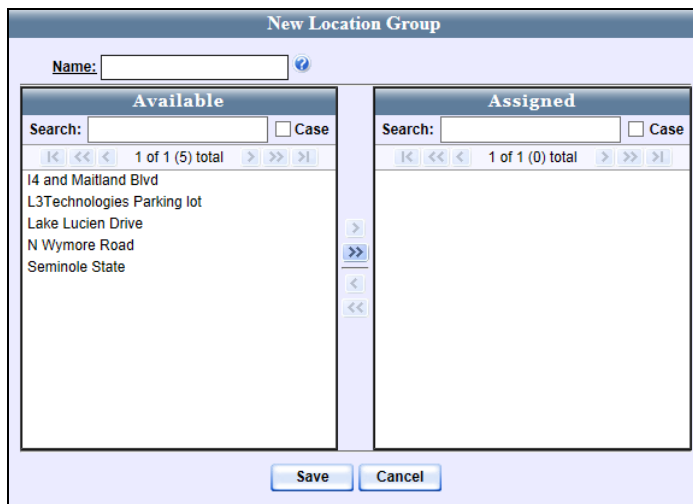
4 Enter a unique name for this Location Group in the *Name* field.

5 Go to the *Available* column and click on the Locations you wish to add to the new Location Group.

6 Click the ▶ icon located between the two columns. The selected Locations display in the *Assigned* column.
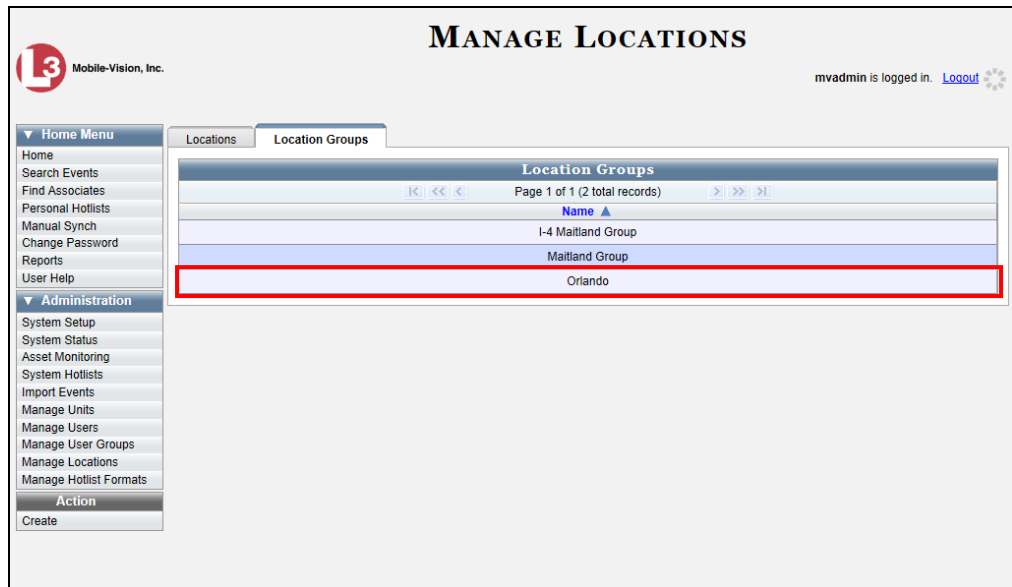
(Continued)

7 Click **Save**. The new Location Group displays on the Location Groups list.

Changing a Location Group

This section describes how to update an existing Location Group. For more on Location Groups and how they are used in AlertVU, see "Maintaining Locations" on page 192.

The *Location Management* permission is required to perform this task.

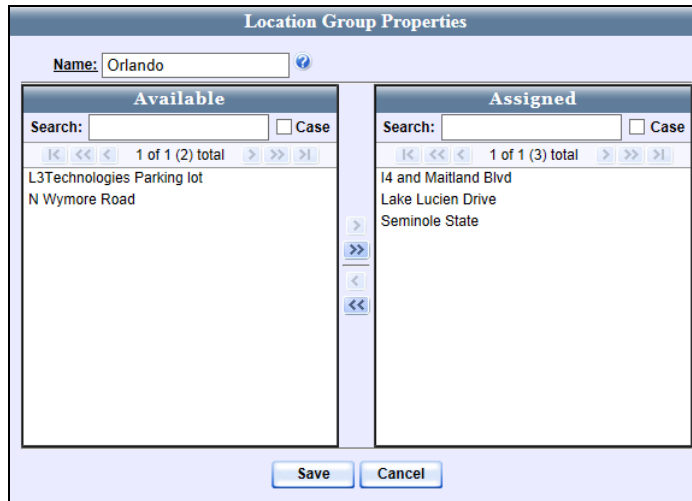**1** Go to ▼ Administration and click **Manage Locations**. The Manage Locations page displays.

2 Click the **Location Groups** tab. A list of existing Location Groups displays, as pictured on the previous page.

3 Click on the Location Group you wish to update.

4 Go to the Action column and click **Edit**. The Location Group Properties form displays.

(Continued)

5 To change the name of this Location Group, enter a new value in the *Name* field. Otherwise proceed to the next step.

6 To add a new Location to this Location Group, proceed to the next step. Otherwise skip to step 9.

7 Go to the *Available* column and click on the Location(s) you wish to add to this Location Group.

8 Click the ▶ icon located between the two columns. The selected Location(s) display in the *Assigned* column.

9 To remove an existing Location from this Location Group, proceed to the next step. Otherwise skip to step 12.

10 Go to the *Assigned* column and click on the Location(s) you wish to remove from this Location Group.

11 Click the ◀ icon located between the two columns. The selected Location(s) display in the *Available* column.

**12** Click **Save**.

Deleting a Location Group

This section describes how to delete a Location Group. For more on Location Groups and how they are used in AlertVU, see "Maintaining Locations" on page 192.

The *Location Management* permission is required to perform this task.

1   Go to ▼ Administration and click **Manage Locations**. The Manage Locations page displays.
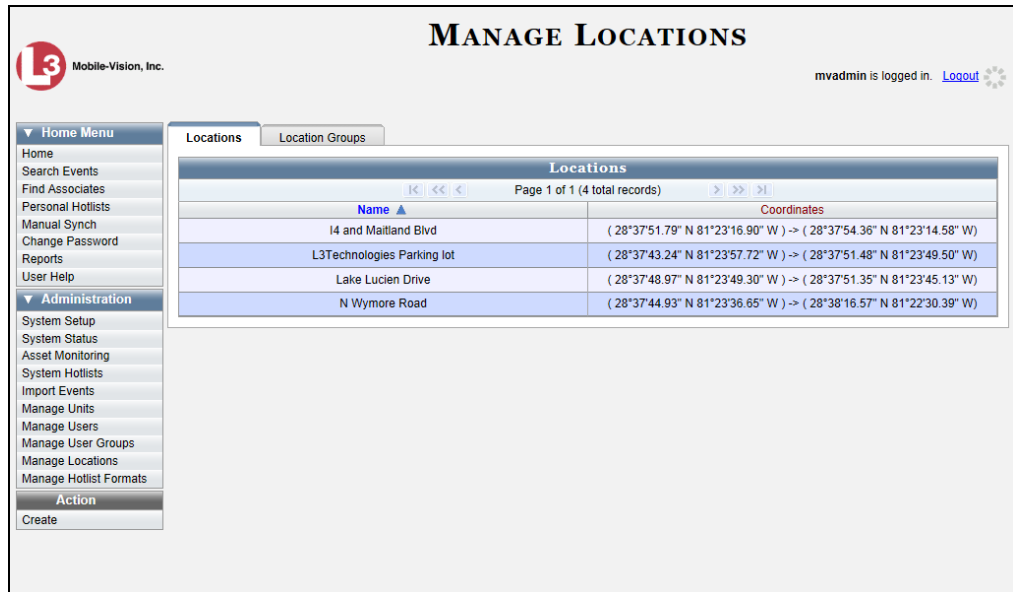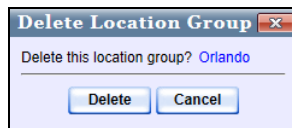

2   Click the **Location Groups** tab. A list of existing Location Groups displays.
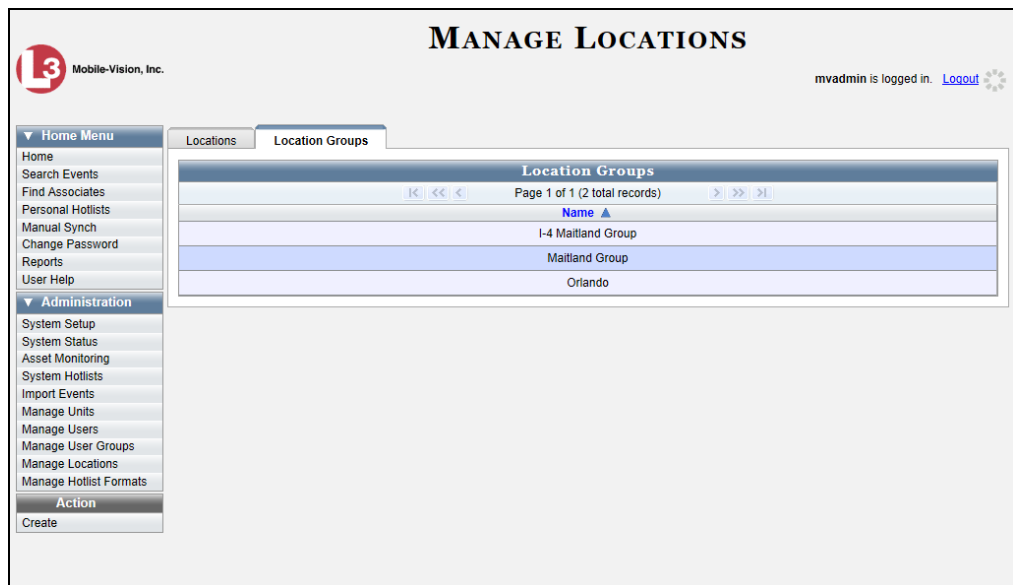
3   Click on the Location Group you wish to delete.

4   Go to the Action column and click **Delete**. A verification message displays.

5   Click **Delete**. A confirmation message displays.

4 Units

There are two types of AlertVU units: *mobile* and *fixed*. Mobile units are installed in a vehicle, such as a patrol car. Fixed units are installed on a stationary device, such as a pole, traffic light, street sign, or even a towable trailer. Both varieties connect to a PC of some kind. Mobile units connect to a mobile data computer, and fixed units connect to a laptop. These PCs control and transmit plate reads to the server via the AlertVU PC applications. For more information on these applications, see "In-Unit PC Applications" in chapter 1.

Each of your AlertVU units has a corresponding record entered in AlertVU Back Office. These records store all the information required for successful communication between your AlertVU units and the server. They are created automatically by the system whenever it discovers a new (i.e., unknown) device on the network. There are two discovery methods available:

❐ *TCP Ping*. By default, a TCP "ping" command is used to test whether a specific unit is reachable across the network. This method requires that you specify a range or ranges of IP addresses that the AlertVU server should search. For more information, see "Maintaining IP Address Ranges" on page 228.
❐ *UDP Broadcast*. This method instructs the server to listen for UDP Unicast "hello" messages sent by the AlertVU Mobile unit on a specified *UDP Listen Port*. By default, AlertVU Mobile units send out this UDP Unicast message to the server's IP address every five seconds.

If neither of these discovery methods works for your particular network configuration, you can use an alternate form of unit-to-server communication called *Passive Download Mode*. With *Passive Download Mode*, the in-car or fixed *AlertVU unit*, rather than the *AlertVU server*, initiates communication. Simply put, the AlertVU unit *pushes* plate capture data out to the server and *pulls* updated hotlists down from the server.

Your AlertVU units typically communicate with the server via a wireless connection. If, for some reason, you lose your wireless connection for a prolonged period of time, you can also transmit events to the server using a manual procedure. For more on this topic, see "Manually Synchronizing Your Unit with the Server" on page 215.

For more information, see:

☐ Viewing Your Units' Status, page 234
☐ Customizing the Asset Monitoring Page, page 235.

Searching for a Unit

This section describes how to search for an existing AlertVU unit record by one or more of the following fields: *Unit Name*, *Last known IP*, *Serial Number*, *Status*, and/or *Version*.

1 Go to ▼ Administration and click **Manage Units**. The Unit Search Results page displays.

2 Enter/select the field values you wish to search on, as described in the following table.

Search Field	Description
Unit Name	Limits your search to the AlertVU unit that has this name.
Last Known IP	Limits your search to the AlertVU unit that last used this IP address.
Serial Number	Limits your search to the AlertVU unit that has this internal software serial number. **Note**: This is the *software* serial number, *not* the hardware serial number found on the outside of the AlertVU unit.
Status	Limits your search to those AlertVU units that have a status of either **Enabled** (in use) or **Disabled** (not in use). *Select a status from the drop-down list provided.*
Version	Limits your search to those AlertVU units that have this software version. *Select a version number from the drop-down list provided.*

After you enter a search value, the system will automatically display those records that match your search criteria.
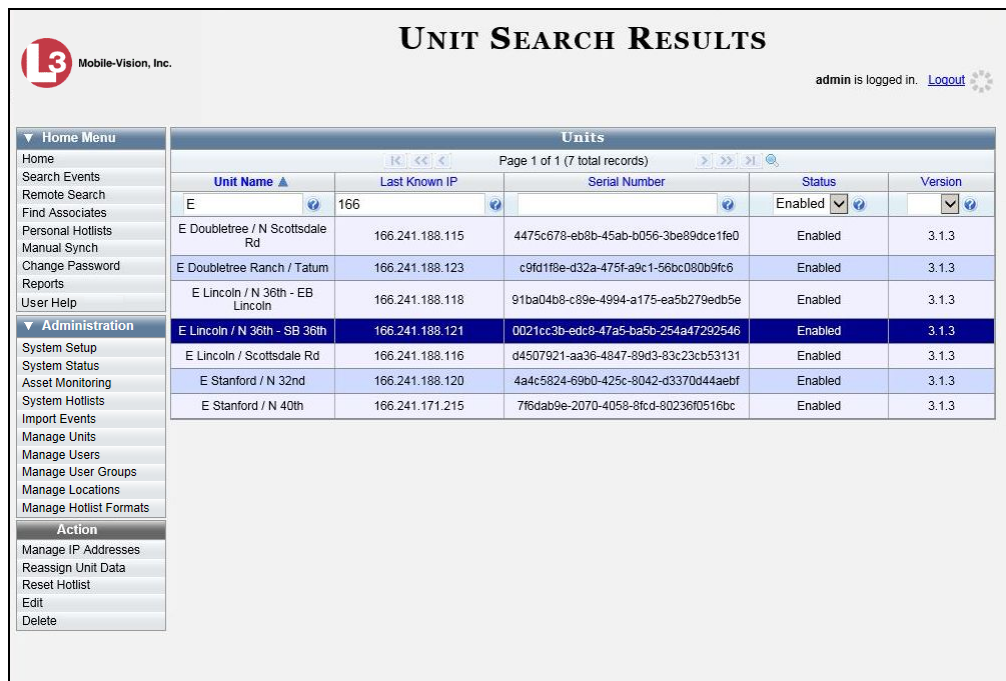
Changing a Unit

This section describes how to update an existing unit record. Perform this task when you need to:

❐ Change a unit's name
❐ Disable a unit that is no longer in service
❐ Change a unit's *type* (i.e., *mobile* vs. *fixed*)
❐ Add a camera to a unit.

1 Search for and select the unit you wish to update. (If necessary, review "Searching for a Unit" on page 208.)

2 Click on the unit record to highlight it.

3 Go to the Action column and click **Edit**.

– OR –

Right-click on the record, then select **Edit** from the popup menu. The Edit Unit popup displays.

The fields on this form are described below.

Edit Unit	
Field	**Description**
Unit Name	The name used throughout the AlertVU Back Office application to reference this unit (e.g., Unit 146).
Last Known IP	The unit's current IP address. This number identifies the unit to the server. *Display only field.*
Version	The version of the L3 Mobile-Vision transmission software that is installed on this unit. **Note**: If this is a mobile unit, this version is for L3 Mobile-Vision's transmission software, *not* the AlertVU Mobile application. *Display only field.*
Status	A system setting that determines whether or not wireless data transmissions are allowed for this unit: ▪ *Enabled* (default). The system will automatically transfer data to and from this unit. ▪ *Disabled*. The system will *not* transfer data to and from this unit. *Select this value from the drop-down list provided.*
Unit Type	The type of unit this is: ▪ *Mobile*. A unit that is installed inside a vehicle, such as a police cruiser. ▪ *Fixed*. A unit that is mounted to a stationary device, such as a pole. Select this value from the drop-down list provided.

4 To change the unit's name, enter a new value in the *Unit Name* field. Otherwise proceed to the next step.

5 To change the unit's status (i.e., *enabled* vs. *disabled*), proceed to the next step. Otherwise skip to step 7.

6 Go to the *Status* drop-down list:

To *enable* the unit so that it will automatically transfer data to/from the server, select **Enabled**.

– OR –

To *disable* the unit so that it will *not* automatically transfer data to/from the server, select **Disabled**.

7 To change the unit's type (i.e., *mobile* vs. *fixed*), proceed to the next step. Otherwise skip to step 9.

8 Go to the *Unit Type* drop-down list:

If this unit is installed in a vehicle, such as a police cruiser, select **Mobile**.

– OR –

If this unit is attached to a stationary device, such as a pole, select **Fixed**.

9 To add a camera to this unit, proceed to the next step. Otherwise skip to step 13.

Adding a Camera

10 Click **Add Camera**. A new camera row displays. The required *Lane ID* and *Label* values can be found in the L3 AlertVU Mobile Administration application, which is installed on the unit's mobile data computer.
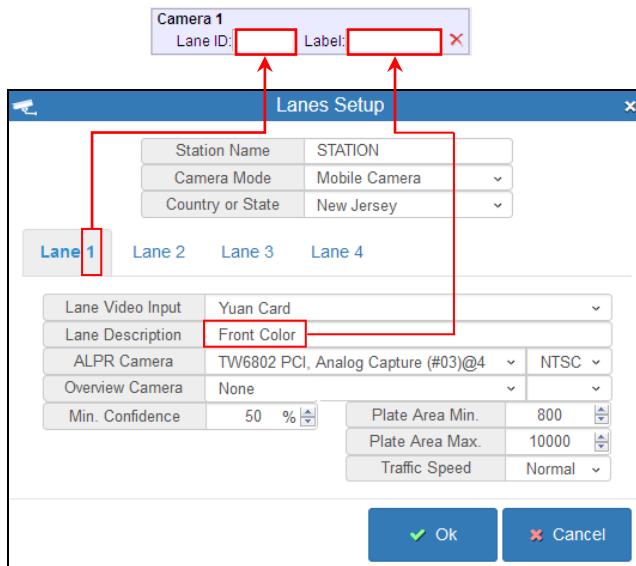
To display the Lanes Setup screen pictured here, first proceed to the AlertVU unit and login to AlertVU Mobile as an Admin user. Next, click the **ALPR** button at the top of the page.
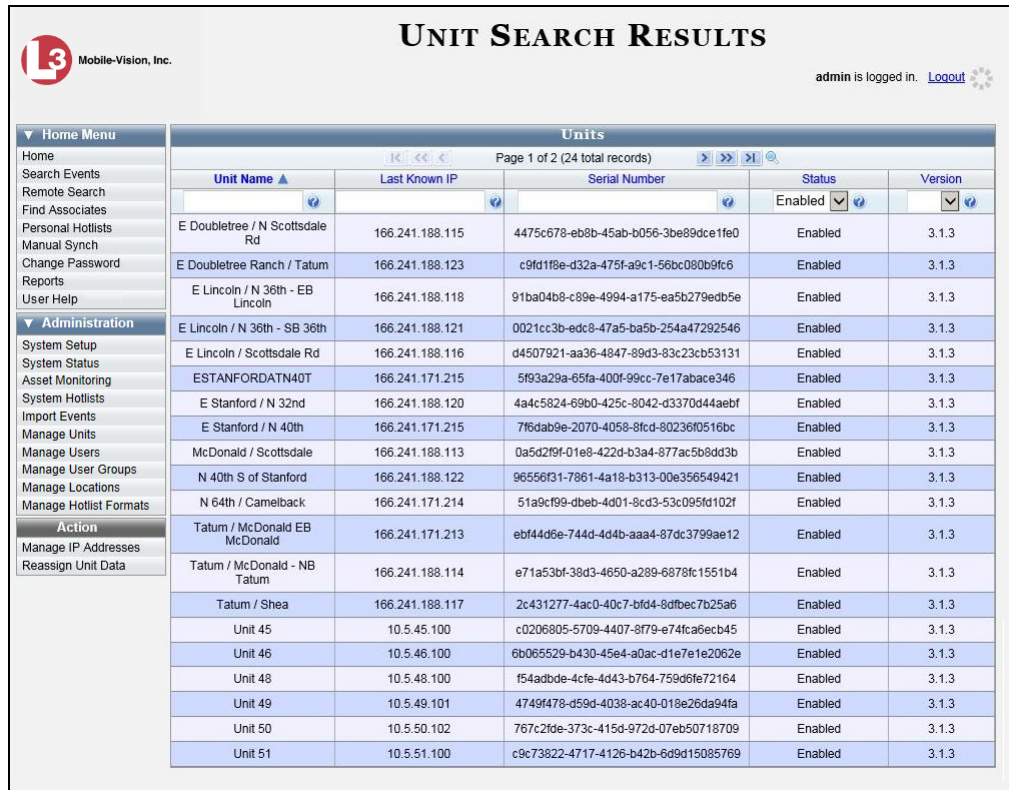
11 Enter the camera's lane number in the *Lane ID* field (1 – 4).

12 Enter the camera's lane description in the *Label* field.

13 Click **Save**.

L3 Mobile-Vision, Inc.

Deleting a Unit

This section describes how to permanently remove a unit record from the server. You can only delete a unit that does not have any event records associated with it.

1 Go to **▼ Administration** and click **Manage Units**. The Unit Search Results page displays.

2 Locate the unit record you wish to delete. If you have a large number of records to scan through, see "Searching for a Unit" on page 208.

3 Click on the unit record to highlight it.

(Continued)

4 Go to the `Action` column and click **Delete**.

– OR –

Right-click on the record, then select **Delete** from the popup menu.

A confirmation message displays.

5 Click **Delete**. The system removes the selected record from the unit list.

Manually Synchronizing Your Unit with the Server

Mobile units only

As long as a unit is within signal range of the wireless network, all newly captured event records will automatically transmit to the server without any action on your part. Similarly, the system will automatically push updated hotlists out to the unit, assuming that the required system settings are selected. However, in the event that a unit loses its wireless signal for a prolonged period of time, you may need to manually transfer data to/from the server, as described in this section.

1   Go to ▼ Home Menu and click **Manual Sync**. The Manual Sync page displays.
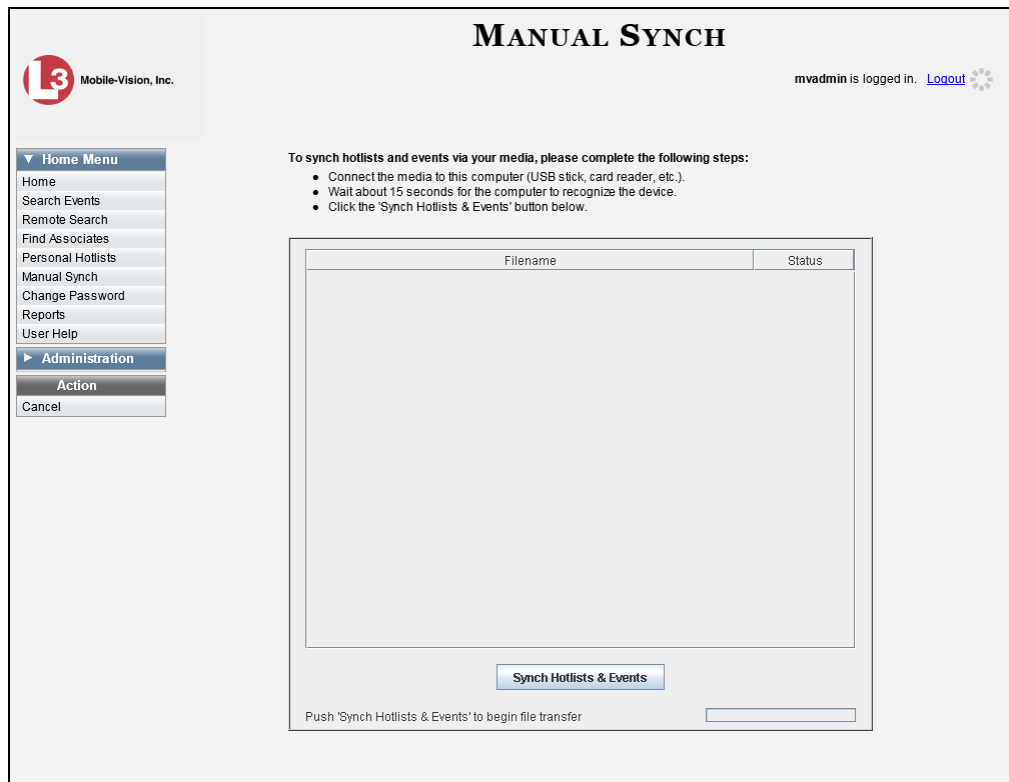
2   If this is your first manual sync, insert a blank, formatted USB drive into a free USB port on your PC.

– OR –

If this is *not* your first manual sync, insert the USB drive that you used for your last manual sync into a free USB port on your PC.

Wait 15 seconds, then proceed to the next step.

3   Click the **Sync Hotlists & Events** button. The system searches the application for updated hotlists that are flagged for unit updates (i.e., hotlists in which the *Update Units* checkbox is selected).

One of two messages display:

Message 1

> **Select an Option**
>
> **?** No formatted device found. Would you like to format an attached device now?
>
> Yes   No   Cancel

Message 2

> **No Files Found**
>
> **i** No event packages found for transfer.
>
> OK
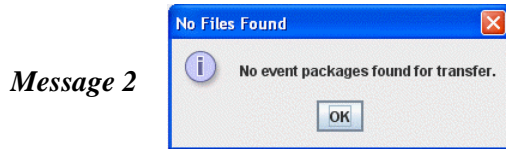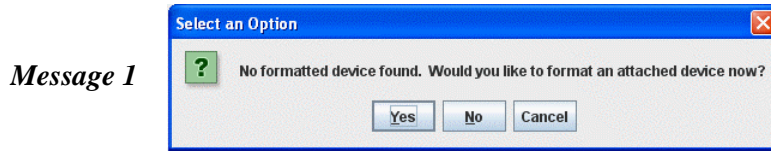
⇒ If *Message 1* displays, proceed to the next step.
⇒ If *Message 2* displays, skip to step 6.

4   Click **Yes**. A drop-down list displays.

> **Select Drive to Format**
>
> **?** Drive to Format:
>
> D:\
>
> OK   Cancel
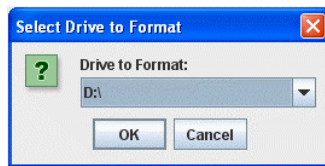
5   Select your USB drive from the drop-down list, then click **OK**. The following message displays.

> **No Files Found**
>
> **i** No event packages found for transfer.
>
> OK

6   Click **OK**. The system copies the hotlist files to your USB drive.

This document consists of general capabilities information that is not defined as controlled technical data under ITAR part 120.10 or EAR

7 Remove the USB drive from your PC.

8 Proceed to the AlertVU unit.

9 Insert the USB drive into a free USB port on the mobile data computer or laptop.

10 Navigate to the **mobile_alpr** folder and double-click on it.

(Continued)

11 Double-click on the **bin** folder.
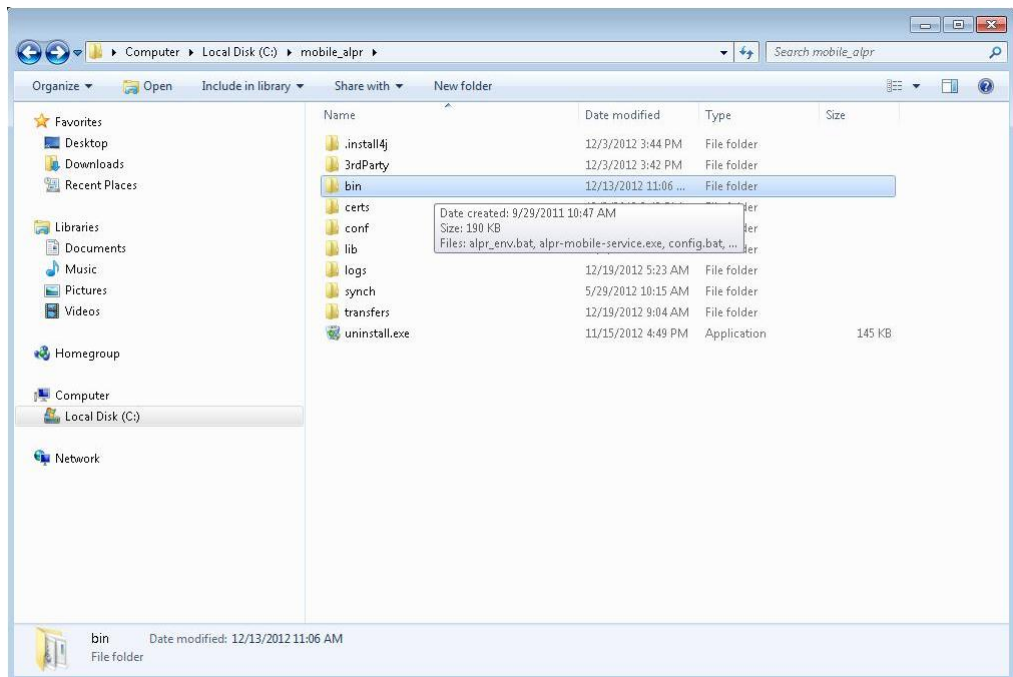
12 Double-click on the **manualSync.bat** file.
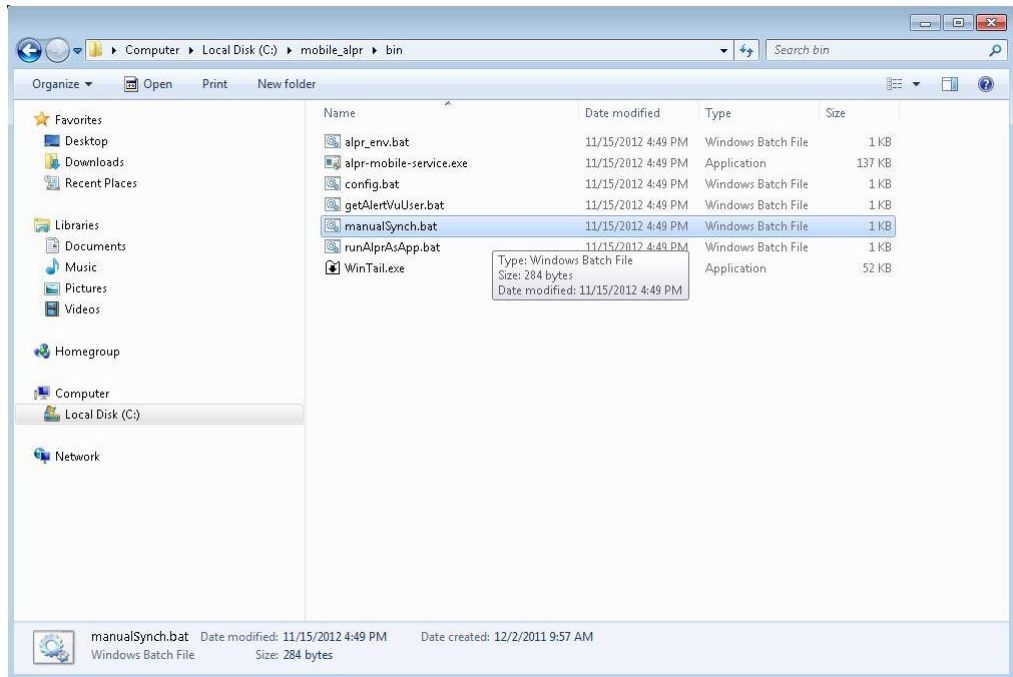
13 Click the **Synch Hotlists & Events** button.
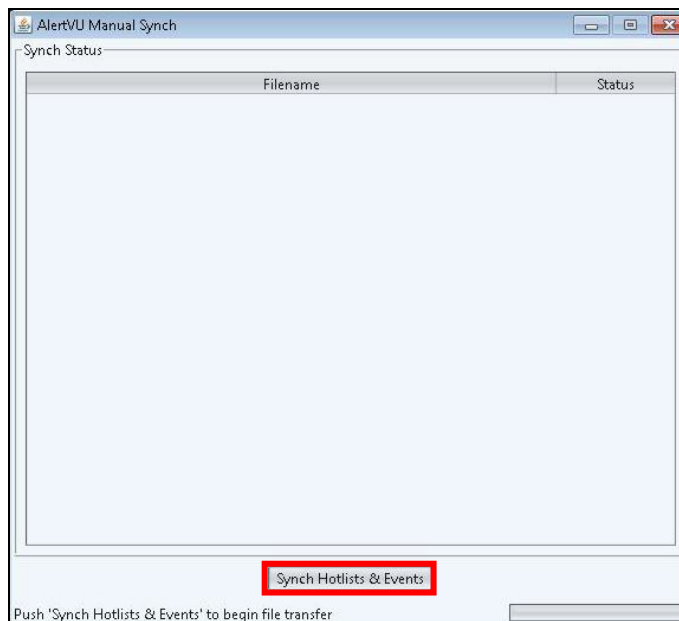
Next, you will see one of three messages.

(Continued)

Message 1
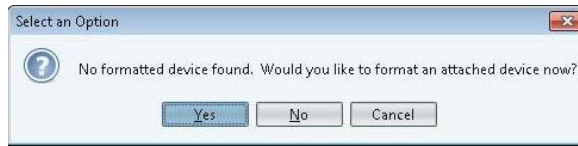
Select an Option

No formatted device found. Would you like to format an attached device now?

Yes   No   Cancel

Message 2

No Files Found

No event files or packages found for transfer.

OK

Message 3

AlertVU Manual Synch

Synch Status

Filename	Status
8b16ef7f-b715-4456-b710-65a019de0db0_1355949009037.xfer	Complete

Synch Hotlists & Events

Complete
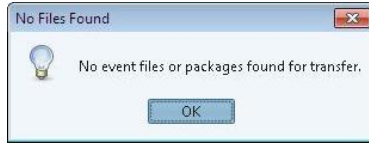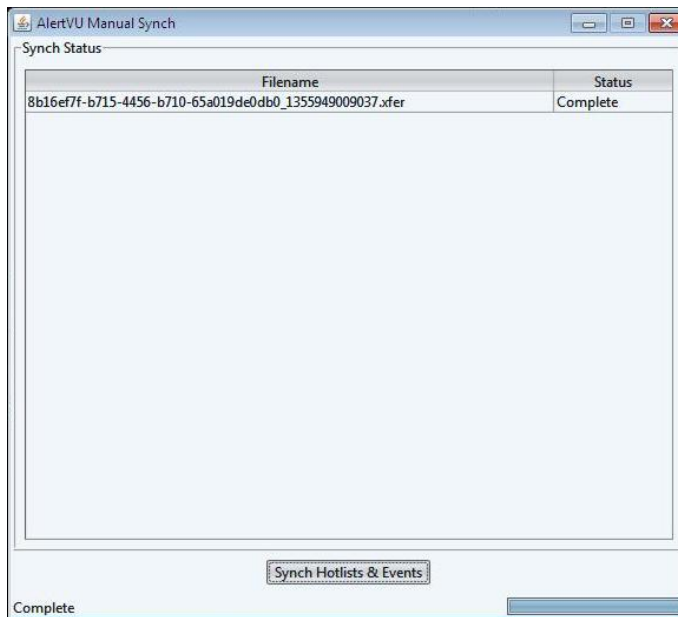
⇒ If *Message 1* displays, proceed to the next step.
⇒ If *Message 2* displays, skip to step 16.
⇒ If *Message 3* displays, skip to step 17.

14 Click **Yes**. A drop-down list displays.

15 Select your USB drive from the drop-down list, then click **OK**.

⇒ If *Message 2* displays, proceed to the next step.
⇒ If *Message 3* displays, skip to step 17.

16 Click **OK**. **End of Procedure**.

17 Remove the USB drive from the mobile data computer or laptop.

18 Return to your precinct and login to the AlertVU Back Office application again.

19 Go to ▼ Home Menu and click **Manual Sync**. The Manual Sync page displays.

Chapter 4: Units
Download Options

L3 Mobile-Vision, Inc.

This document consists of general capabilities information that is not defined as controlled technical data under ITAR part 120.10 or EAR
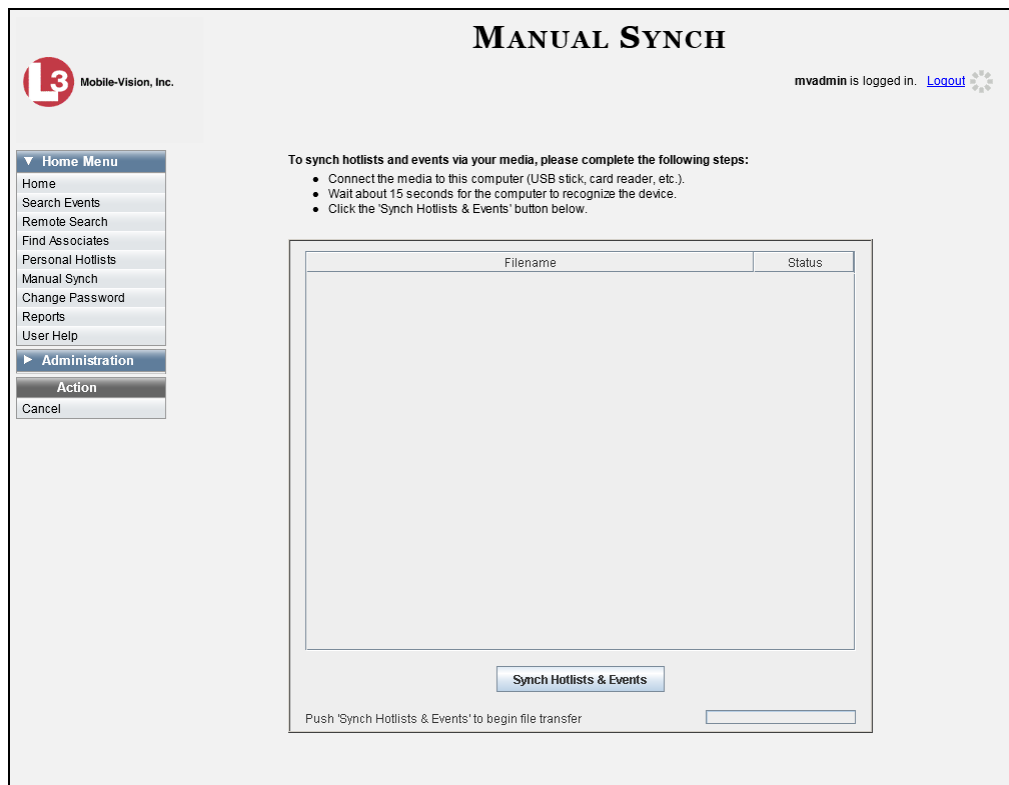
20 Insert the USB drive into an available USB port on your PC. Wait 15 seconds, then proceed to the next step.

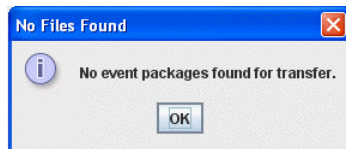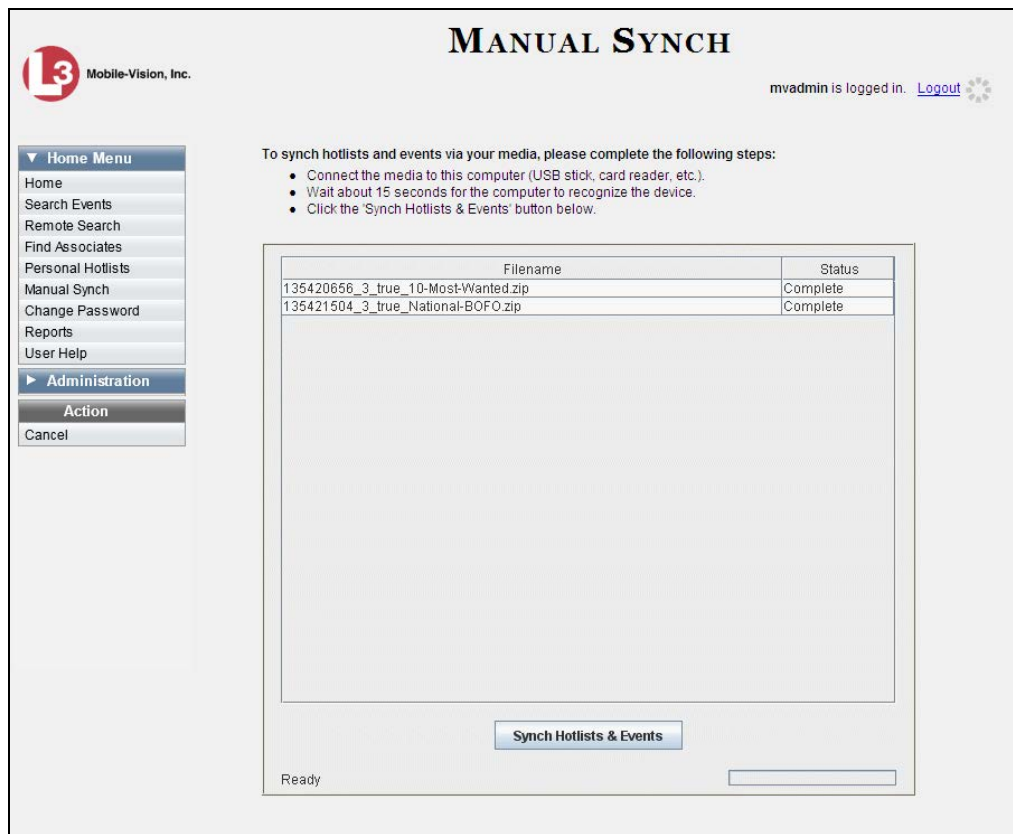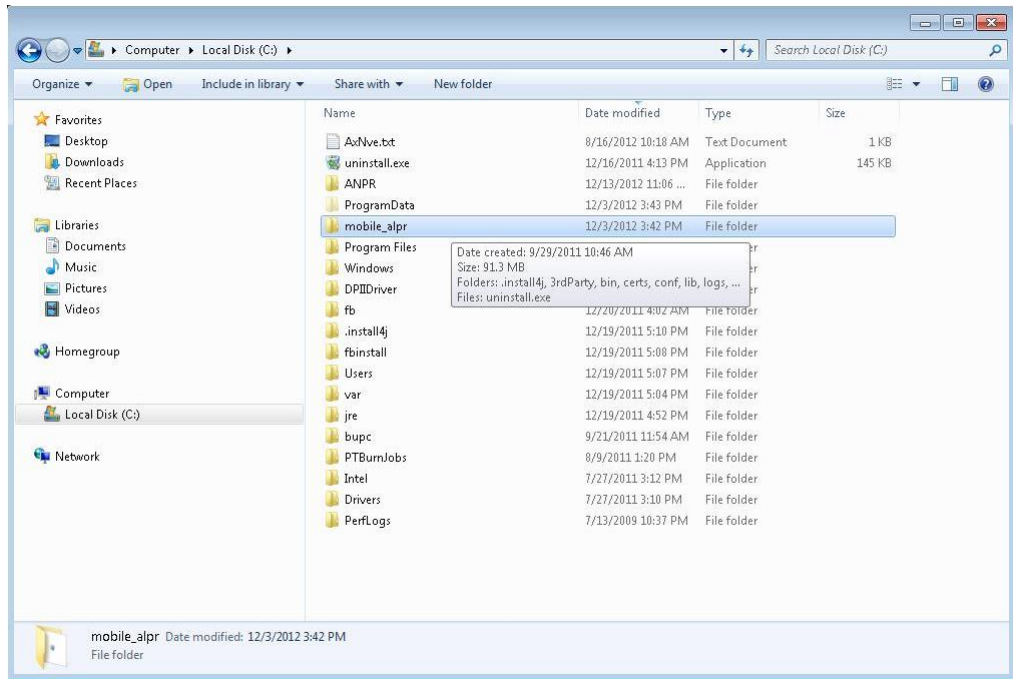21 Click the **Sync Hotlists & Events** button. The system copies the event files to the server.

22 Remove the USB drive from the PC.

Download Options

A "download" is the process by which event records are transferred from your Alert-VU units to the server. At system start-up, your System Implementation Specialist (SIS) will help you select the download settings that are appropriate for your agency. After that, you need only change these settings on an "as needed" basis.

For specific instructions, see:

☐ Changing Download Options, next page
☐ Resetting Download Options, page 225
☐ Updating Hotlists in a Unit, page 227.

Changing Download Options

This section describes how to change download options as needed. For more on AlertVU's download feature, see the previous section.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 Click the **System Settings** tab.

3   Click the **Download Options** tab.

4   Go to the Action column and click **Edit**. The Download Options popup displays.

The Download options are described in the table on the next page.

(Continued)

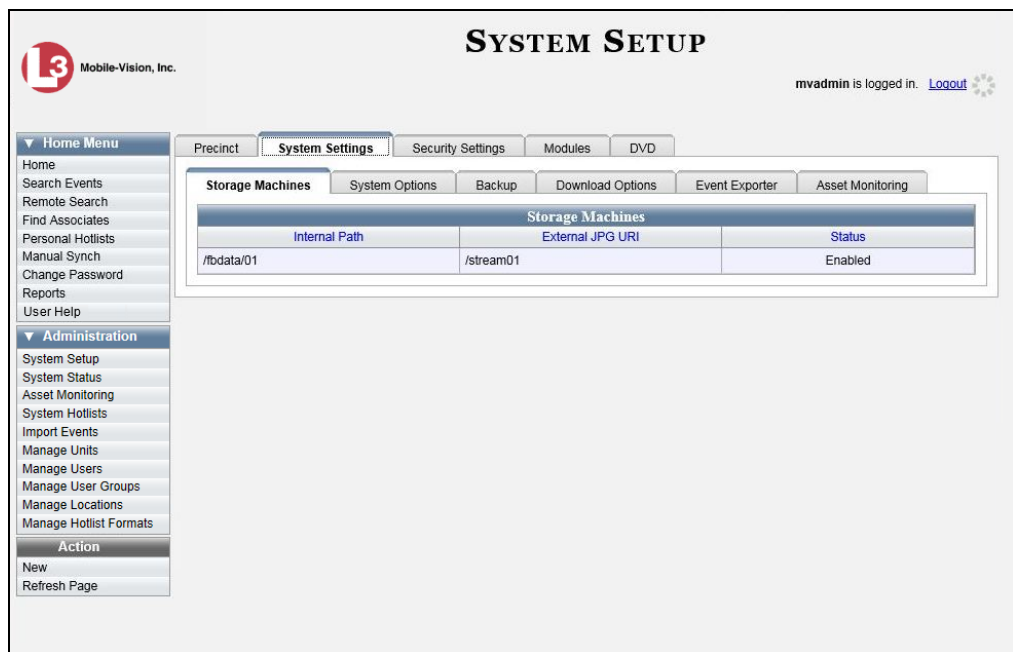| Download Options	
Passive Download Mode	An alternate form of unit-to-server communication in which the in-car or fixed *AlertVU unit*, rather than the *AlertVU server*, initiates communication. With this type of communication, the AlertVU unit *pushes* plate capture data out to the server and *pulls* updated hotlists down from the server.
Discovery Mode	The discovery method that your server will use to initiate event downloads from AlertVU units. There are two discovery methods: *TCP ping* (default) and *UDP Broadcast*. For a description of these methods, see page 207. **WARNING**: Do not change this setting unless instructed to do by your agency's Network Administrator or by an L3 Mobile-Vision Support Representative.
Create Unit Automatically	A checkbox used to indicate whether or not you want the system to automatically create a new unit record whenever it discovers a new AlertVU unit on the network. ☑ Create a new unit record whenever the system discovers a new AlertVU unit ☐ Do *not* create a new unit record whenever the system discovers a new AlertVU unit
Maximum Number of Downloads	The total number of AlertVU units that the server is allowed to download from at the same time.
Web Service Port	The port that the downloader service uses to communicate with the AlertVU units.
UDP Listen Port *(UDP Discovery Method only)*	The port that the downloader service will listen to for incoming UDP announcements from AlertVU units when using UDP Discovery.
Batch Download Timeout	The number of minutes that must elapse before the downloader will disconnect and try downloading an events file again. By limiting this time period, you prevent the system from "hanging" for a long period of time after a failed download attempt. You also prevent the system from downloading a file when there is a connectivity issue between the AlertVU server and the LPR client.

5 Enter/select your desired changes.

6 Click **Save**.

7 If you selected *Passive Download Mode*, you will also need to:

❐ Restart your AlertVU server. If you are not familiar with this procedure, contact L3 Mobile-Vision Support for assistance.

❐ Change the Communication Settings for each of your AlertVU units. See **NOTE** below.
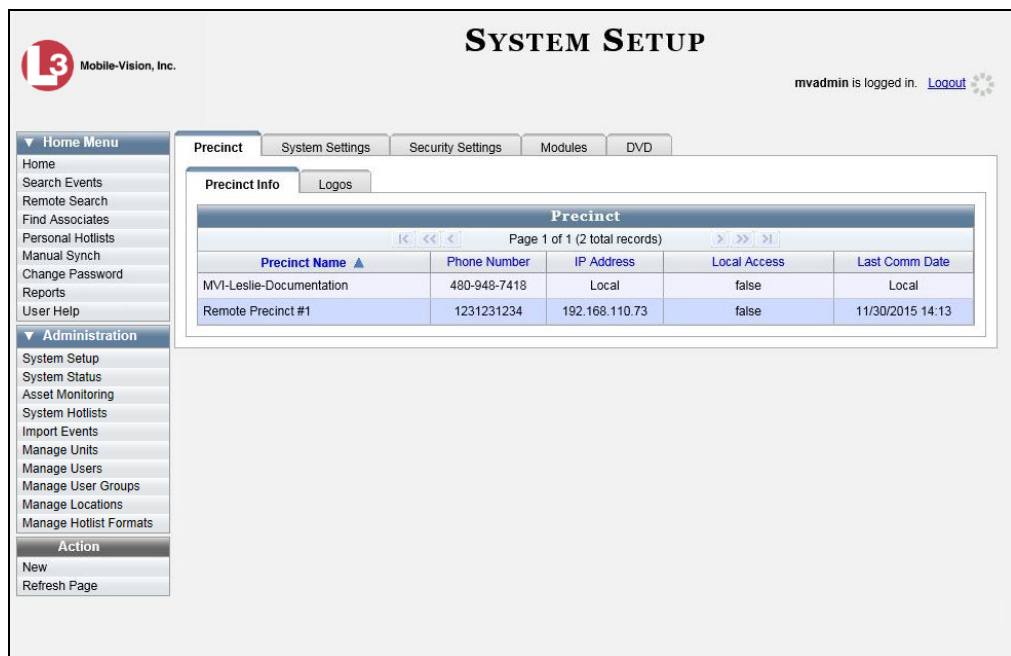
NOTE: Whenever you change the download method to *Passive Download Mode*, you have to reconfigure all of your AlertVU units, as described in "Method 2: Passive Download Mode" in the *AlertVU Mobile Administrator's Guide*. Begin with step 2, "Configure the MDC."

Resetting Download Options

This section describes how to reset your download options to the system defaults. For more on AlertVU's download feature, see "Download Options" on page 221.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 Click the **System Settings** tab.

(Continued)

3   Click the **Download Options** tab.

These options are described in the table on page 224.

4   Go to the │Action│ column and click **Restore Defaults**. A confirmation message displays.

Download options have been reset to factory defaults.

Updating Hotlists in a Unit

This section describes how to retransmit the most recent set of system hotlists from the server to a unit. If the selected unit is within signal range of the wireless network (typical), the update will occur immediately. If the unit is a mobile AlertVU that's currently outside the signal range, the transmission will occur as soon as the unit reenters signal range.

1 Search for the unit you wish to update. (If necessary, review "Searching for a Unit" on page 208.)

2 Click on the unit record to highlight it.

3 Go to the Action column and click **Reset Hotlist**. The following confirmation message displays.

4 Click **Yes**. As soon as this unit is within signal range of the wireless network, the server will retransmit all enabled system hotlists.

Maintaining IP Address Ranges

The system automatically creates a new unit record whenever it discovers a new (i.e., unknown) device on the network. If you selected the **TCP "ping"** discovery method, the system will search for new units within a user-defined range or ranges of IP addresses. This section describes how to maintain these range records.

For specific instructions, see:

❐ Adding an IP Address Range, below
❐ Changing an IP Address Range, 230
❐ Deleting an IP Address Range, page 232.

Adding an IP Address Range

This section describes how to add a new IP address range. These ranges are used in conjunction with the TCP "ping" discovery method, as described in the previous section.

If you prefer to update an *existing* IP address range, see "Changing an IP Address Range" on page 230.

1 Go to ▼ Administration and click **Manage Units**. The Unit Search Results page displays.

2 Go to the `Action` column and click **Manage IP Addresses**. The Manage IP Addresses page displays.

3 Go to the `Action` column and click **New**. The New IP Range popup displays.

4 Enter the first address of your IP range in the *First IP Address* field.

5 Enter the last address of your IP range in the *Last IP Address* field. You only have to enter the last segment of this address, as the system will automatically populate the first three segments.

NOTE: Each IP range is limited to a maximum of 256 addresses in the last segment, numbered 0 through 255.

6 Click **Save**.

Changing an IP Address Range

This section describes how to change an existing IP address range. These ranges are used in conjunction with the TCP "ping" discovery method, as described in "Maintaining IP Address Ranges" on page 228.

To create an entirely *new* IP address range instead, see "Adding an IP Address Range" on page 228.

1 Go to ▼ Administration and click **Manage Units**. The Unit Search Results page displays.

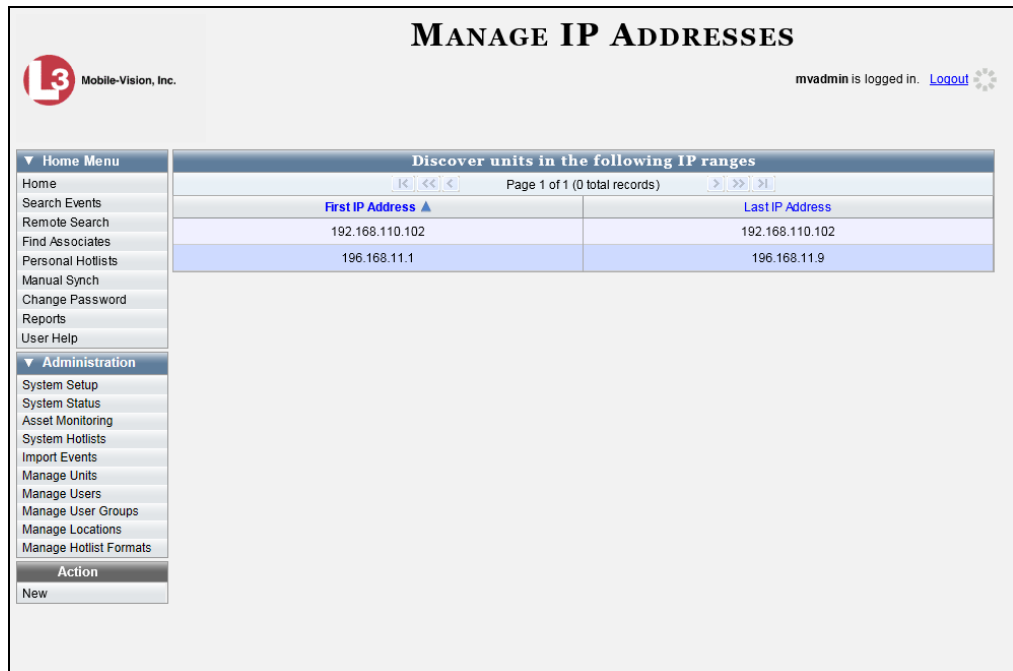**2** Go to the Action column and click **Manage IP Addresses**. The Manage IP Addresses page displays.

3 Click on the record you wish to update.

4 Go to the Action column and click **Edit**. The Edit IP Range popup displays.

(Continued)

Edit IP Range

First IP Address: 196.168.11.1

Last IP Address: xxx.xxx.xxx. 9
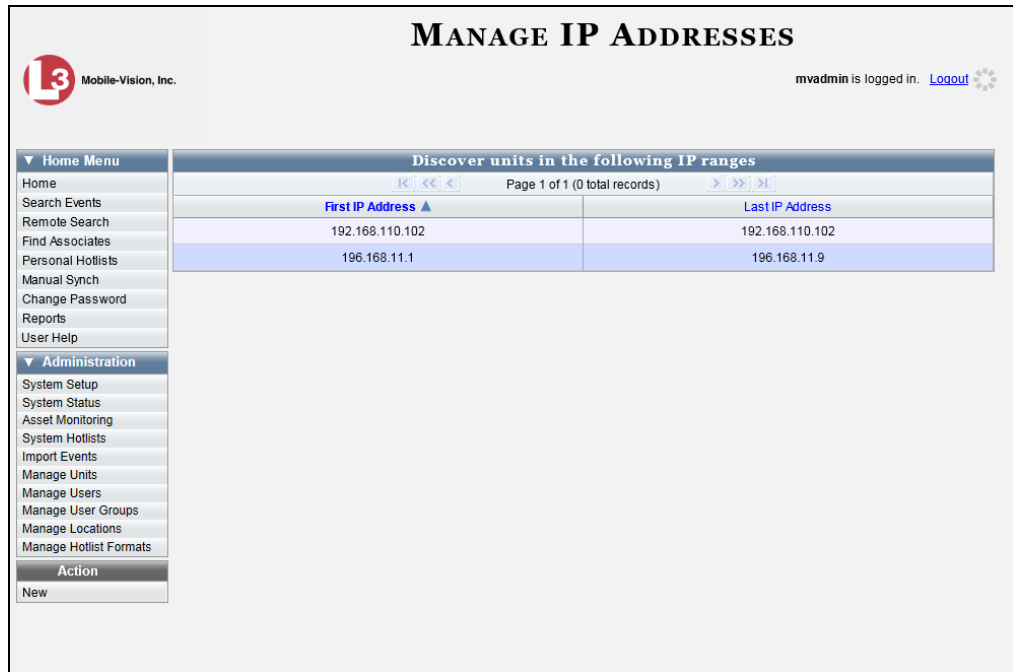
Save   Cancel

5 Enter your changes in the appropriate field(s).

6 Click **Save**.

Deleting an IP Address Range

This section describes how to delete an existing IP address range. You can only perform this procedure if there are no unit records that have an IP address within the selected range.
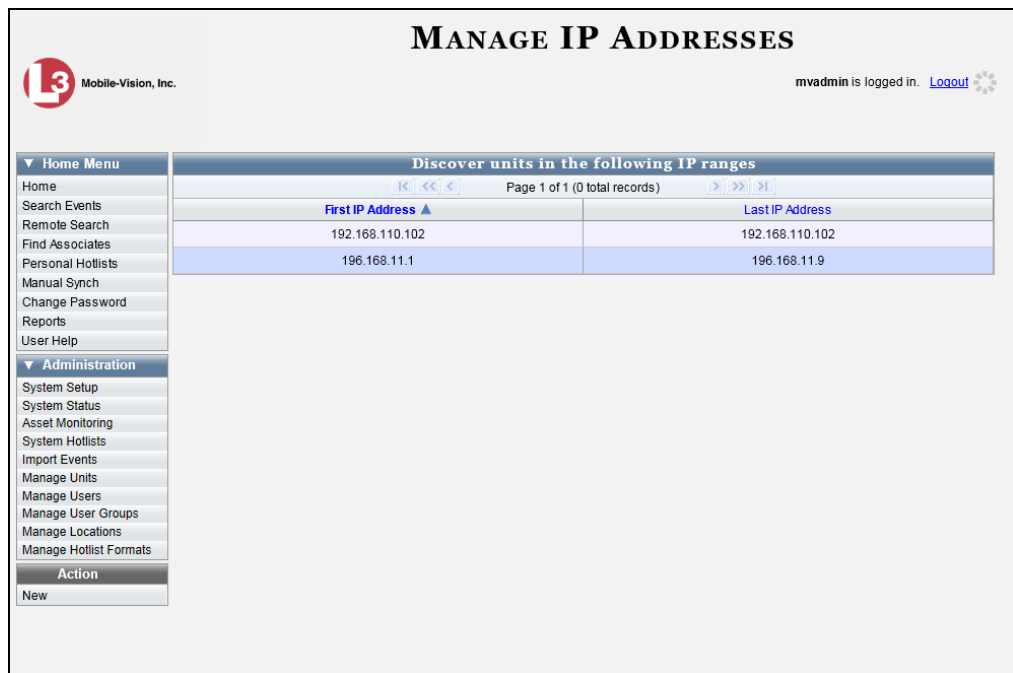
1 Go to ▼ Administration and click **Manage Units**. The Unit Search Results page displays.

UNIT SEARCH RESULTS

admin is logged in.   Logout

Unit Name ▲	Last Known IP	Serial Number	Status	Version
E Doubletree / N Scottsdale Rd	166.241.188.115	4475c678-eb8b-45ab-b056-3be89dce1fe0	Enabled	3.1.3
E Doubletree Ranch / Tatum	166.241.188.123	c9fd1f8e-d32a-475f-a9c1-56bc080b9fc6	Enabled	3.1.3
E Lincoln / N 36th - EB Lincoln	166.241.188.118	91ba04b8-c89e-4994-a175-ea5b279edb5e	Enabled	3.1.3
E Lincoln / N 36th - SB 36th	166.241.188.121	0021cc3b-edc8-47a5-ba5b-254a47292546	Enabled	3.1.3
E Lincoln / Scottsdale Rd	166.241.188.116	d4507921-aa36-4847-89d3-83c23cb53131	Enabled	3.1.3
ESTANFORDATN40T	166.241.171.215	5f93a29a-65fa-400f-99cc-7e17abace346	Enabled	3.1.3
E Stanford / N 32nd	166.241.188.120	4a4c5824-69b0-425c-8042-d3370d44aebf	Enabled	3.1.3
E Stanford / N 40th	166.241.171.215	7f6dab9e-2070-4058-8fcd-80236f0516bc	Enabled	3.1.3
McDonald / Scottsdale	166.241.188.113	0a5d2f9f-01e8-422d-b3a4-877ac5b8dd3b	Enabled	3.1.3
N 40th S of Stanford	166.241.188.122	96556f31-7861-4a18-b313-00e356549421	Enabled	3.1.3
N 64th / Camelback	166.241.171.214	51a9cf99-dbeb-4d01-8cd3-53c095fd102f	Enabled	3.1.3
Tatum / McDonald EB McDonald	166.241.171.213	ebf44d6e-744d-4d4b-aaa4-87dc3799ae12	Enabled	3.1.3
Tatum / McDonald - NB Tatum	166.241.188.114	e71a53bf-38d3-4650-a289-6878fc1551b4	Enabled	3.1.3
Tatum / Shea	166.241.188.117	2c431277-4ac0-40c7-bfd4-8dfbec7b25a6	Enabled	3.1.3
Unit 45	10.5.45.100	c0206805-5709-4407-8f79-e74fca6ecb45	Enabled	3.1.3
Unit 46	10.5.46.100	6b065529-b430-45e4-a0ac-d1e7e1e2062e	Enabled	3.1.3
Unit 48	10.5.48.100	f54adbde-4cfe-4d43-b764-759d6fe72164	Enabled	3.1.3
Unit 49	10.5.49.101	4749f478-d59d-4038-ac40-018e26da94fa	Enabled	3.1.3
Unit 50	10.5.50.102	767c2fde-373c-415d-972d-07eb50718709	Enabled	3.1.3
Unit 51	10.5.51.100	c9c73822-4717-4126-b42b-6d9d15085769	Enabled	3.1.3

2 Go to the Action column and click **Manage IP Addresses**. The Manage IP Addresses page displays.

3 Click on the record you wish to delete.

4 Go to the Action column and click **Delete**. The selected record is removed from the list of IP ranges.

Viewing Your Units' Status

This section describes to view up-to-date information on your AlertVU units, including:

1 The date and time at which each unit last communicated with the AlertVU server. See *Last Communicated* column.

2 The date and time at which each unit last captured an event record. See *Last Event Captured* column.

3 The GPS coordinates for each unit's last known location. See *Last GPS Location* column.

4 The total number of events captured by each unit in the last 24 hours, 7 days, and 30 days.

You must have the *Asset Monitoring* permission to perform this task.

⇒ Go to ▼ Administration and click **Asset Monitoring**. The Asset Monitoring page displays.

By default, the color of the *Last Communicated* and *Last Event Captured* fields change from black to yellow after three hours have elapsed since the displayed date/time. After 24 hours, they change from yellow to red. These settings are the same for both Mobile and Fixed units, but you can customize this display option if desired. For more information, see the next section, "Customizing the Asset Monitoring Page."

This document consists of general capabilities information that is not defined as controlled technical data under ITAR part 120.10 or EAR

Customizing the Asset Monitoring Page

This section describes how to change the number of hours that must elapse before the text color for the date/time fields on the Asset Monitoring page change from black to yellow or red. There are two date/time fields:

❒ *Last Communicated*. Displays the date and time at which the unit last communicated with the AlertVU server

❒ *Last Event Captured*. Displays the date and time at which the unit last captured an event record

1 Go to **▼ Administration** and click **System Setup**. The System Setup page displays.

2 Click the **System Settings** tab.

(Continued)

3 Click the **Asset Monitoring** tab. The Asset Monitoring page displays.

4 Go to the Action column and click **Edit**. The Edit Asset Monitoring Setting form displays.

L3 Mobile-Vision, Inc.

The settings on this form are described in the following table.

Edit Asset Monitoring Settings	
Setting	**Description**
Enable Alerting	If a user has the *Asset Monitoring* permission, then when this checkbox is selected, the system will send an alert to their *Inbox Messages* list and regular email[*] whenever a unit's *Last Communicated* field value turns red. For example: There has been no communication between the AlertVu server and unit, Unit 54, in the last 24 hour(s)
Fixed Unit Last Comm Red Indicator (in hours)	For all AlertVU fixed units, change the color of the text in the *Last Communicated* field from yellow to red after X number of hours have elapsed since the displayed date/time.
Fixed Unit Last Comm Yellow Indicator (in hours)	For all AlertVU fixed units, change the color of the text in the *Last Communicated* field from black to yellow after X number of hours have elapsed since the displayed date/time.
Fixed Unit Last Event Red Indicator (in hours)	For all AlertVU fixed units, change the color of the text in the *Last Event Captured* field from yellow to red after X number of hours have elapsed since the displayed date/time.
Fixed Unit Last Event Yellow Indicator	For all AlertVU fixed units, change the color of the text in the *Last Event Captured* field from black to yellow after X number of hours have elapsed since the displayed date/time.

(Continued)

---

[*]   If you previously configured the system to forward system messages to your regular mailbox

Edit Asset Monitoring Settings (cont'd)	
Setting	**Description**
Mobile Unit Last Comm Red Indicator (in hours)	For all AlertVU mobile units, change the color of the text in the *Last Communicated* field from yellow to red after X number of hours have elapsed since the displayed date/time.
Mobile Unit Last Comm Yellow Indicator (in hours)	For all AlertVU mobile units, change the color of the text in the *Last Communicated* field from black to yellow after X number of hours have elapsed since the displayed date/time.
Mobile Unit Last Event Red Indicator (in hours)	For all AlertVU mobile units, change the color of the text in the *Last Event Captured* field from yellow to red after X number of hours have elapsed since the displayed date/time.
Mobile Unit Last Event Yellow Indicator (in hours)	For all AlertVU mobile units, change the color of the text in the *Last Event Captured* field from black to yellow after X number of hours have elapsed since the displayed date/time.

5 To send alert messages to the *Inbox Messages* list and regular email[*] of all users who have the *Asset Monitoring* permission (see *Enable Alerting* on the previous page), select the *Enable Alerting* checkbox. Otherwise proceed to the next step.

6 To increase or decrease the number of hours that must elapse before the date/time fields change color (see descriptions in the previous table), enter your changes in the appropriate fields.

7 Click **Save**.

---

[*]   If you previously configured the system to forward system messages to your regular mailbox

5   Backups

Your AlertVU Back Office software interfaces with a robotic disc burner. L3 Mobile-Vision sells two types of burners: the *Bravo*, a stand-alone unit, and the *Rimage*, a combination disc burner/computer. Rimage units can burn CDs, DVDs, and Blu-Ray discs. Most Bravo units can burn CDs and DVDs. A few higher-end Bravos can burn Blu-Ray discs as well.

If archiving is enabled, the system uses your disc burner to create periodic backup discs (i.e., archives) that contain your event and hotlist records. This process occurs automatically without any action on your part. The automatic archive discs that the disc burner generates are called *Certified Backup Discs*. Because the process of burning DVDs is resource-intensive, one computer is dedicated to this task. This computer is referred to as a *Backup PC*. If you are using a *Bravo* burner, then the backup PC is a separate computer workstation connected to the disc burner. If you are using a *Rimage* burner, the Backup PC refers to the computer component of the Rimage.

If your agency has more than one storage server, you can connect those servers to a single Backup PC. However, if your agency has more than one Bravo DVD burner, you must connect each DVD burner to a separate Backup PC. Any time you add a new Backup PC/DVD Burner to your setup, you will have to enter a new backup PC record, as described on the next page.

Your System Implementation Specialist (SIS) will initially install and configure your DVD burner(s) and Backup PC(s) during implementation. However, you may occasionally need to perform tasks related to this device, such as viewing the Backup PC Status page, which logs any Backup PC errors that may occur.

For more information, see:
- ❒ Adding a Backup PC, next page
- ❒ Changing a Backup PC, page 243
- ❒ Deleting a Backup PC, page 245
- ❒ Viewing the Backup PC Status Page, page 247
- ❒ Turning the Backup Feature On/Off, page 249
- ❒ Changing the Maximum Number of Days Between Backups, page 252
- ❒ Customizing Disc Labels, page 254
- ❒ Viewing the Certified Backup Discs List, page 256.

Adding a Backup PC
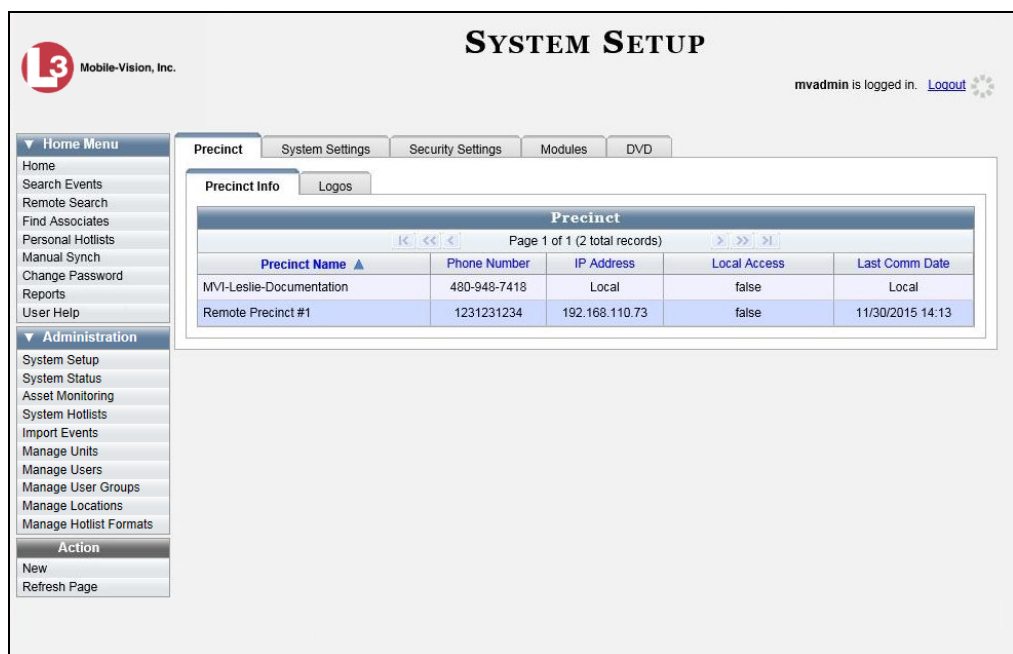
This section describes how to enter a new record for a Backup PC. This information will be used to control your robotic DVD burner. For more on Backup PCs and how they are used in AlertVU, see the previous section.

Regarding Bravo units

Every Bravo DVD burner has one or two *input* bins and one *output* bin. The *input* bin is where the blank DVDs go. The *output* bin is where the robotic DVD burner places the completed DVDs.

There are two modes used to configure a Bravo DVD burner: *regular* mode and *kiosk* mode. In *regular* mode, the DVD burner's right and left bins are used as the *input* and *output* bins, respectively. In *kiosk* mode, both the left and right bins are used as *input* bins, and a center "catch" tray is used as the *output* bin. If you prefer to configure your DVD burner in *kiosk* mode, ask an L3 Mobile-Vision Technical Support Engineer to assist you.

1 Contact L3 Mobile-Vision Service at 800-336-8475 (when prompted, select the phone option for "Service", then "Back Office"). A Technical Support Engineer will assist you with the preliminary setup tasks required to add a new burning station. This step is sometimes referred to as "pre-staging."

2 Obtain an IP address for the new Backup PC. If the Backup PC will be connected to the Mobile-Vision network, your TSE will provide you with this address. If the Backup PC will be connected to your agency's network, your agency's Network Specialist will provide you with this address.

3 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

4   Click the **System Settings** tab.

5   Click the **Backup** tab.

6   Make sure that the **Backup PC** tab is selected, as pictured above. The columns on this form are described in the table on the next page.

Backup PC	
Column	**Description**
Name	The name of this Backup PC.
IP	The IP address of this Backup PC.
Disk Type	The type of disc that will be used to create your backups: DVDR .... DVD single layer disc DVDRDL .... DVD dual layer disc BD .... Blu-ray single layer disc[*] BDDL.............. Blu-ray dual layer disc[*]

7 Go to the Action column and click **New**. The New Backup PC popup displays.

8 Enter a descriptive name for this backup PC in the *Name* field.

9 Enter the IP Address for this backup PC in the *IP Address* field.

10 If this record is for a *Bravo* burner, proceed to the next step.

– OR –

If this record is for a *Rimage* burner, skip to step 12.

11 If you plan to use the DVD burner in *kiosk* mode (see description on page 240), proceed to the next step.

– OR –

If you plan to use the DVD burner in *regular* mode (see description on page 240), keep the *Left bin (bin 2)* field set to **OUTPUT**, then skip to step 13.

---

[*] Requires a Blu-ray burner

L3 Mobile-Vision, Inc.

12 Go to the *Left bin (bin 2)* field and select the type of disc that you plan to place in the DVD burner's *left* bin (Bravo units) or bin 2 (Rimage units):

DVDR.............. DVD single layer discs
DVDRDL .... DVD dual layer discs
BD .... Blu-ray single layer discs
BDDL.............. Blu-ray dual layer discs

13 Go to the *Right bin (bin 1)* field and select the type of disc that you plan to place in the DVD burner's *right* bin (Bravo units) or bin 1 (Rimage units), as listed in step 12 above.
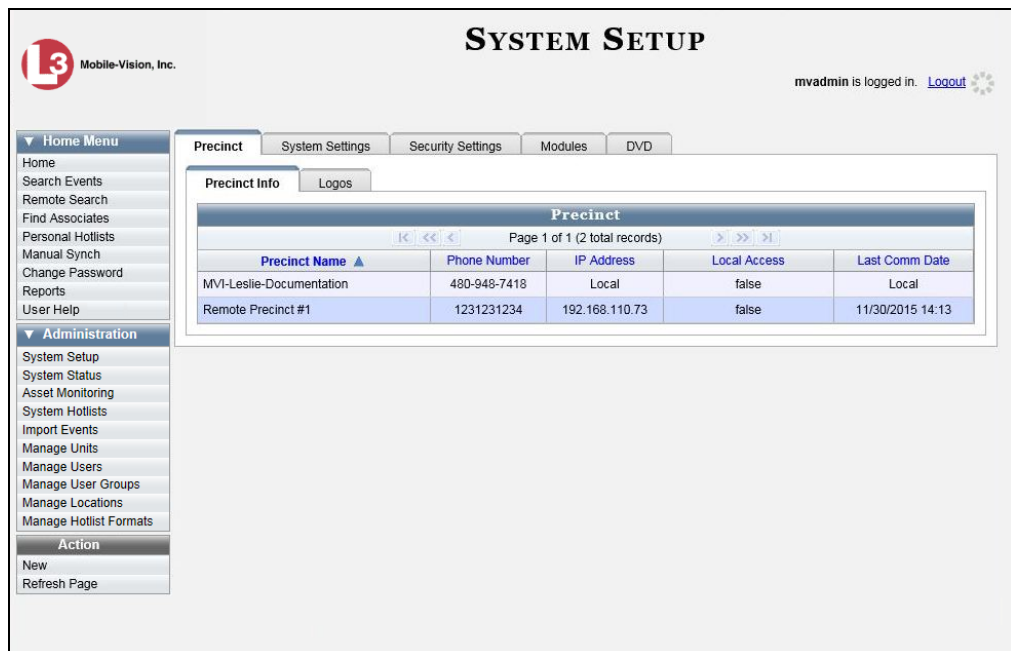
After you select a value from the drop-down list, the system will automatically populate the *Archive* field.

14 Click **Save**. The new Backup PC record displays on the Backup PC list.

Changing a Backup PC

This section describes how to update an existing backup PC record. If, for example, you decide to switch from using *single* layer DVDs to *dual* layer DVDs, you'd need to update the associated backup PC record.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 Click the **System Settings** tab.

3 Click the **Backup** tab.

4 Make sure that the **Backup PC** tab is selected, as pictured above. For a description of the columns on this form, see the table on page 242.

5 Click on the record you wish to update.

Chapter 5: Backups
Deleting a Backup PC

L3 Mobile-Vision, Inc.

This document consists of general capabilities information that is not defined as controlled technical data under ITAR part 120.10 or EAR

6 Go to the Action column and click **Edit**.

– OR –

Right-click on the record, then select **Edit** from the popup menu.

The Edit Backup PC popup displays.

7 Enter/select your changes in the appropriate field(s), then click **Save**.

Deleting a Backup PC

This section describes how to delete an existing backup PC record. Perform this task *after* a backup PC/DVD burner has been decommissioned, or as directed by an L3 Mobile-Vision Technical Support Engineer.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 Click the **System Settings** tab.

3 Click the **Backup** tab.

4 Make sure that the **Backup PC** tab is selected, as pictured above.

5 Click on the record you wish to delete.

6 Go to the Action column and click **Delete**.

– OR –

Right-click on the record, then select **Delete** from the popup menu.

A confirmation message displays.

Confirm Delete

Delete this backup pc? Archives

Yes   No

7 Click **Yes**. The selected record is removed from the system.

Viewing the Backup PC Status Page

This section describes how to view the current status of a backup PC workstation.

1 Go to **▼ Administration** and click **System Status**. The System Status page displays.

2 Click the **Backup PC** tab. The current status of your backup PC displays. If there are any error messages, they will display here.

(Continued)

The columns on the Backup PC page are described below.

Backup PC	
Column	**Description**
Name	The name of this Backup PC
State	The current state of this Backup PC: ▪ READY. Backup PC is up and running; DVD burner is ready to burn ▪ ERROR. A problem has occurred that is preventing the Backup PC from processing burn request(s). ▪ OFFLINE. The Backup PC and/or robotic DVD burner is turned off.
Error Message	A description of the error that has occurred, if applicable. You can fix many of these problems yourself (for example, *The color cartridge is in the black cartridge holder*, or *The cover on the unit has been open for an extended period of time*).
Discs	The number of discs that are left in the DVD burner's input bin. When this number gets low, you need to add more discs to the input tray.
Ribbon Count *(Rimage units only)*	The exact number of disc labels that can still be printed using the Rimage's heat transfer printing mechanism.
Black Color % *(Bravo units only)*	The percentage of remaining ink left in the Bravo's ink jet cartridges.
Version	*This field is used by L3 Mobile-Vision employees only.*

Turning the Backup Feature On/Off

This section describes how to enable or disable the backup feature. If this feature is *enabled*, the system will automatically burn an archive disc (i.e., *Certified Backup Disc*) whenever there are enough event files to fill a disc *or* whenever a certain number of days has elapsed[*], whichever comes first.

If the Backup feature is *disabled*, the system will not archive any events prior to removing them from the server.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 Click the **System Settings** tab.

(Continued)

---

[*] According to the preset *Maximum Days Between Archives*. See next section for more information on this setting.

3 Click the **Backup** tab.

4 Click the **Backup Options** tab.

SYSTEM SETUP

5 Go to the Action column and click **Edit**. The Edit Backup Options popup displays.

6 Go to the *Backup Mode* drop-down list and select a backup setting: **ALL** (perform backups) or **NONE** (do *not* perform backups).

7 Click **Save**.

Changing the Maximum Number of Days Between Backups

This section describes how to change the maximum number of days that you wish to elapse between automatic archives. The system default is 30 days.

1 Go to **▼ Administration** and click **System Setup**. The System Setup page displays.

2 Click the **System Settings** tab.

3 Click the **Backup** tab.

4 Click the **Backup Options** tab.

5 Go to the Action column and click **Edit**.

(Continued)

The Edit Backup Options popup displays.

Edit Backup Options

Backup Mode: NONE ▼ ❷

Maximum Days Between Archives: 30 ❷

Save   Cancel
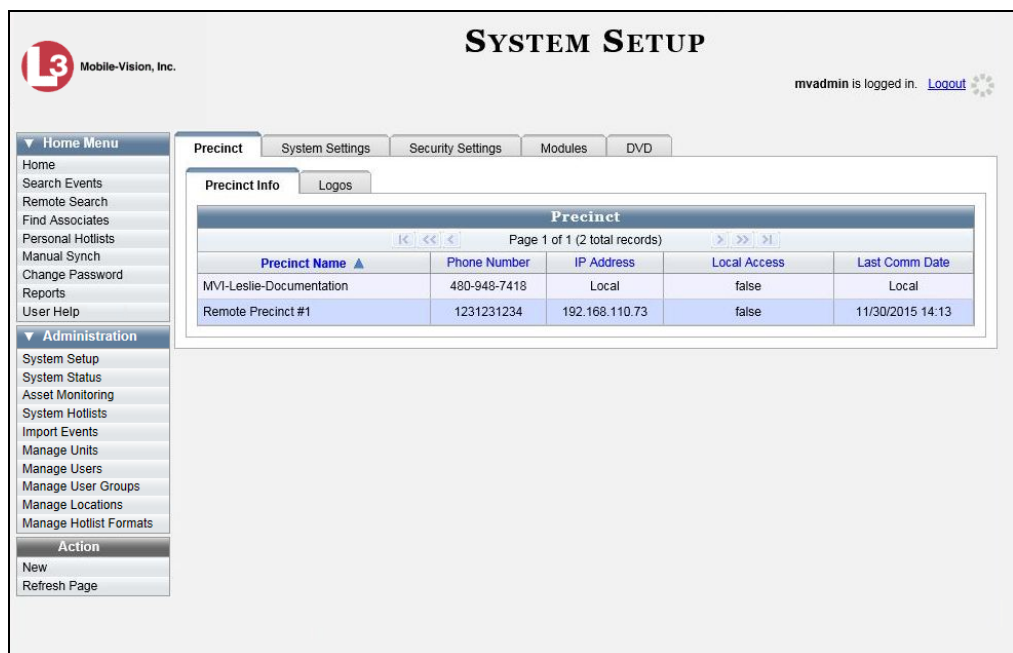
6 Enter a new number in the *Maximum Days Between Archives* field.

7 Click **Save**.

Customizing Disc Labels

This section describes how to customize the labels for your system-generated archive discs, also referred to as *Certified Backup Discs*.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

SYSTEM SETUP

mvadmin is logged in.   Logout

▼ Home Menu
Home
Search Events
Remote Search
Find Associates
Personal Hotlists
Manual Synch
Change Password
Reports
User Help

▼ Administration
System Setup
System Status
Asset Monitoring
System Hotlists
Import Events
Manage Units
Manage Users
Manage User Groups
Manage Locations
Manage Hotlist Formats

Action
New
Refresh Page

| Precinct | System Settings | Security Settings | Modules | DVD |

| Precinct Info | Logos |

Precinct

|◀ ◀◀ ◀   Page 1 of 1 (2 total records)   ▶ ▶▶ ▶|

Precinct Name ▲	Phone Number	IP Address	Local Access	Last Comm Date
MVI-Leslie-Documentation	480-948-7418	Local	false	Local
Remote Precinct #1	1231231234	192.168.110.73	false	11/30/2015 14:13

2 Click the **DVD** tab. A mock-up of the DVD label displays.

L3 Mobile-Vision, Inc.
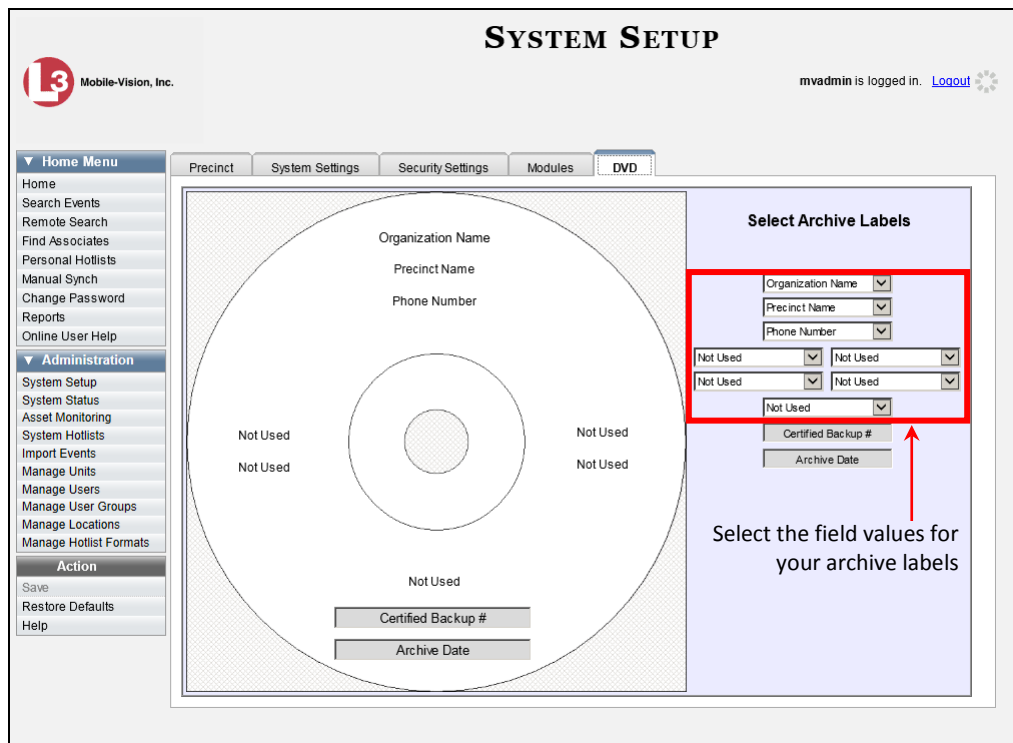
3 Using the drop-down lists in the *Select Archive Labels* column, select or enter values for each section of the DVD label. Note that the drop-down lists are in the exact same order and layout as the label itself.

To enter a *custom* field, select **Administrator Static** from a drop-down list, then enter a field value in the space provided (e.g., *For Internal Use Only*).
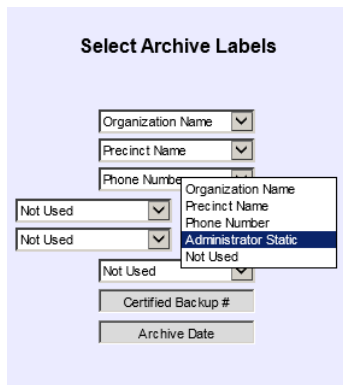
NOTE: Two fields on the label—*Certified Backup #* and *Archive Date*—are generated automatically by the system.
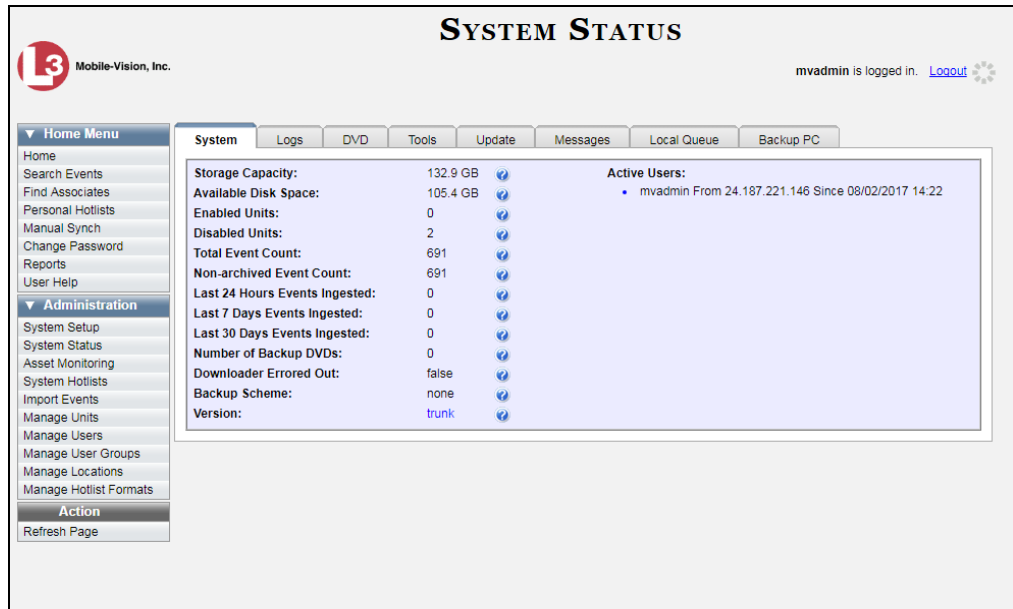
4 Once you've finished customizing the label, go to the Action column and click **Save**.

Viewing the Certified Backup Discs List

This section describes how to view a list of the following:

❒   All of the Certified Backup Discs that the system has ever burned.
❒   All of the pending burn jobs for Certified Backup Discs. These are the archive discs that are *waiting* to be burned.

1   Go to ▼ Administration and click **System Status**. The System Status page displays.

SYSTEM STATUS

Mobile-Vision, Inc.   mvadmin is logged in.   Logout

▼ Home Menu
Home
Search Events
Find Associates
Personal Hotlists
Manual Synch
Change Password
Reports
User Help

▼ Administration
System Setup
System Status
Asset Monitoring
System Hotlists
Import Events
Manage Units
Manage Users
Manage User Groups
Manage Locations
Manage Hotlist Formats

Action
Refresh Page
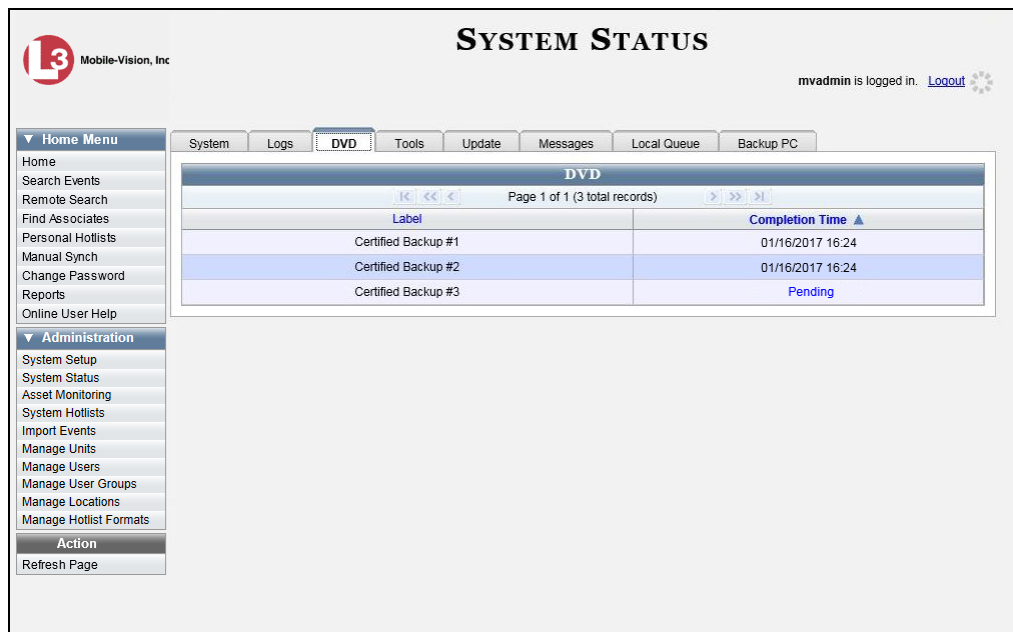
| System | Logs | DVD | Tools | Update | Messages | Local Queue | Backup PC |

Storage Capacity:	132.9 GB	
Available Disk Space:	105.4 GB	
Enabled Units:	0	
Disabled Units:	2	
Total Event Count:	691	
Non-archived Event Count:	691	
Last 24 Hours Events Ingested:	0	
Last 7 Days Events Ingested:	0	
Last 30 Days Events Ingested:	0	
Number of Backup DVDs:	0	
Downloader Errored Out:	false	
Backup Scheme:	none	
Version:	trunk	

Active Users:
• mvadmin From 24.187.221.146 Since 08/02/2017 14:22

2   Click the **DVD** tab. If the backup function is enabled, a list of completed and pending backup discs will display.

The columns on the DVD Backups list are described in the following table.

Column	Description
Label	The number of the Certified Backup Disc. Disc numbers are assigned automatically by the system in sequential order, beginning with no. 1. The highest number on this list is the most recent disc burned.
Completion Time	The date and time at which the robotic DVD burner finished burning the Certified Backup Disc. If a disc has not been burned yet, the word **Pending** will display here.

6 Utilities

This chapter describes how to perform those system maintenance procedures that are not covered in any other part of this guide. Perform these procedures as needed in response to agency needs, user requests, and/or inbox messages received.

For more information, see:

Viewing the System Logs

This section describes how to view the system logs. These logs track:

❒ User activities, such as plate searches and hotlist edits.
❒ System activities, such as hotlist alert notifications.

1 Go to ▼ Administration and click **System Status**. The System Status page displays.

(Continued)

2 Click the **Logs** tab. The system logs display.

The columns on this form are described in the following table.

L3 Mobile-Vision, Inc.

System Logs	
Column	**Description**
Date	The date and time at which this activity occurred.
User	The User ID of the individual who either performed this activity *or* was involved in this activity, such as a user who received an alert notification.
IP Address	The IP address of the machine on which this activity occurred. If this log is associated with a system activity, such as an alert notification, this field will be blank.
Event	The type of activity that occurred.
Details	A detailed description of the activity.

3 To narrow the logs list to those activities associated with a specific user, select a user name from the *User* drop-down list.

4 To narrow the logs list to those activities whose description contains specific text (such as a plate number), enter that text in the *Details* field.
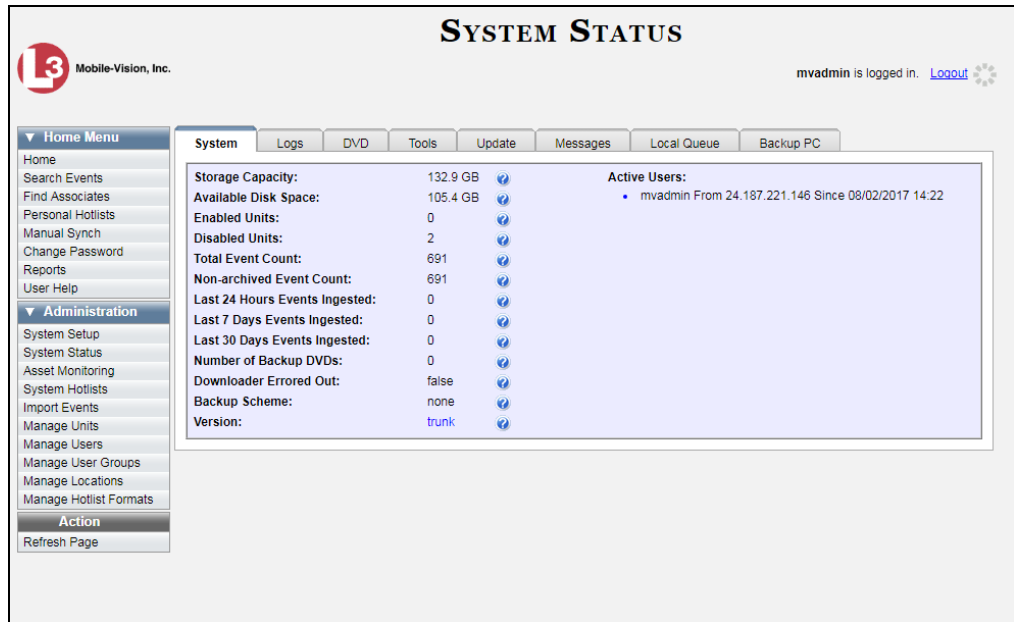
HINT: To display all activities that involve the creation of new records, enter the word **created** in the *Details* field. To display all activities that involve changes to existing records, enter the word **edited** in the *Details* field.

Viewing the System Status Page

This section describes how to view the system status messages. This page provides important information and statistics on events, units, and users. It also indicates what version of AlertVU Back Office you are running.

1 Go to ▼ Administration and click **System Status**. The System Status page displays.

2 If it is not already selected, click the **System** tab, as pictured above. The statuses on this page are described below.

System Status Settings	
Field	**Description**
Storage Capacity	The total amount of usable space allotted for storing events and hotlists on the server.
Available Disk Space	The amount of storage space that is currently available to store events and hotlists.
Enabled Units	The number of active AlertVU units. Active units have a status of *Enabled*.*
Disabled Units	The number of disabled AlertVU units. Disabled units have a status of *Disabled*.*
Total Event Count	The total number of searchable events on the server.

---
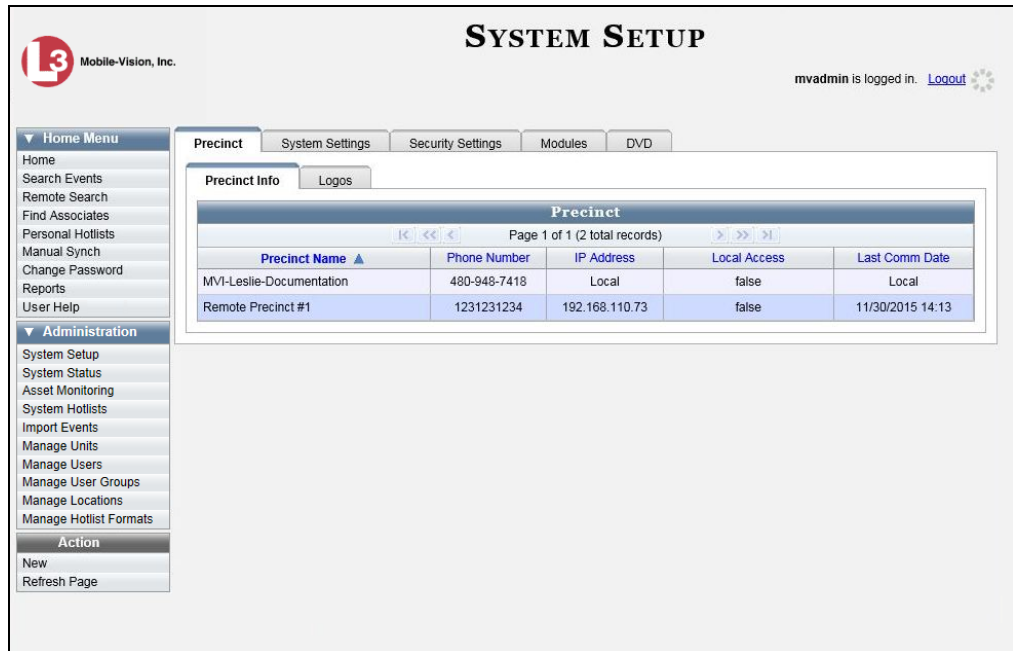
* To view a particular unit's status, go to ▼**Administration** and click **Manage Units**.

System Status Settings (cont'd)	
Field	**Description**
Non-archived Event Count	The number of events on the server that have not been burned to backup disc yet.
Last 24 Hours Event Count	The number of events that have been downloaded from AlertVU units to the server in the last 24 hours.
Last 7 Days Event Count	The number of events that have been downloaded from AlertVU units to the server in the last seven days.
Last 30 Days Event Count	The number of events that have been downloaded from AlertVU units to the server in the last 30 days.
Number of Backup DVDs	The total number of archive discs (i.e., *Certified Backup Discs*) that the system has burned since AlertVU Back Office was installed.
Downloader Errored Out	A true/false display that indicates whether or not there is currently a problem with the transmission of event files from units to server: ▪ *True*. There is an event transmission problem. ▪ *False*. There is no event transmission problem.
Backup Scheme	The current backup scheme: ▪ *all*. Backup everything ▪ *none*. Backup nothing
Version	The version of AlertVU Back Office that you currently have installed. This field also includes a link to the technical Release Notes. Whenever you call L3 Mobile-Vision Technical Support, please have the current version number on hand.
Active Users *(right column)*	Information on all users who are currently logged into AlertVU Back Office: ▪ User ID ▪ IP address of the PC used to log into the application ▪ Date and time at which the user last logged in.
Action	
Action	**Description**
Refresh Page	Redisplay the System Status page so that you can see any changes that have occurred since you first displayed the page. The system updates screen information every 15 minutes.

Updating Precinct Information

During installation, your System Implementation Specialist (SIS) will enter your Precinct information into AlertVU Back Office. By default, the system prints some of this information on your archive discs, including your home precinct's name and phone number. This section describes how to update this information as needed.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 If it is not already selected, click the **Precinct** tab.

3 If it is not already selected, click the **Precinct Info** tab. Your precinct record(s) display, as pictured above.

4 Click on the precinct record you wish to update.

5 Go to the Action column and click **Edit**.

– OR –

Right-click on the record, then select **Edit** from the popup menu.

The Edit Precinct popup displays. This popup will be slightly different depending on whether this is the *home* precinct or a *remote* precinct.

(Continued)

Edit Precinct

Precinct Data

Remote Precinct

Organization Name:	Remote Precinct #1
Precinct Name:	Remote Precinct #1
Address:	123 MVI Drive
Phone Number:	1231231234
IP Address:	192.168.110.73
Grant Local Access:	☐
Enable SSL:	☐
Max Concurrent Searches:	2
Search Type:	L3 Mobile Vision
API Port:	80
API Context:	/alertvu/services/LPRHandlerService
Last Comm Date:	11/30/2015 14:13

Save   Cancel

The Precinct Data fields for the home precinct are described below. The data fields for the remote precinct(s) are described on page 268.

Home Precinct Data	
Field	**Description**
Organization Name	The name of your agency. By default, the system will print this field on your backup discs.
Precinct Name	The name of the precinct that this AlertVU server is installed at, if applicable. By default, the system will print this field on your backup discs. If you don't need this field to specify precinct information, you can use it to enter default text that you wish to print on backup discs, such as "For Official Use Only."
Address	Your precinct's mailing address.
Phone Number	Your precinct's phone number. By default, the system will print this field on your backup discs.
Registration Key	Your AlertVU product identification code. *Display-only field*.
Support Expiration	The date on which your service contract with L3 Mobile-Vision expires. *Display-only field*.

For information on the Mail Server function, see "Forwarding System Messages to Your Regular Mailbox" on page 270.

6 Enter your changes in the appropriate field(s).

7 Click **Save**.

Configuring the System to Perform Remote Searches
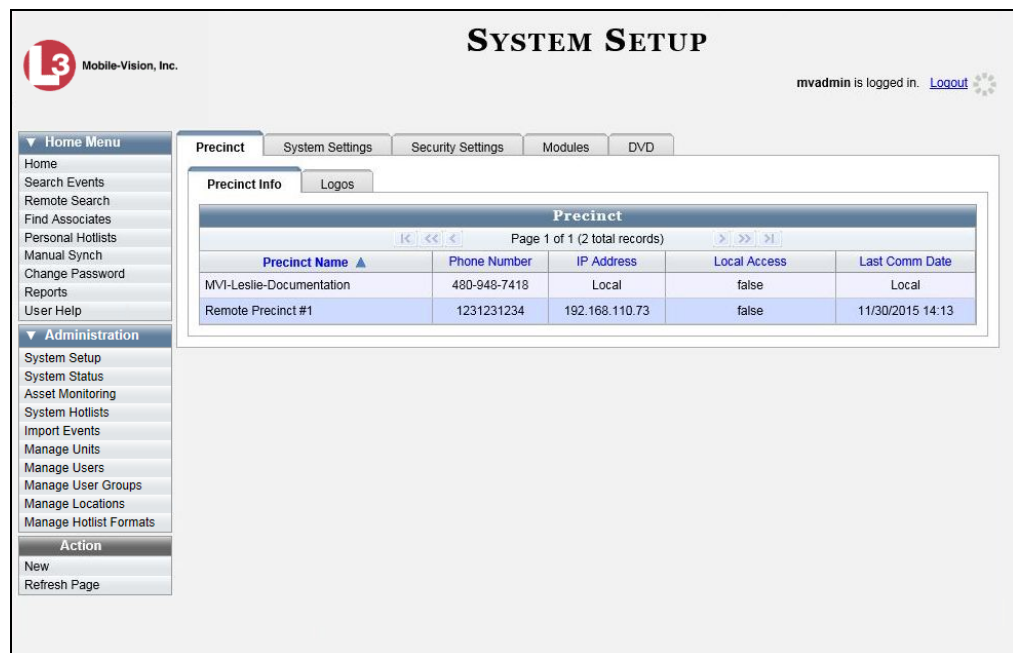
The optional Enterprise AlertVU Administration module allows your organization to perform event searches on other precincts' databases. You can remotely search both AlertVU databases *and* non-AlertVU databases that conform to NIJ (National Institute of Justice) standards.

To configure the system for remote searches, you will need to add a precinct record for each remote precinct you wish to search. If your agency will be searching remote *AlertVU* servers, you will also need to contact the System Administrator at each remote precinct and ask him to add *your* precinct record to *their* database, taking care to select the *Grant Local Access* checkbox on the precinct record.

WARNING: The following procedure should only be performed with the assistance of your L3 Mobile-Vision Technical Support Engineer (TSE) or System Implementation Specialist (SIS).

1   Go to **▼ Administration** and click **System Setup**. The System Setup page displays.

2   If it is not already selected, click the **Precinct** tab.

3   If it is not already selected, click the **Precinct Info** tab.

4   Go to the **Action** column and click **New**. The New Precinct popup displays.

(Continued)

The fields on this screen are described below.

Remote Precinct Data	
Field	**Description**
Organization Name	The name of the remote agency.
Precinct Name	The name of the remote precinct which houses the server that will be searched.
Address	The remote precinct's mailing address.
Phone Number	The remote precinct's phone number.
IP Address	The network address of the remote precinct's server.
Grant Local Access	A checkbox used to grant the remote precinct access to local data when a user on the remote server is performing a remote search.
Enable SSL	A checkbox used to enable encrypted communication between servers when performing remote searches.
Max Concurrent Searches	The number of remote searches that can be executed at the same time on the remote precinct.
Search Type	The search method that this remote precinct will be using: ▪ L3 Mobile Vision. The proprietary L3 Mobile Vision search method. ▪ External NIJ. The non-proprietary National Institute of Justice search method. Only select this option if the remote precinct is a **non-AlertVU** third party system that conforms to NIJ standards. Select this value from the drop-down list provided.

L3 Mobile-Vision, Inc.

Remote Precinct Data (cont'd)	
Field	**Description**
API Port	The number of the network port that will be used for communication between precinct servers. If the *Enable SSL* checkbox is selected, this field defaults to **443**. Otherwise the field defaults to **80**. You cannot change this field unless the selected *Search Type* is **External NIJ**.
API Context	The internal server path to the service that will be used to facilitate Enterprise AlertVU communication. You cannot change this field unless the selected *Search Type* is **External NIJ**.
Last Comm Date	The date that the remote precinct server last communicated with the local server. *Display-only field*.

5 Enter the remote agency's name in the *Organization Name* field.

6 Enter the remote precinct's name in the *Precinct Name* field.

7 Enter the remote precinct's mailing address in the *Address* field.

8 Enter the remote precinct's phone number in the *Phone Number* field.

9 Enter the network address of the remote precinct's server in the *IP Address* field.

10 If you want the remote precinct to be able to search your local server as well, select the *Grant Local Access* checkbox. Otherwise proceed to the next step.

(Continued)

11 To enable encrypted communication between servers when performing remote searches, select the *Enable SSL* checkbox. Otherwise proceed to the next step.

12 If you selected the *Grant Local Access* checkbox, proceed to the next step. Otherwise skip to step 17.

13 To allow two concurrent searches on the remote server (default), proceed to the next step. Otherwise enter a different value in the *Max Concurrent Searches* field.

14 If the remote precinct you are configuring has an *AlertVU* server (default), skip to step 17.

– OR –

If the remote precinct you are configuring has a *non-AlertVU* server, select **External NIJ** from the drop-down list. Proceed to the next step.

15 Enter the number of the network port that will be used for communication between precinct servers in the *API Port* field.

16 If your L3 Mobile Vision Technical Support Engineer (TSE) instructed you to change the value of the *API Context* field, enter that value. Otherwise proceed to the next step.

17 Click **Save**. The new record displays on the Precinct list.

18 To enter another remote precinct, repeat steps 4 – 17.

Forwarding System Messages to Your Regular Mailbox

By default, AlertVU system messages display in the *Inbox Messages* section of the Message Board, located on the AlertVU Home Page. However, if your precinct has its own SMTP mail server, you can configure the system so that users' *Inbox* messages, including hotlist alerts, are copied to their regular email accounts as well.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.
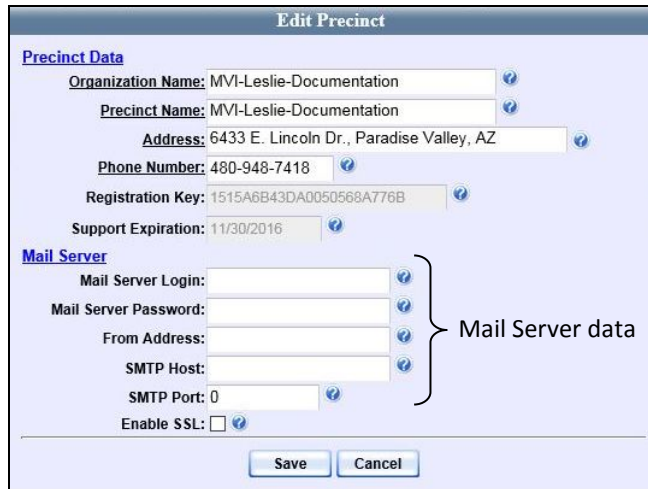
2 If it is not already selected, click the **Precinct** tab.

3 If it is not already selected, click the **Precinct Info** tab.

4 Click on the precinct record to highlight it.
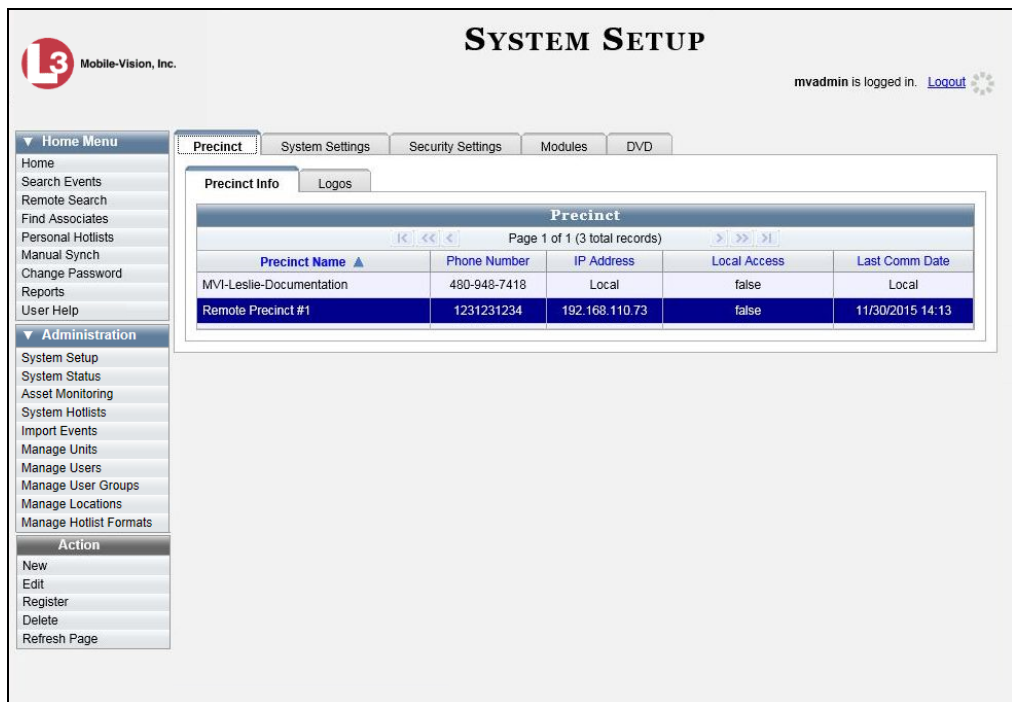
5 Go to the Action column and click **Edit**.

– OR –

Right-click on the record, then select **Edit** from the popup menu.
The Edit Precinct popup displays.

The Mail Server fields are described below.

Mail Server	
Field	**Description**
Mail Server Login	A User ID that has send-mail privileges within your mail system.
Mail Server Password	The security password for the *Mail Server Login* above.
From Address	The email address that will display in the *From Address* field of the forwarded emails (e.g., System_Admin@L3com.com).
SMTP Host	The SMTP email host.
SMTP Port	The SMTP email port.

For a description of the *Precinct Data* fields, see the table on page 266.

6 Position your cursor in the *Mail Server Login* field. Enter a User ID with send-mail privileges, then press **Tab**.

7 Enter the security password for the *Mail Server Login*, then press **Tab**.

8 Enter the email address that will display in the *From Address* field of the forwarded emails, then press **Tab**.

9 Enter the name of the SMTP email host, then press **Tab**.

10 Enter the number of your SMTP email port.

11 Click **Save**.

Changing the Application Display Logo

This section describes how to change the graphics file that displays in the upper left corner of the AlertVU application. You may, for example, want to replace the default logo with your agency's logo.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.
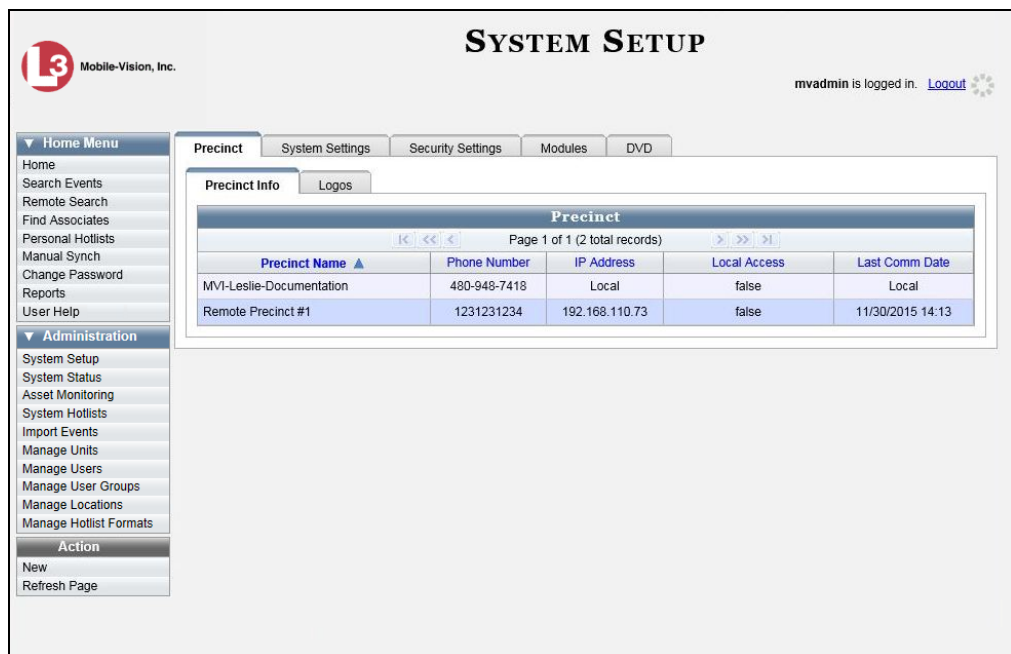
2 If it is not already selected, click the **Precinct** tab. Your precinct record(s) display, as pictured above.

3 Click the **Logos** tab.

(Continued)
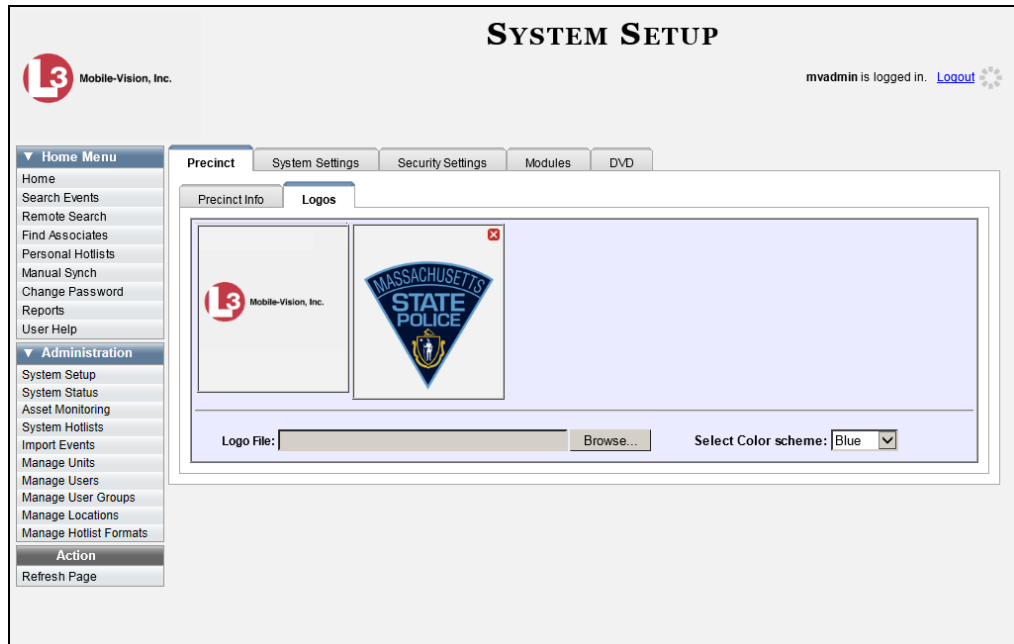
If you previously uploaded any graphics files to AlertVU, a thumbnail image of those file(s) will display on-screen. Otherwise just the L3 Mobile-Vision logo will display.

4 If the desired graphic already displays on-screen, skip to step 8. Otherwise proceed to the next step.

5 Click the **Browse** button to the right of the *Logo File* field. The Choose File to Upload popup displays.

6 Navigate to the disk drive location where the graphics file is located.

7 Double-click on the graphics file you wish to upload. A thumbnail image of the graphic displays in the space above the *Logo File* field.

8 Click on the thumbnail image of the graphic you wish to display. That graphic will appear in the upper left corner of the AlertVU application.

Please note that the graphic you select here will display on *every* page of the AlertVU Back Office application, not just on the Home page.

Maintaining Storage Devices

The **Storage Machines** tab lists the settings that AlertVU uses to determine where data is stored on the server and how to interact with client workstations. These Storage Machines may be located on internal or external storage devices, such as a RAID unit. RAID is an acronym for *Redundant Array of Independent Disks*—a storage device that contains multiple disk drive components.

Storage server data is configured by your System Implementation Specialist (SIS) during installation. You do not need to modify this data unless the disk resources available to the server have changed.

WARNING: Do not modify any of the field values on a Storage Device record without the assistance of your agency's network specialist OR an L3 Mobile-Vision Technical Support Engineer. Entering incorrect data could have dire consequences. Some of your events could become inaccessible, wireless transmission could fail, and/or data could be permanently lost.

For specific instructions, see:

❒ Adding a Storage Device, below
❒ Viewing/Changing a Storage Device, page 278
❒ Deleting a Storage Device, page 280.

Adding a Storage Device

This section describes how to set up a new storage device on AlertVU Back Office. Your System Implementation Specialist (SIS) or Technical Support Engineer (TSE) will perform this task when your agency acquires a new RAID storage unit. For more on RAIDs, see the previous section.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

(Continued)
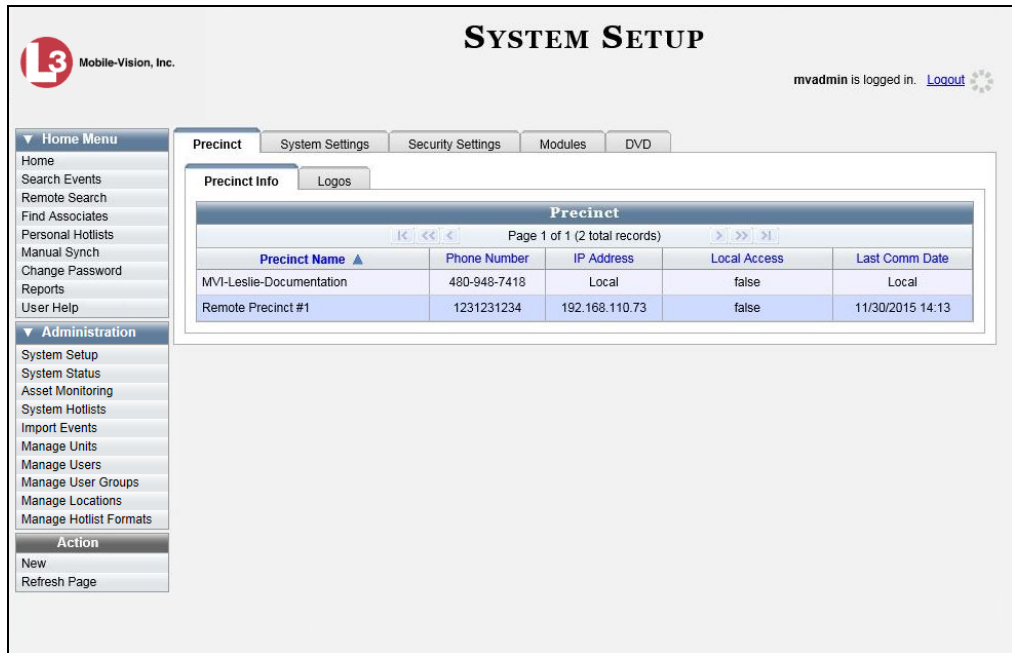
2 Click the **System Settings** tab.
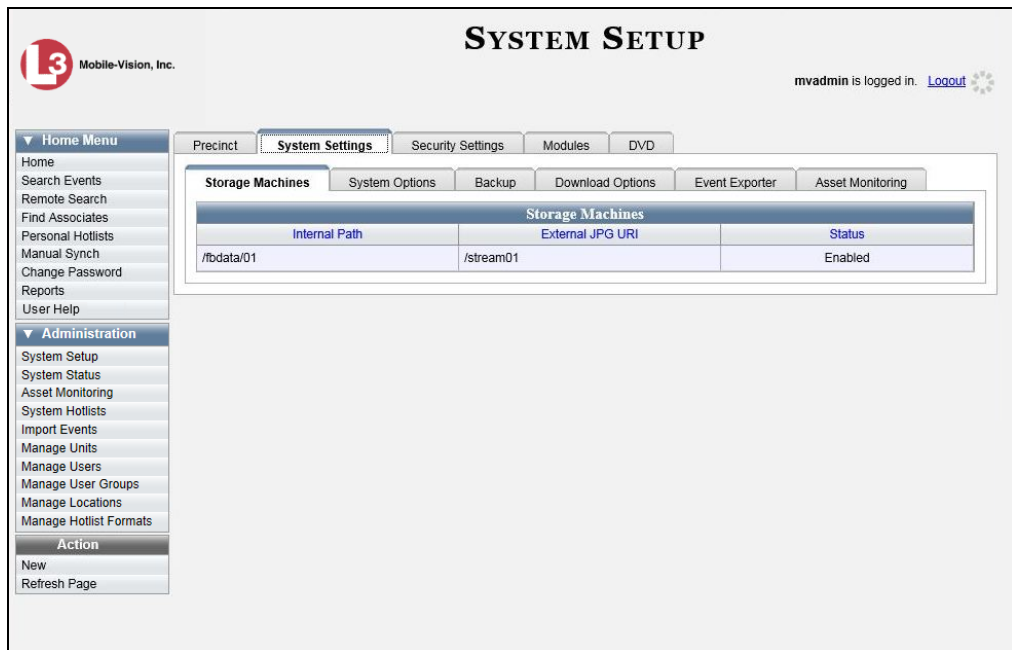
3 If it is not already selected, click the **Storage Machines** tab, as pictured above.

4 Go to the Action column and click **New**. The New Storage popup displays.

The fields on the New Storage popup are described below.

New Storage	
Field	**Description**
<u>Internal Path</u>	The server path to the new storage machine, such as /fbdata/00.
<u>External JPG URI</u>	The path by which data will be served through the web application (e.g., /stream00/).
Status	The current status of this storage device: ▪ *Enabled*. This storage device is available to receive events and hotlists. ▪ *Disabled*. This storage device is *not* available to receive events and hotlists.

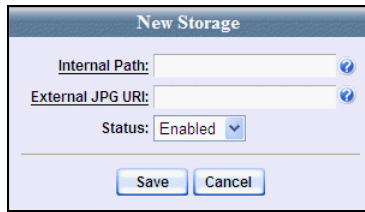**NOTE**: The values entered on this form *must* match the actual configuration of the storage server.

5   Enter the top level path to data storage (e.g., /fbdata/00) in the *Internal Path* field.

6   Enter the path by which data will be served through the web application (e.g., /stream00/) in the *External JPG URI* field.

7   If you want this storage device to be immediately available to receive events (default), proceed to the next step.

     – OR –

     If you do *not* want this storage device to be immediately available to receive events, select **Disabled** from the *Status* drop-down list.

8   Click **Save**. A confirmation message displays at the top of your page.
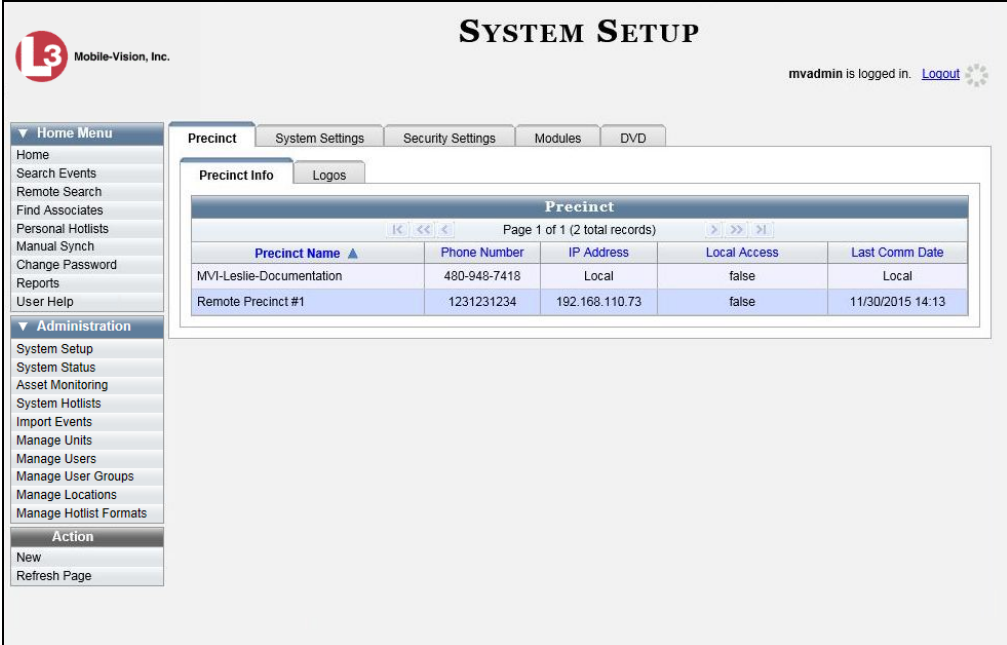
> **Storage save successful**

Viewing/Changing a Storage Device

This section describes how to view and/or update a storage machine record. These records contain the settings that AlertVU uses to determine where data is stored on the server and how to interact with client workstations.

Because storage server data is configured by your System Implementation Specialist (SIS) during implementation, you do not need to modify this data unless the disk resources available to the server have changed.

1 Go to **▼ Administration** and click **System Setup**. The System Setup page displays.

2 Click the **System Settings** tab.

3   If it is not already selected, click the **Storage Machines** tab, as pictured above.

4   Click on the storage device record you wish to view/edit.

(Continued)

5 Go to the Action column and click **Edit**.

– OR –

Right-click on the record, then select **Edit** from the popup menu.

The Edit Storage popup displays.

Edit Storage

Internal Path: /fbdata/01

External JPG URI: /stream01

Status: Enabled

Save   Cancel

For a description of the fields on this form, see the table on page 277.

6 To change your storage configuration, proceed to the next step. Otherwise click **Cancel** to close the popup.

WARNING: Do not modify any of the field values on this popup without the assistance of your agency's network specialist OR an L3 Mobile-Vision Technical Support Engineer.

7 Enter/select your changes in the appropriate field(s).

8 Click **Save**. A confirmation message displays at the top of the page.

Storage save successful

Deleting a Storage Device

This section describes how to delete an existing storage device record. Only perform this procedure when instructed to do so by an L3 Mobile-Vision Technical Support Engineer.

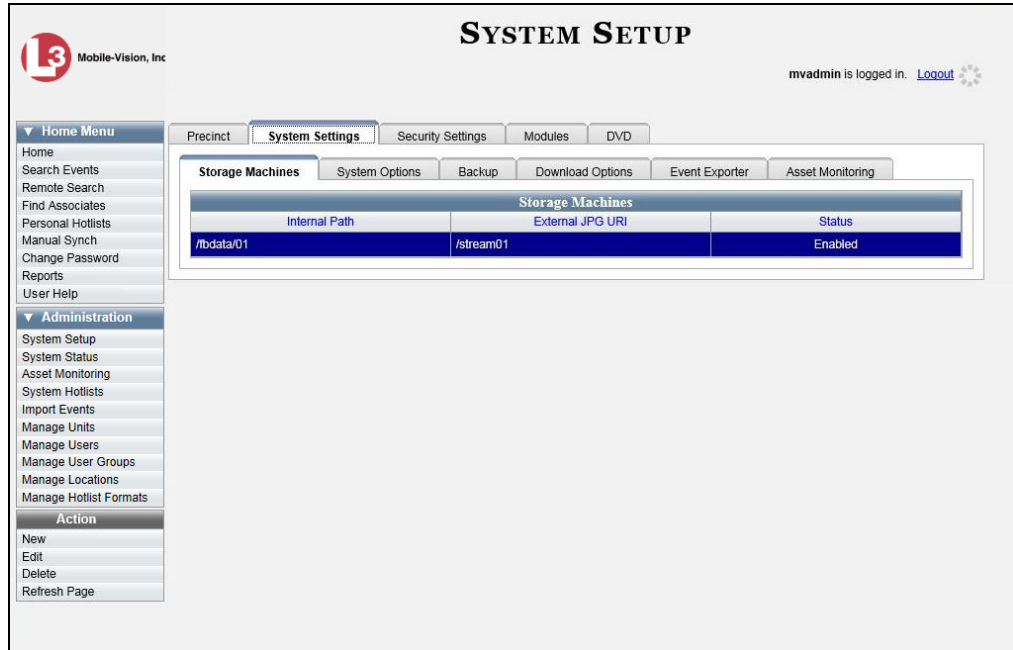**1** Go to ▼ Administration and click **System Setup**. The System Setup page displays.
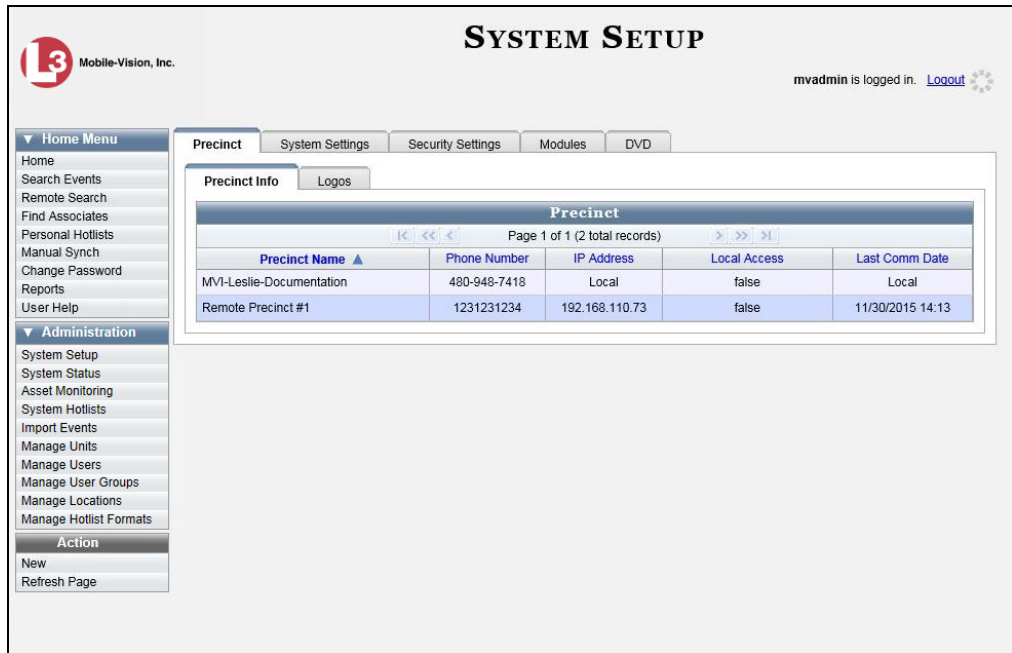
2 Click the **System Settings** tab.
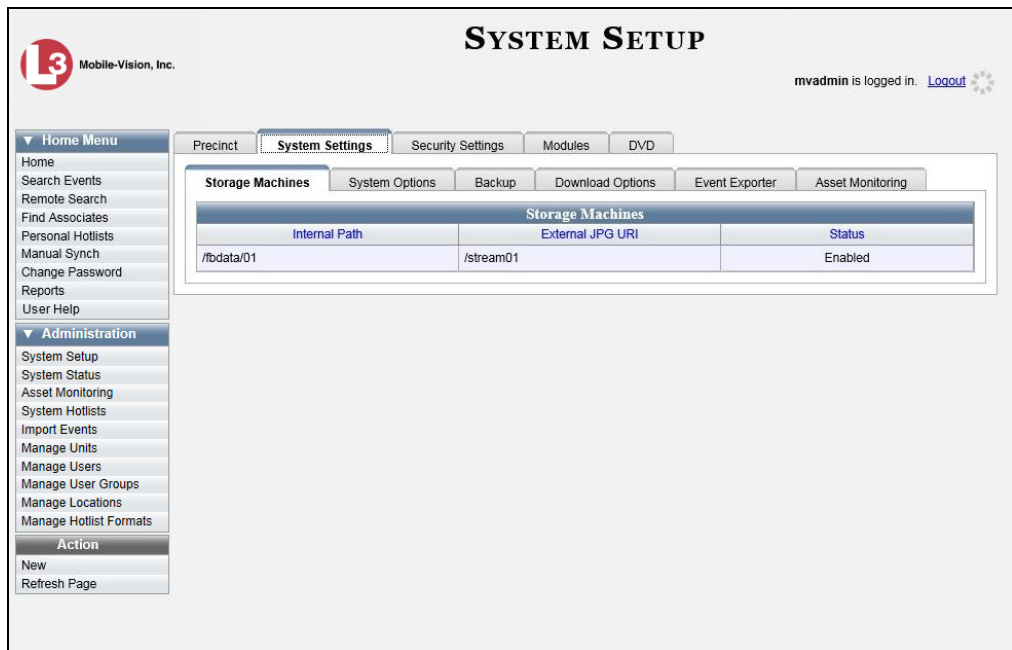
3 Make sure that the **Storage Machines** tab is selected, as pictured above.

4 Click on the storage device you wish to delete.

(Continued)

5 Go to the Action column and click **Delete**.

– OR –

Right-click on the record, then select **Delete** from the popup menu.

A confirmation message displays.

6 Click **Yes**. The selected storage device is removed from the Storage Machines list.

Accessing Product Manuals & Training Videos

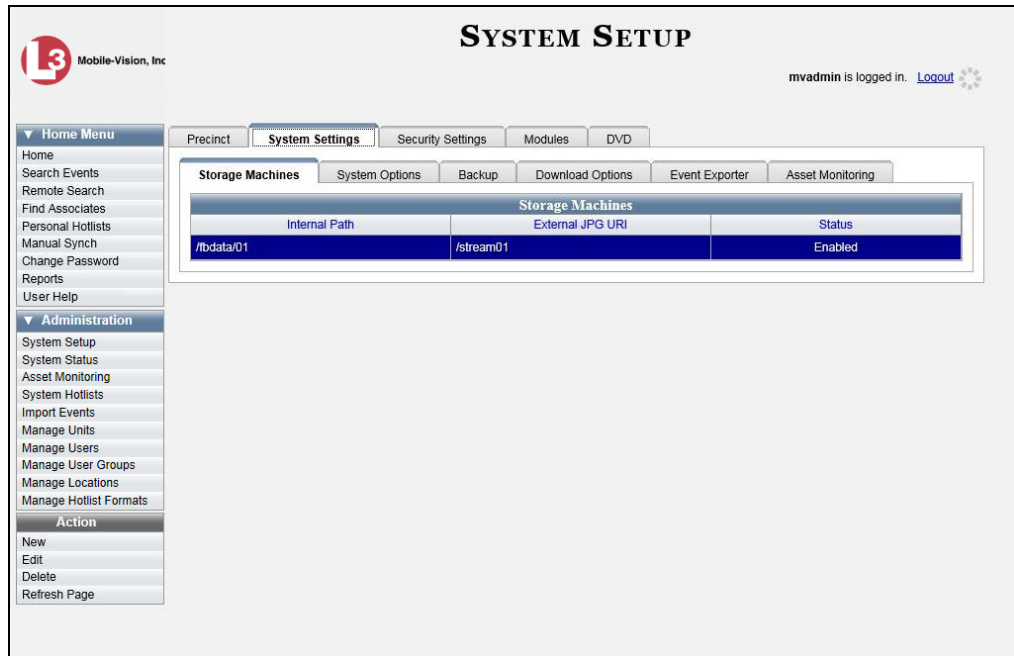This section describes how to access L3 Mobile-Vision's product manuals and training videos via links to our Online Support Center.

This procedure requires that you have Adobe Reader or other .pdf reader software installed on your PC.

1 Go to ▼ Administration and click **System Status**. The System Status page displays.
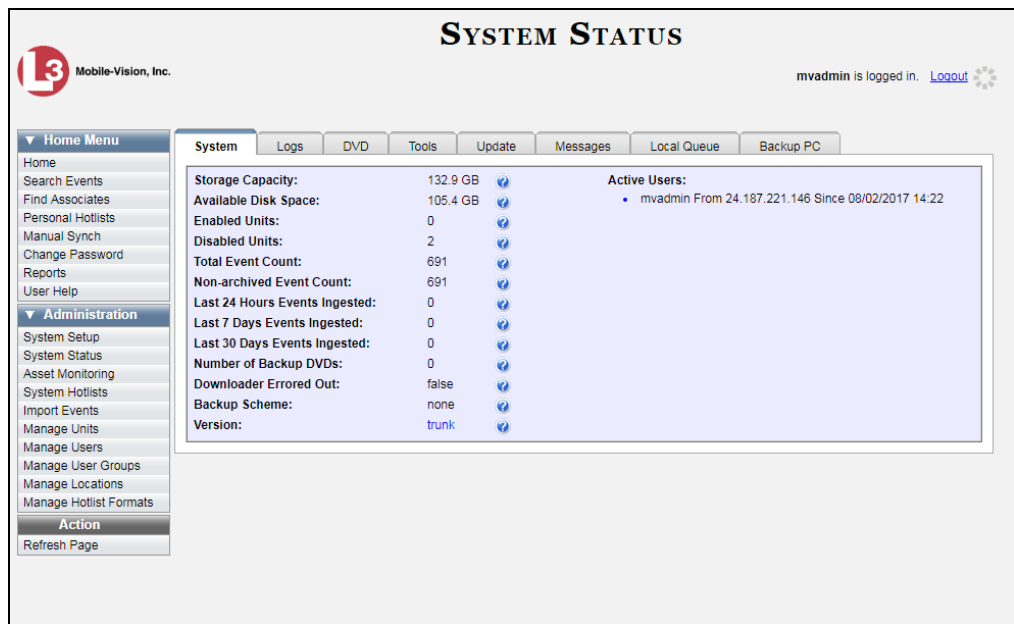
2 Click the **Tools** tab. The video and documentation links are listed on the right side of the page.
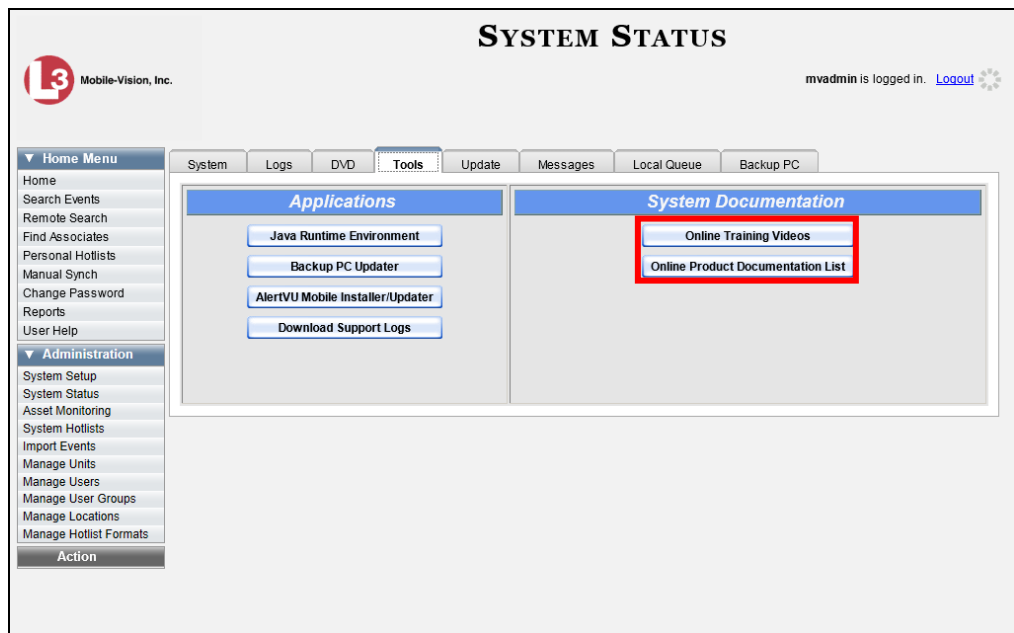
3 Click on the appropriate button:

To view a list of training videos, click **Online Training Videos**.

– OR –

To view a list of manuals and quick reference guides, click **Online Product Documentation List**.

A Windows prompt displays.

4 Click **Open**. A PDF file displays.

5 Click on the desired documentation or video link. If you selected the Product Documentation List (pictured above), the AlertVU documentation that pertains to your agency is listed below.
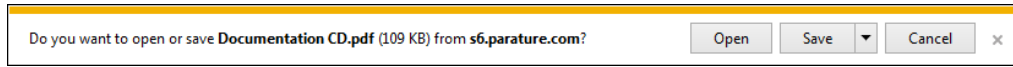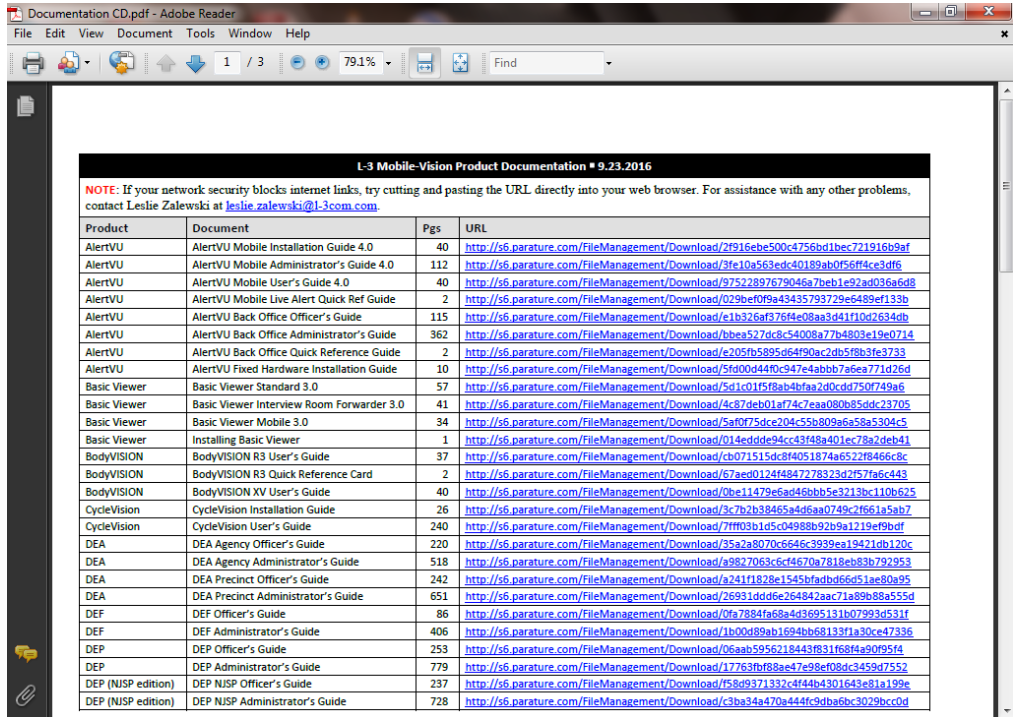
Document	Audience
AlertVU Mobile Installation Guide	AlertVU Mobile installers
AlertVU Mobile Administrator's Guide	▪ AlertVU Mobile installers ▪ AlertVU Mobile system administrators and supervisory users
AlertVU Mobile User's Guide	AlertVU Mobile non-supervisory users
AlertVU Back Office Officer's Guide	AlertVU Back Office non-supervisory users
AlertVU Back Office Administrator's Guide	AlertVU Back Office system administrators and supervisory users

Document	Audience
AlertVU Back Office Quick Reference Guide	All AlertVU Back Office users
AlertVU Fixed Hardware Installation Guide	AlertVU Fixed installers

6 Follow the Windows prompts to view the selected document. If you selected the training video document, please note that the AlertVU videos are on the *last page* of that file.

Updating Software

This section describes how to update those server and PC applications that are a part of the AlertVU system, including:
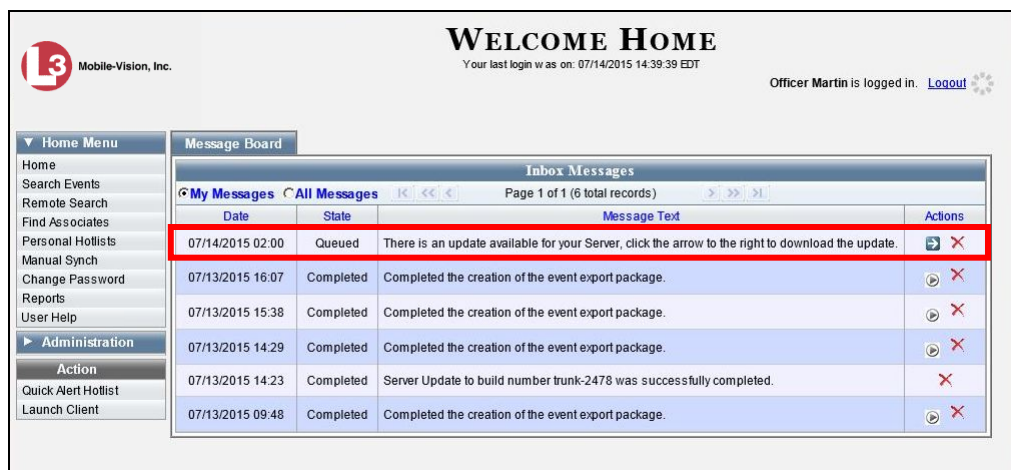
❐ Server application (AlertVU Back Office). Your server is typically installed in an agency building, such as the computer room in your local precinct.
❐ PC transmission software. The PC transmission software is installed on the mobile data computers and/or laptops that are located at each AlertVU unit site.

For specific instructions, see:

❐ Updating the Server Application, below
❐ Updating the PC Transmission Software, page 289.

Updating the Server Application

If your agency has an up-to-date Extended Maintenance Agreement (EMA) and your hardware/software configuration meets our system requirements, you qualify for software upgrades whenever one is available. This section describes how to update the AlertVU Back Office application after you receive an upgrade notification in your in-box (*"There is an update available for your Server…"*).
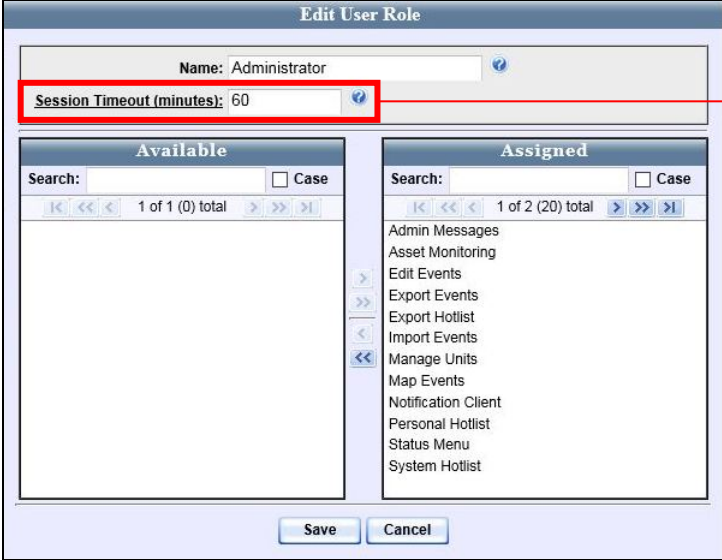
The following procedure requires that your AlertVU server have internet access to our Auto Update server. If you do *not* have direct access to our update server *or* your agency does not *allow* direct access to our server for security reasons, please contact L3 Mobile-Vision Service at 973-263-1090. A Technical Support Engineer will provide you with an alternate method for upgrading your software.

Before you begin an update, make sure that your user type has a *Session Timeout* setting of at least 60 minutes to prevent you from being logged out during the update process.

Make sure that this field is set to 60 or higher

For instructions on changing this setting, see "Changing the Session Timeout Setting" on page 293.

Depending on the size of the update and speed of the network connection, the update process may take up to an hour.

1 Make sure the Home page displays. (If necessary, go to ▼ Home Menu and click **Home**.)

This document consists of general capabilities information that is not defined as controlled technical data under ITAR part 120.10 or EAR

L3 Mobile-Vision, Inc.

2 Go to your *Inbox Messages* list and click on the arrow icon to the right of the upgrade notification link (*'There is an update available for your Server…'*).

The Update tab displays.
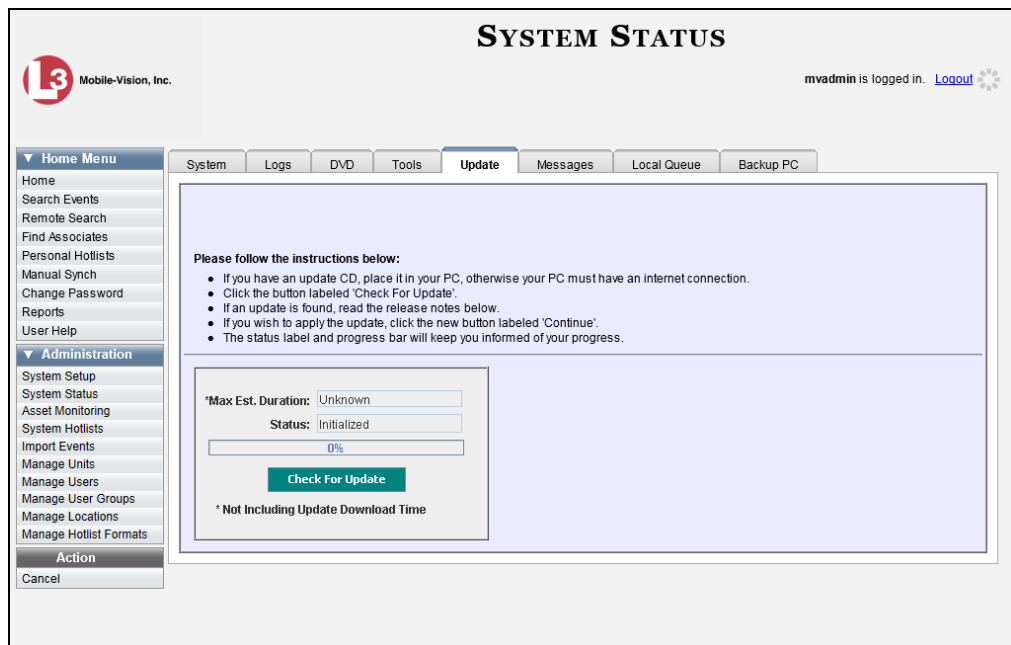
3 Click the **Check for Update** button. The system searches for the new update.

Once the system locates the update, the words "Update Found" will display in the *Status* field and the technical release notes for the update will display at the bottom of the page.

(Continued)
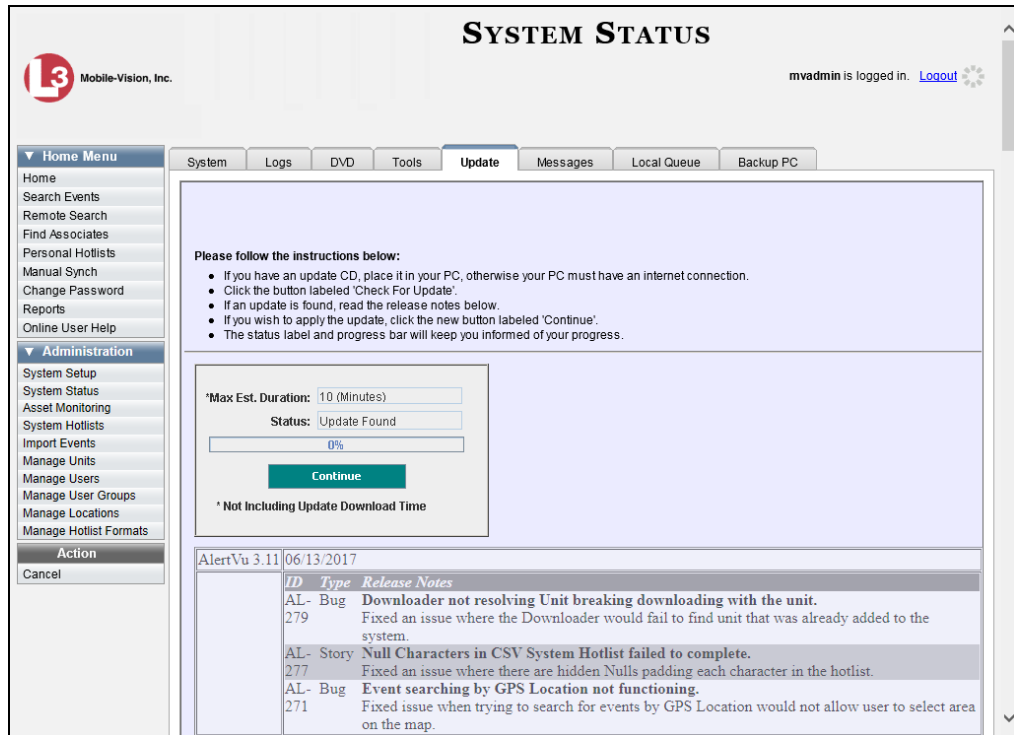
4 Click **Continue**. The system begins installing the update.
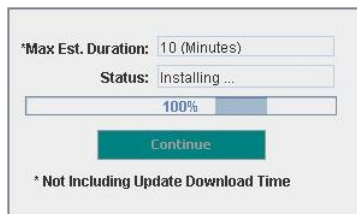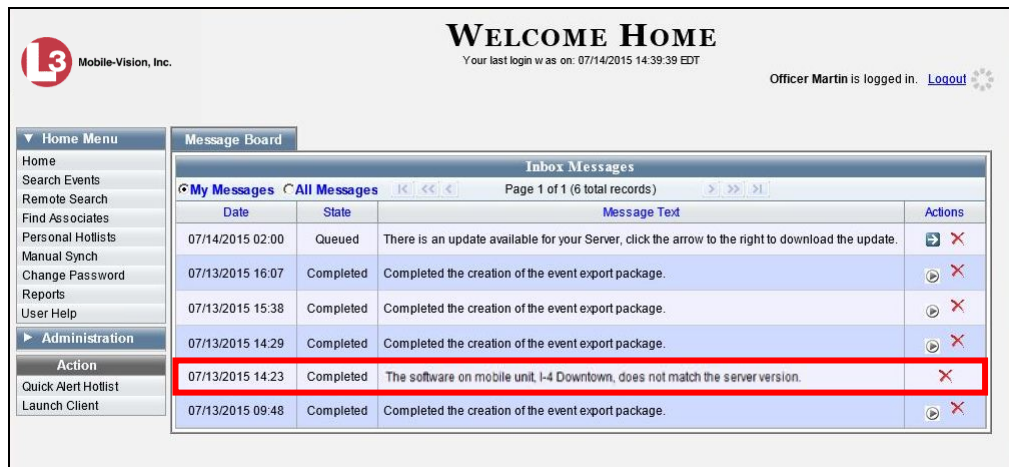
When the update is complete, a confirmation message displays.
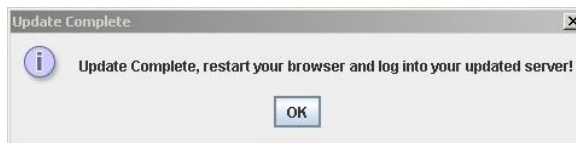
5 Click **OK**.

6 Restart your browser.

7 Log into AlertVU Back Office again.

L3 Mobile-Vision, Inc.

Updating the PC Transmission Software

This section describes how to update the L3 Mobile-Vision transmission software that's installed on the mobile data computers and/or laptops located at each AlertVU unit site. Perform this task whenever you receive the following notification in your in-box (*"The software on mobile unit XYZ does not match the server version…"*).


NOTE: The following procedure is performed from the *server*, not from the mobile data computer.

1   Go to ▼ Administration and click **System Status**. The System Status page displays.

(Continued)

2 Click the **Tools** tab.

3 Click on the **AlertVu Mobile Installer/Updater** button. A Windows message displays.

4 Click **Run**. A warning message displays.

Example 1

Example 2
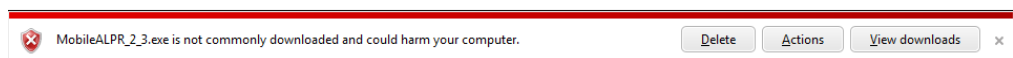
If your popup includes a **Run** button (as in *Example 1* above), click on it. Next, skip to step 8 for further instructions.

– OR –

If your popup does *not* include a **Run** button (i.e., it looks more like *Example 2* above), proceed to the next step.

5 Click the **Actions** button. The following popup displays.
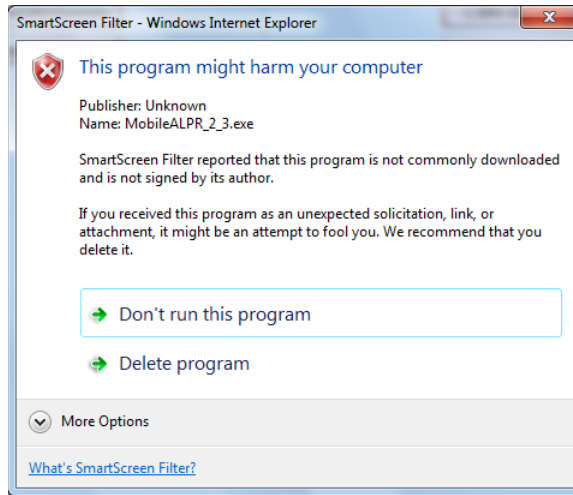
6 Click **More Options**. The following popup displays.
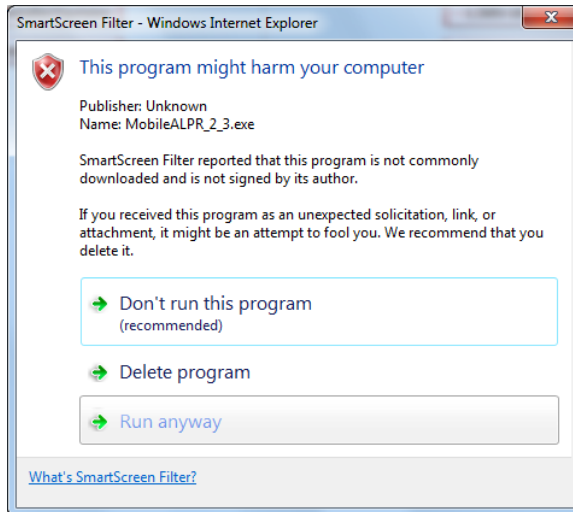
7 Click **Run anyway**. The Mobile ALPR Setup Wizard displays.
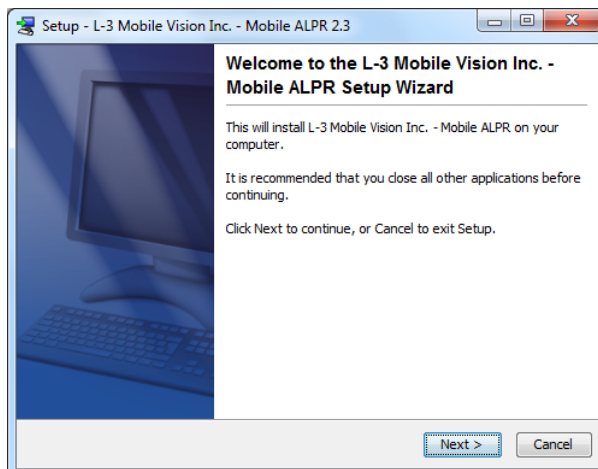
8 Click **Next**. The system begins installing the application.
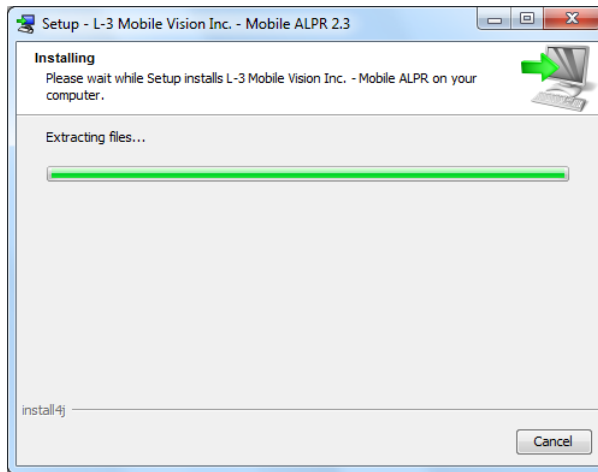
Once the installation is complete, a confirmation screen displays.
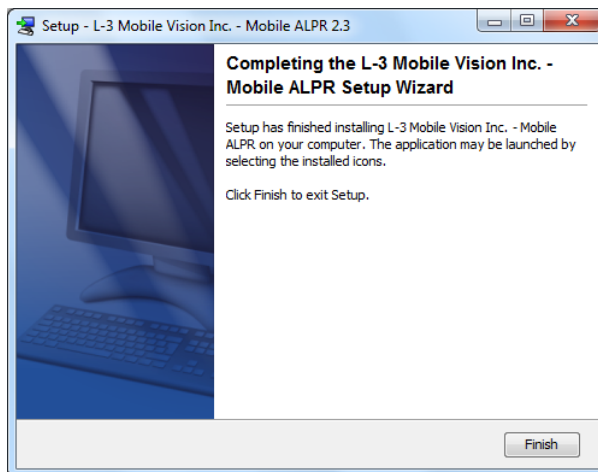
9 Click **Finish**. The system prompts you to restart your computer.
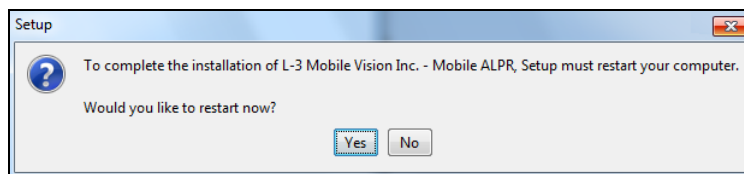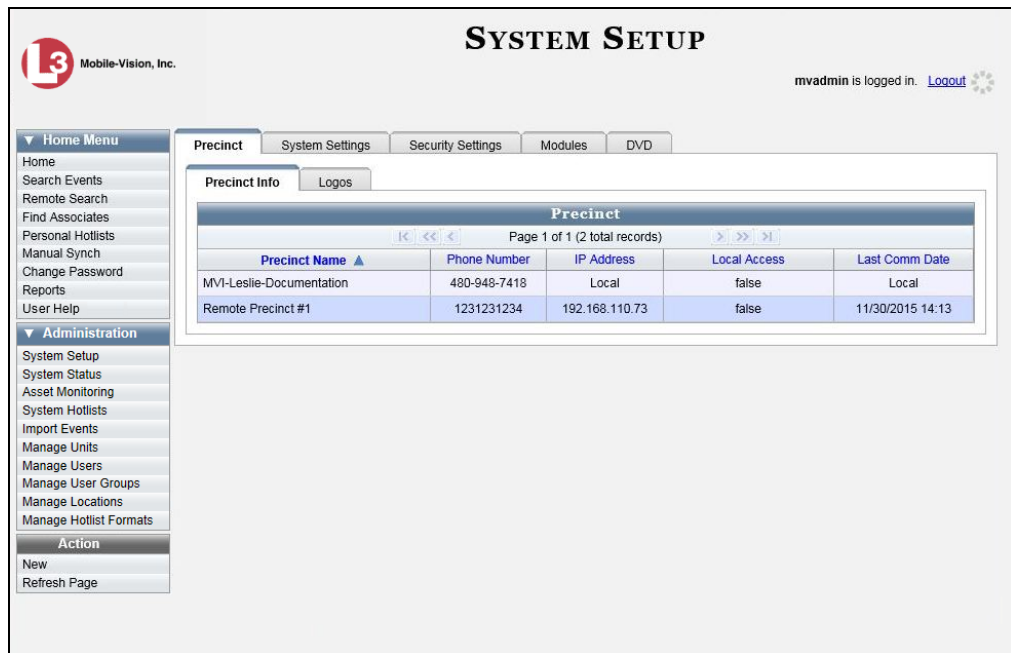
10 Click **Yes**. The system reboots. Once the reboot is complete, login to AlertVU Back Office again.

Changing the Session Timeout Setting

The Session Timeout Setting refers to the number of minutes of inactivity the system will allow before automatically logging a particular user type off AlertVU Back Office. If a user type will be performing time-intensive tasks, such as installing software updates, it's recommended that you set their session timeout to a *minimum* of 60 minutes.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 Click the **Security Settings** tab.

(Continued)

3   Click the **User Roles** tab. A list of system users displays.

4   Click on the user role to highlight it.

5 Go to the Action column and click **Edit**.

– OR –

Right-click on the record, then select **Edit** from the popup menu.
The Edit User Role popup displays.

6 Go to the *Session Timeouts (minutes)* field and enter the number of minutes you wish to elapse before this user type is automatically logged off the system.

7 Click **Save**. A confirmation message displays:

> **User Role Officer successfully saved.**

Changing the Application's Color Scheme

This section describes how to change the application's color scheme from the current color to *blue*, *brown*, *green*, *orange*, or *red*.

1 Go to **▼ Administration** and click **System Setup**. The System Setup page displays.

2 If it is not already selected, click the **Precinct** tab.

3 Click the **Logos** tab.

4 Select a new color scheme from the *Select Color scheme* drop-down list.

The system will prompt you to login to the application again, at which point the new color scheme will take effect.

Downloading the Support Logs

This section describes how to download the logs that are occasionally used by L3 Mobile-Vision's Technical Support Engineers to troubleshoot technical problems. This procedure is only used by those customers who have no remote access what-soever (i.e., your agency is unable or unwilling to allow remote access to its AlertVU server). Perform this task when instructed to do so by a Technical Support Engineer.

1 Go to ▼ **Administration** and click **System Status**. The System Status page displays.
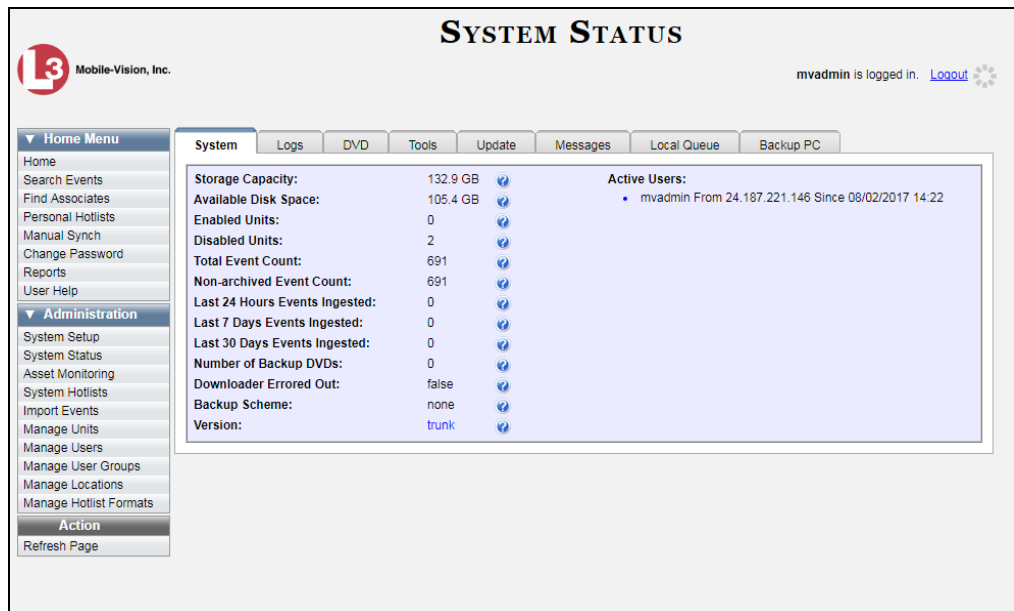
2 Click the **Tools** tab.
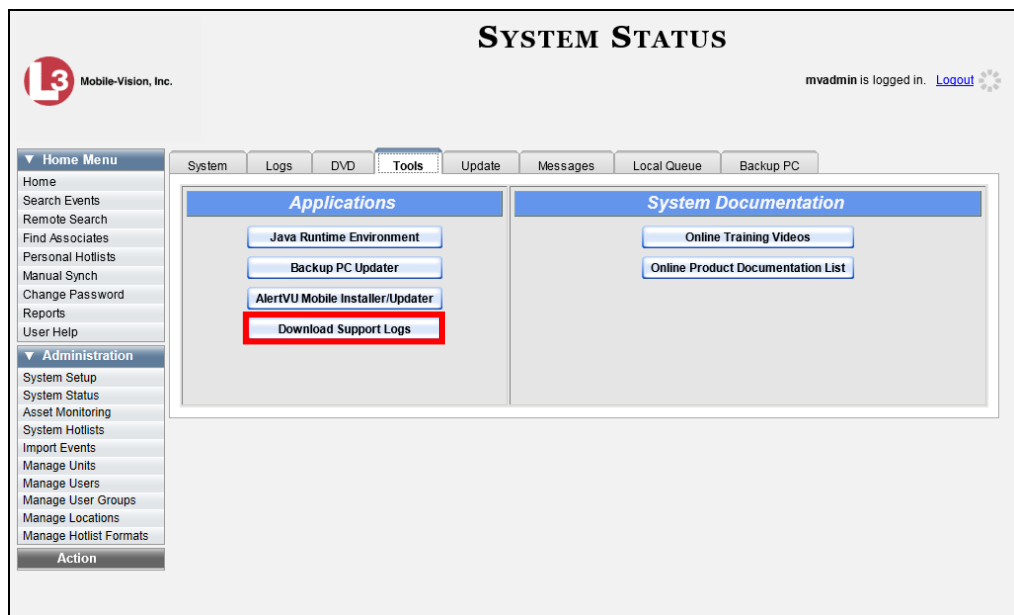
3 Go to the *Applications* column and click the **Download Support Logs** button. The following message displays.

Compressing logs. Please wait

After a delay of a few seconds to a few minutes, a Windows message displays.

Do you want to open or save **logs.mvl** (199 MB) from **trinity**?	Open	Save ▼	Cancel	✕

4 Select **Save As** from the *Save* drop-down list. The Save As popup displays.

5 Navigate to the disk drive location where you wish to temporarily save the log file. (You will be uploading this file to L3 Mobile-Vision.)

6 Click **Save**. The system copies the log file to the selected location.

When the process is complete, a confirmation message will display.

The logs.mvl download has completed.	Open ▼	Open folder	View downloads	✕

7 Click **Open Folder** to display the file.

8 Upload the file to L3 Mobile-Vision as per your Technical Service Engineer's instructions.

Viewing System Messages from the 'Messages' Tab

Occasionally, the system may send notification messages to users with the Administrator role, informing you of a possible problem or error that may require some action on your part. These messages show up in two places: on your Home page's Inbox Messages list, and on the Messages tab. The difference between viewing messages on the Inbox Messages list and viewing them on the Messages tab is that the messages on the Messages tab are grouped by *type*, whereas the messages on the Inbox list are listed *individually*. Also, the messages on the Home page may be mixed in with other non-urgent messages, such as a server update confirmation.

As System Administrator, you may want to review the combined system messages on the Messages tab first, as described in this section, and then review individual messages on the Home page if more information is required.

1 Go to ▼ Administration and click **System Status**. The System Status page displays.

(Continued)

2 Click the **Messages** tab. Any notification messages for Administrators display.

The columns on this tab are described in the following table.

Messages Tab	
Column	**Description**
Quantity	The number of messages related to the issue described in the *Message Type* column.
State	The current status of the issue described in the *Message Type* column.
Message Type	A description of the system issue. Because system messages are grouped by *type*, any information that is specific to an individual message is replaced by **{0}**. If you want to review the specific message content, you will have to view the message from your *Inbox Messages* list on the Home Page.
Action	An icon used to delete all messages related to the issue described in the *Message Type* column.

3 After you have resolved the issue associated with a notification message, click the ✕ to the right of that message to delete all messages related to that issue.

Changing the Days Online Setting for Messages

By default, each of your Home page messages will remain online for a minimum of 45 days. Once a message reaches that age, it may be purged by the system. The following procedure describes how to increase or decrease this setting.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 Click the **System Settings** tab.

3 Click the **System Options** tab.

4 Go to the Action column and click **Edit**. The System Options popup displays.

This document consists of general capabilities information that is not defined as controlled technical data under ITAR part 120.10 or EAR

5 Enter a new value in the *Days to Retain User Messages* field.

6 Click **Save**.

Downloading the Java Runtime Environment (JRE) Application

The Java Runtime Environment (JRE) application is required on workstations to perform certain functions, such as performing system updates. A download of this application is provided within AlertVU Back Office as a convenience.

1 Save and close any open PC files/applications other than AlertVU Back Office.

2 Go to ▼ Administration and click **System Status**. The System Status page displays.
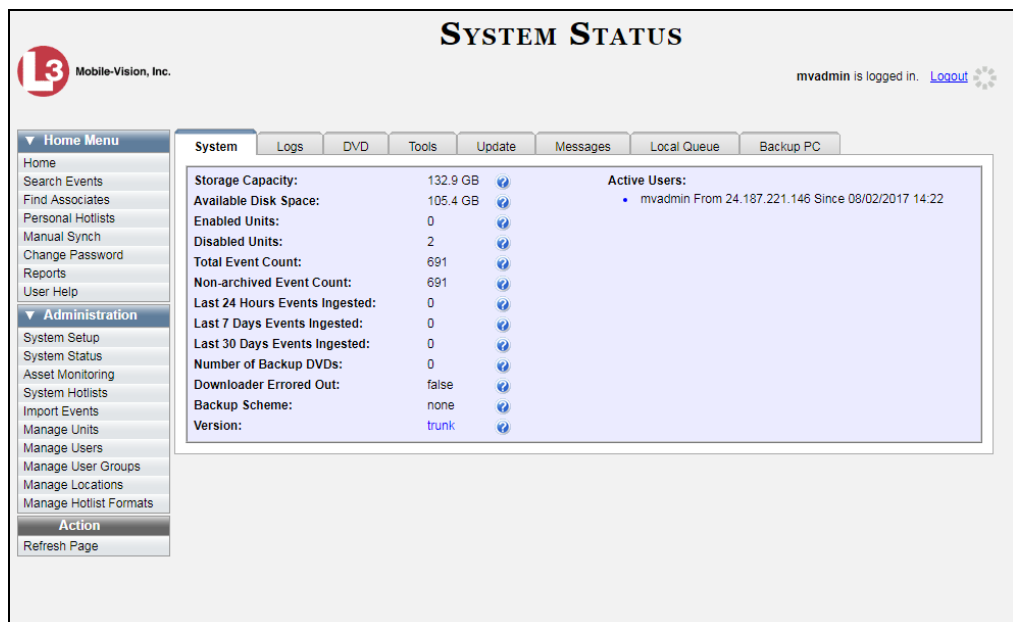
3   Click the **Tools** tab.
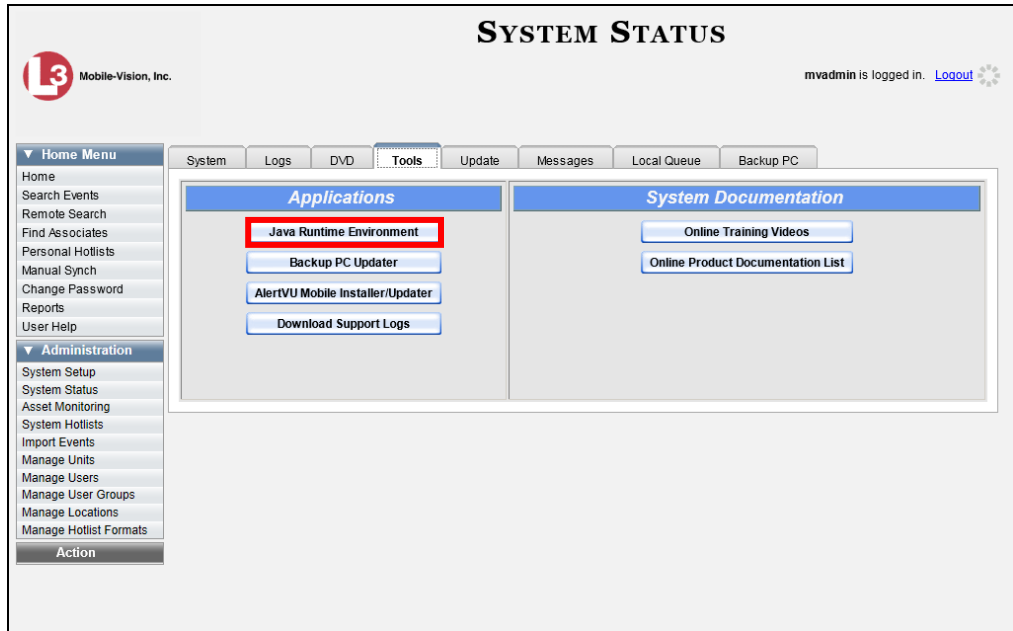
4   Go to the *Applications* column and click the **Java Runtime Environment** button. A Windows download message displays.
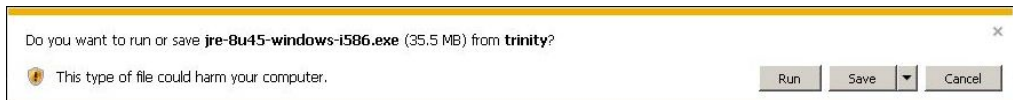
5   Click **Run**.

6   If you receive a security warning, click **Run** again. Otherwise proceed to the next step.

7   Click **Install**.

8 Follow the Java system prompts. At the end of the installation process, a confirmation message will display.

9 Click **Close**.

10 Exit AlertVU.

11 Reboot your PC.

AlertVU Back Office Administrator's Guide
L3 Mobile-Vision • 8.7.2017

7 Security

User Roles   AlertVU includes a security feature called *user roles*. A user role is simply a group of permissions that you can assign to one or more users. When a user logs in to AlertVU Back Office, the system will grant him access to the various system functions according to his assigned user role. If desired, you may also grant certain users access to additional permissions above and beyond what is included in their assigned user role.

Password Rules   To further enhance your application security, AlertVU also allows you to define the rules that apply to a user password. These include password length, password complexity, and the number of logon attempts allowed before the system disables a password.

For more information, see:

❐ Assigning Permissions, below
❐ Defining Password Policies, page 330
❐ Changing Security Log Settings, page 336.

Assigning Permissions

As previously discussed, users are granted access to various system functions by assigning them a *user role*. There are two types of user roles: *system-defined* and *custom*.

For more information, see:

❐ Permissions-Driven Tasks, below
❐ System-Defined User Roles, 309
❐ Custom User Roles, page 316
❐ Assigning Permissions to a User, page 327.

Permissions-Driven Tasks

The following table describes all the system functions that are permissions-driven. These are the tasks that you can link to a *user role*, thus granting access to all users who are assigned that role.

Permissions for User Roles	
Permission Name	**Allows the User to…**
Admin Messages	Send administrator messages to the user's *Inbox Messages* list on the Home page
Asset Monitoring	Access the Asset Monitoring menu
Edit Events	Correct license plate misreads
Export Events	Copy an events search results list to a .csv spreadsheet file
Export Hotlist	Copy a hotlist to a .csv spreadsheet file
Import Events	Import event records that were previously archived or exported from either AlertVU or the ELSAG license plate reader
Location Management	Add, change, or delete Location records and/or Location Group records
Manage Units	Access the Manage Units menu
Manage Users	Access the Manage Users menu
Manual Sync	Manually synchronize a unit with the server so that an AlertVU unit that has been without a wireless connection for a prolonged period of time can 1) receive updated hotlists from the server, and 2) transfer new event records to the server.
Map Events	View an events search results list in Map View
Notification Client	Activate the Live Alert utility, which allows you to display real-time alerts whenever an AlertVU unit receives a hit on a license plate that's on a system hotlist for which you have Notification rights
Personal Hotlist	Create a hotlist for your personal use
Promote Hotlist	Upgrade a personal hotlist to a system-level hotlist
Quick Alert Hotlist	Create a one-plate "Amber Alert" style hotlist that you can immediately push out to all AlertVU units
Remote Search	Search for event records on a remote agency's server
Search Map	Search for events within a specified geographical location
Setup Menu	Access the System Setup menu
Status Menu	Access the System Status menu
System Hotlist	Create a system-level hotlist that you can push out to all AlertVU units
View Reports	View the predefined activity reports

L3 Mobile-Vision, Inc.

System-Defined User Roles

System-Defined User Roles are pre-defined user groups that come standard with AlertVU. These include:

❒ Administrator
❒ Officer
❒ Supervisor
❒ View Only - Event.

These roles are customizable. You can add or remove permissions from them as desired. However, the names of these roles cannot be changed, nor can they be deleted from the system.

For a description of system permissions, see the table on the previous page.

For more information, see:

❒ Default Permissions for System-Defined User Roles, below
❒ Changing the Settings for a System-Defined User Role, next page
❒ Restoring a System-Defined User Role to its Default Settings, page 314.

Default Permissions for System-Defined User Roles

The following table lists the default permissions for the system-defined user roles that come standard with AlertVU. For more on user roles, refer to this chapter's introduction and/or "System-Defined User Roles" above.

	Administrator	Officer	Supervisor	View Only – Events
Admin Messages	✔		✔	
Asset Monitoring	✔			
Edit Events	✔		✔	
Export Events	✔		✔	
Export Hotlist	✔		✔	
Import Events	✔			
Location Management	✔			
Manage Units	✔		✔	
Manage Users	✔		✔	
Manual Sync	✔		✔	
Map Events	✔	✔	✔	✔
Notification Client	✔			

(Continued)

	Administrator		
		Officer	
			Supervisor
View Only – Events			
Personal Hotlist	✔	✔	✔
Promote Hotlist	✔		✔
Quick Alert Hotlist	✔		✔
Remote Search	✔		✔
Search Map	✔		✔
Setup Menu			✔
Status Menu	✔		✔
System Hotlist			✔
View Reports			✔

Changing the Settings for a System-Defined User Role

This section describes how to change the default settings for one of the predefined user roles that come with AlertVU:
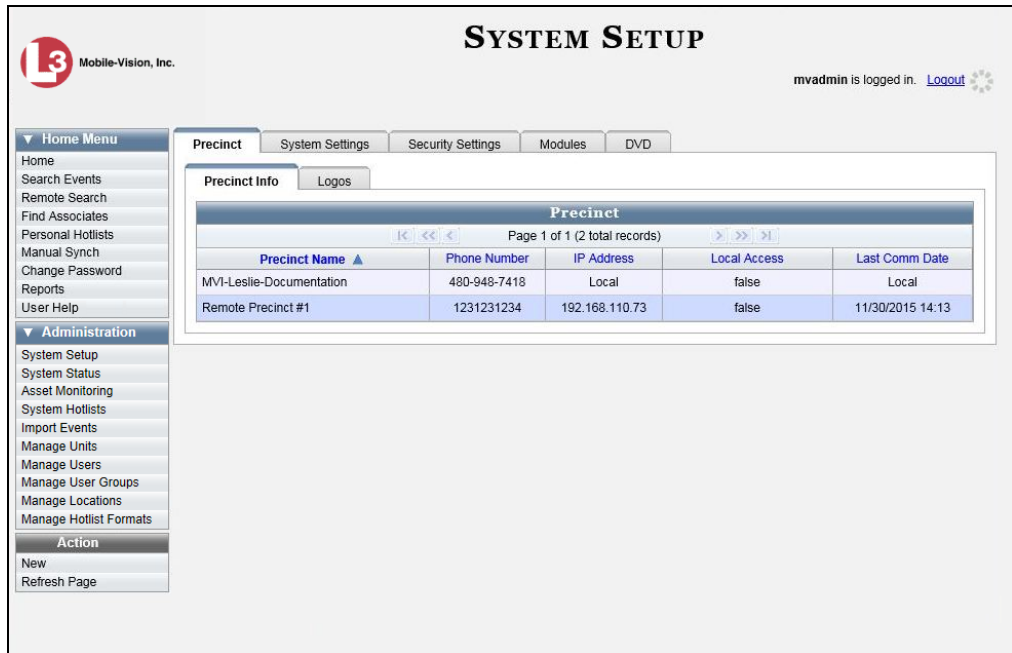
❑ Administrator
❑ Officer
❑ Supervisor
❑ View Only–Event.

You can change a user role's *session timeout setting* and/or its *permissions*, as described below.

❑ *Session Timeout*. The *session timeout* setting is the number of idle-time minutes that must pass before the system automatically logs a user off the system.
❑ *Permissions*. A user role's *permissions* determine what system functions a user will or will not be able to access. You can add/remove any number of permissions to/from a selected user role. For a list of permissions, see "Permissions for User Roles" in the table on page 308.

Please note that you cannot change the *name* of a system-defined user role. If the predefined names (*Administrator*, *Officer*, *Supervisor*, and *View Only–Event*) do not meet your agency's needs, see "Adding a Custom User Role" on page 316 instead.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 Click the **Security Settings** tab.
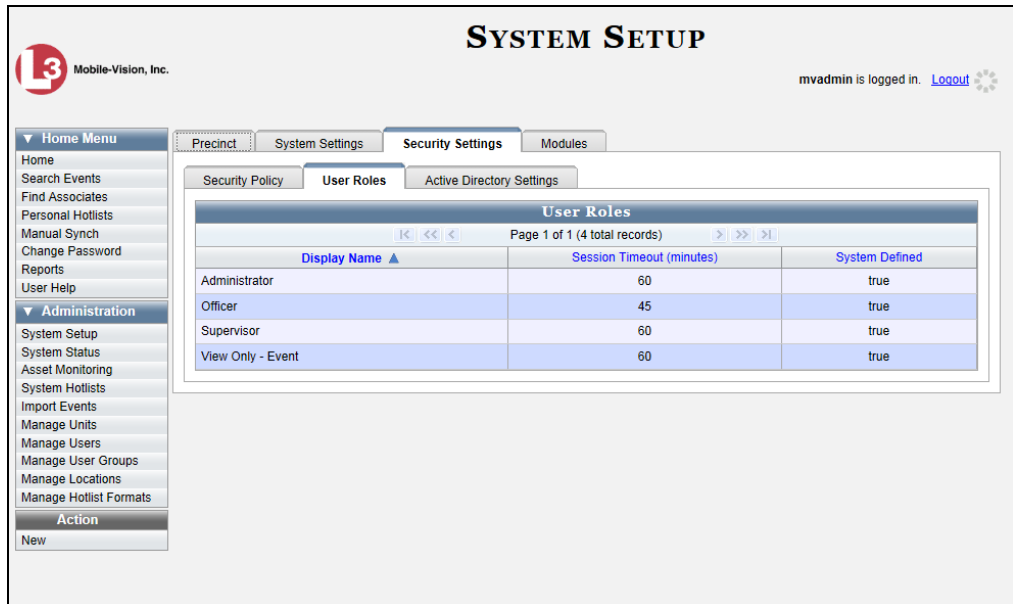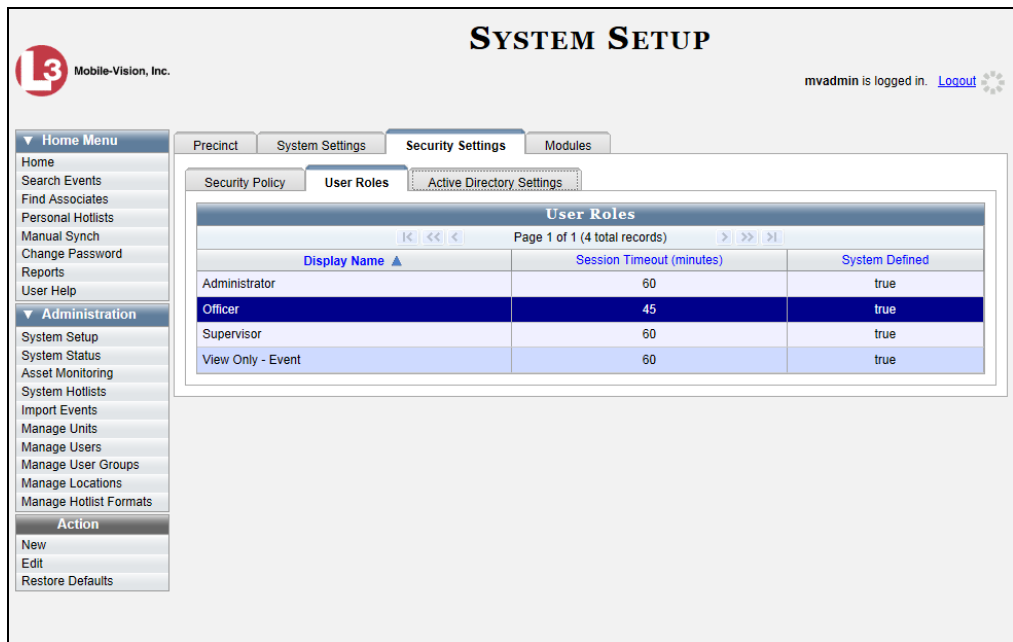

3 Click the **User Roles** tab. A list of User Roles displays.

4 Click on the user role you wish to update.

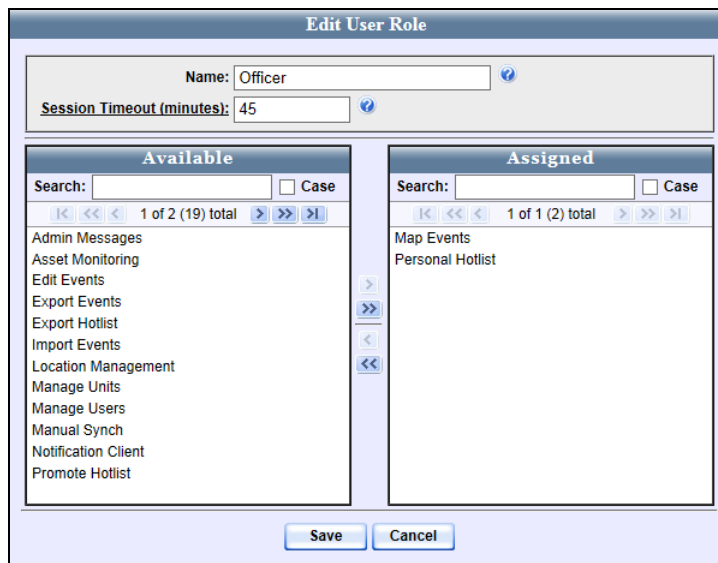**5** Go to the Action column and click **Edit**.

– OR –

Right-click on the record, then select **Edit** from the popup menu.

The Edit User Role popup displays.

L3 Mobile-Vision, Inc.

Edit User Role

Name: Officer

Session Timeout (minutes): 45

Available	Assigned
Search: ☐ Case	Search: ☐ Case
⏮ ⏪ ◀ 1 of 2 (19) total ▶ ⏩ ⏭	⏮ ⏪ ◀ 1 of 1 (2) total ▶ ⏩ ⏭
Admin Messages	Map Events
Asset Monitoring	Personal Hotlist
Edit Events	
Export Events	
Export Hotlist	
Import Events	
Location Management	
Manage Units	
Manage Users	
Manual Synch	
Notification Client	
Promote Hotlist	

Save   Cancel
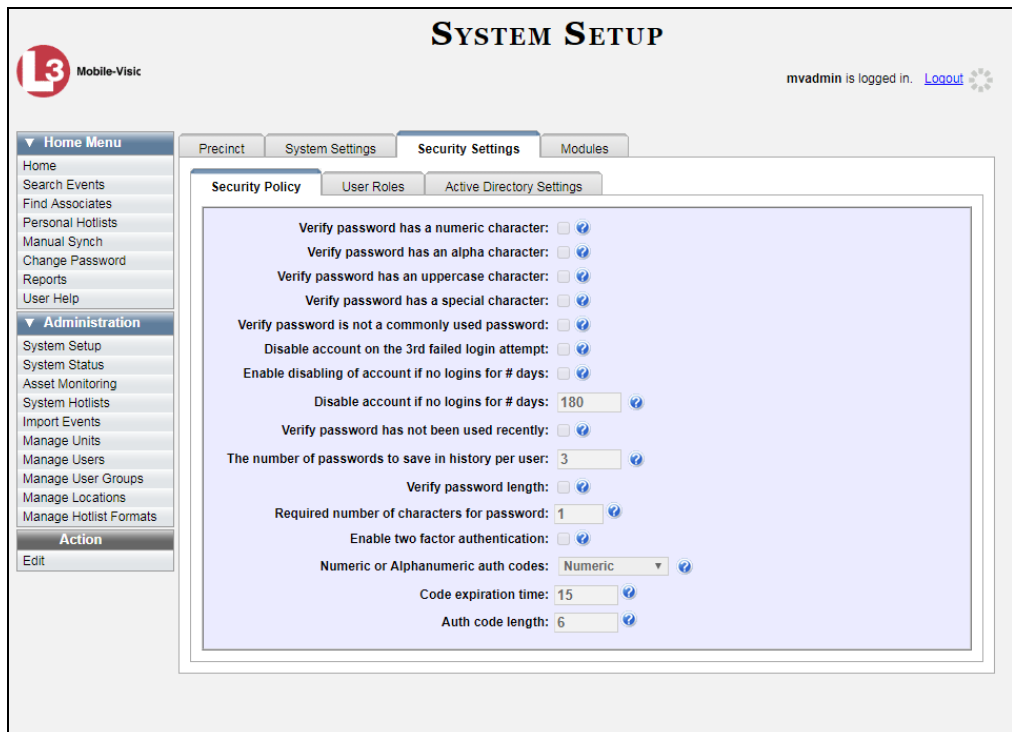
6 To change the *Session Timeout* setting[*] for this user role, proceed to the next step. Otherwise skip to step 8.

7 Enter a new value in the *Session Timeout (minutes)* field.

8 To *add* a permission to this user role, proceed to the next step. Otherwise skip to step 11.

9 Go to the left column (Available) and click on each of the permissions you wish to add. If a permission you're looking for does not appear on-screen, use the navigation arrows at the top of the column to scroll through the permissions list.

10 Once you've highlighted the desired permissions, click the ▶ icon located between the two columns. The selected permissions display in the right column (Assigned).

11 To *remove* a permission from this user role, proceed to the next step. Otherwise skip to step 14.

12 Go to the right column (Assigned) and click on each of the permissions you wish to remove.

13 Once you've highlighted the desired permissions, click the ◀ icon located between the two columns. The selected permissions are removed from the *Assigned* list.

14 Click **Save**. The system analyzes your selections to make sure that they are logical. If there are any problems, the system will prompt you to make another selection.

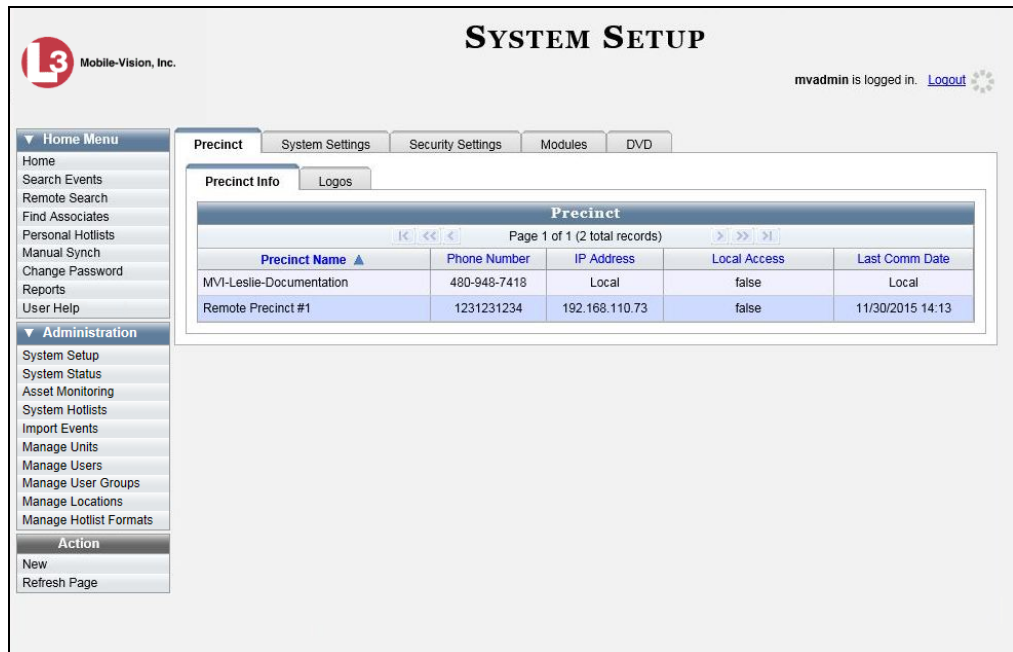[*] The number of idle-time minutes that must pass before the system automatically logs a user off the system.

This document consists of general capabilities information that is not defined as controlled technical data under ITAR part 120.10 or EAR

Once you've saved the user role without any errors, a confirmation message displays.

User Role Officer successfully saved.

Restoring a System-Defined User Role to its Default Settings

This section describes how to restore a system-defined user role to its original factory settings. Perform this task if you previously changed the settings for a system-defined user role and you now wish to restore that user role to its original settings.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 Click the **Security Settings** tab.

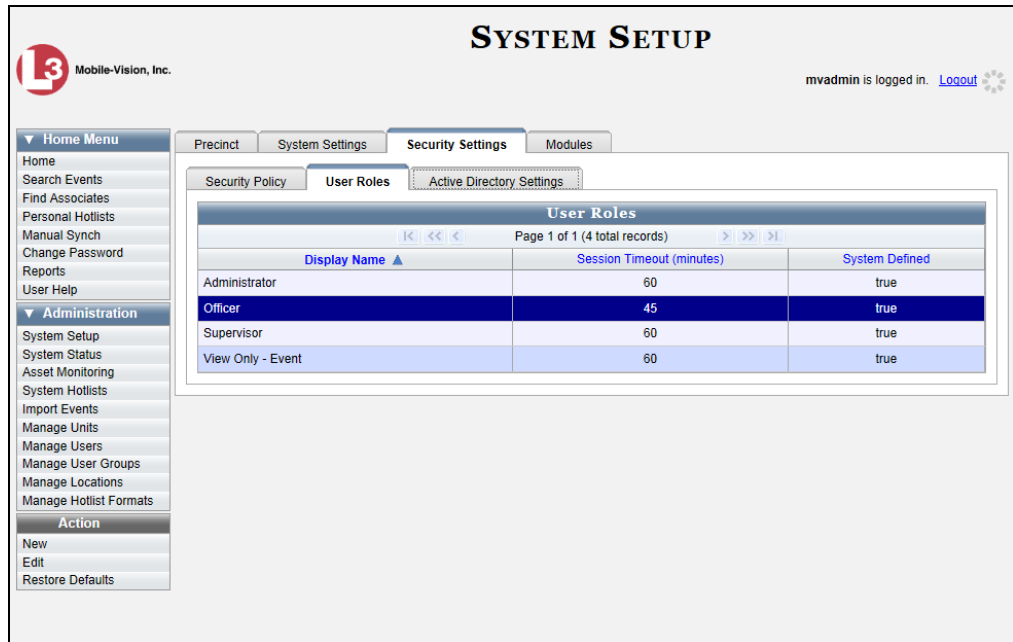**3** Click the **User Roles** tab. A list of User Roles displays.

4 Click on the user role that you wish to restore.

(Continued)

5 Go to the Action column and click **Restore Defaults**. A confirmation message displays.

> User Role **Officer** successfully saved.

Custom User Roles

A *custom* user role is a group of permissions that has a unique name, that is, a name which differs from the four default names[*]. As with system-defined user roles, you can add or remove permissions from custom user roles as desired. For a list of permissions, see "Permissions for User Roles" in the table on page 308.

For specific instructions, see:

❒ Adding a Custom User Role, below
❒ Changing a Custom User Role, page 320
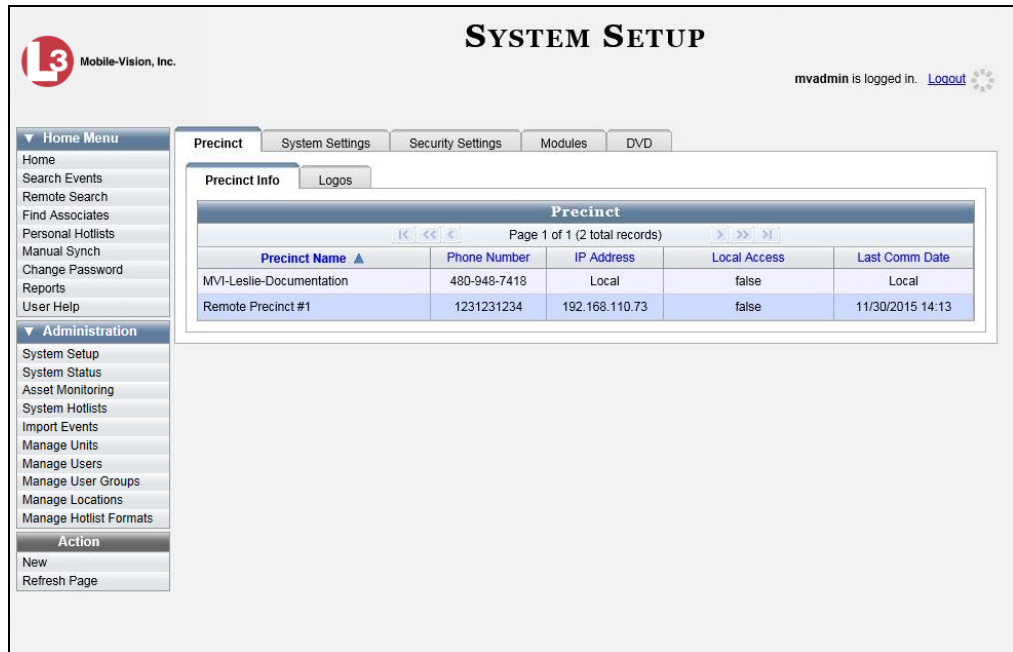❒ Deleting a Custom User Role, page 324.

Adding a Custom User Role

This section describes how to create a new user role. For more on user roles, refer to this chapter's introduction and/or "Custom User Roles" above.

Perform this task when you wish to create a user role that has a *unique name*. Otherwise you can simply customize the system-defined user roles that come with AlertVU, as described in "Changing the Settings for a System-Defined User Role" on page 310.

---

[*] Administrator, Officer, Supervisor, and View Only-Event

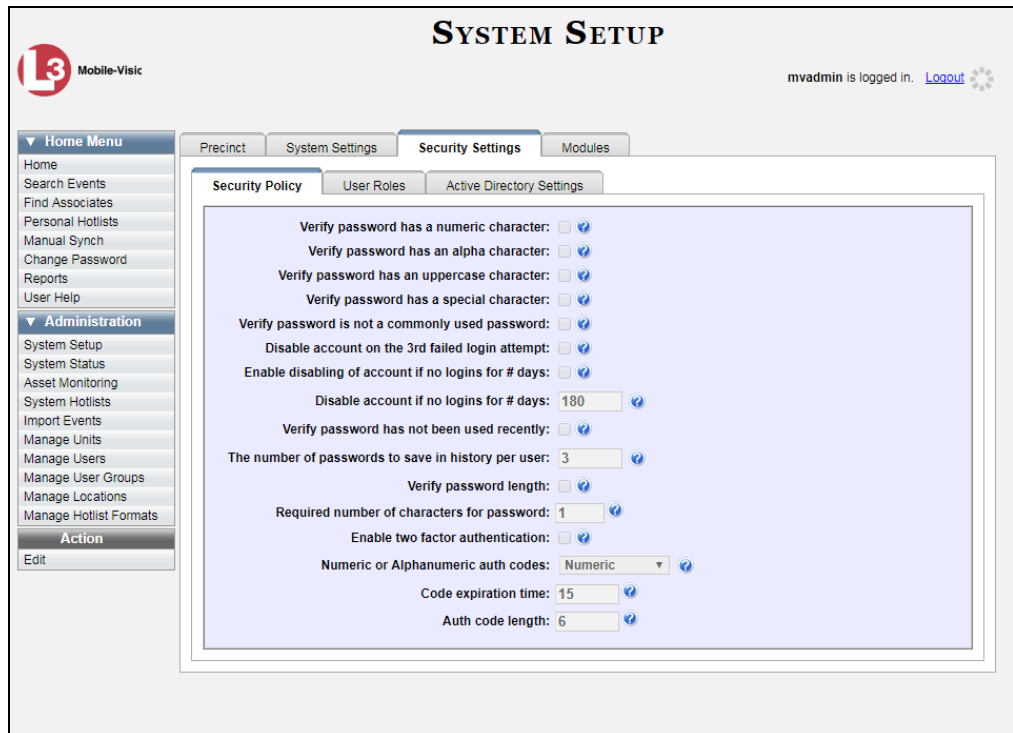**1** Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 Click the **Security Settings** tab.

3 Click the **User Roles** tab. A list of User Roles displays.

The columns on this form are described below.

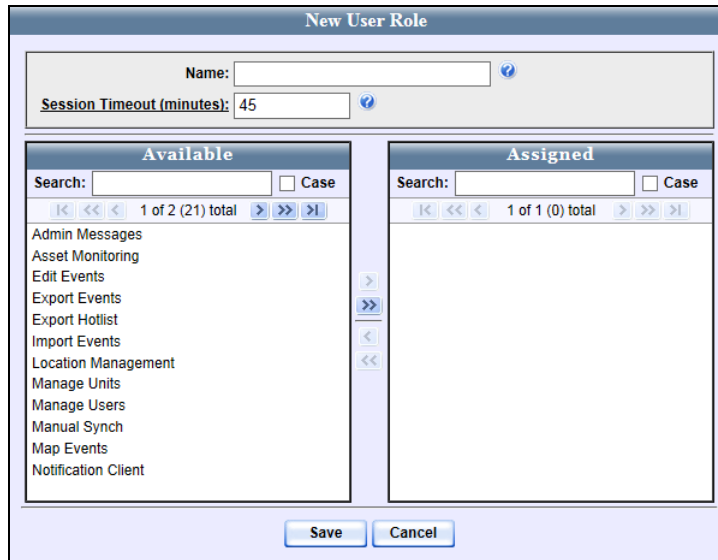| User Roles	
Column	**Description**
Display Name	The name of this user role. The *system-defined* user role names never change. They are: ▪ Administrator ▪ Officer ▪ Supervisor ▪ View Only–Event
AD Group Name *(Active Directory users only)*	The Active Directory Group that this user role belongs to, if applicable. This field will only display if your agency is using the Active Directory Integration feature, which links AlertVU to your agency's existing internal network.
Session Timeout (minutes)	The number of idle-time minutes that must pass before the system automatically logs a user with this user role off the system.
System Defined	A true/false indicator that denotes whether or not this user role is system-defined: **True** ....The user role is system-defined **False**...........The user role is *not* system-defined (i.e., it is user-defined)

L3 Mobile-Vision, Inc.

**4**   Go to the Action column and click **New**. The New User Role form displays.

5   Go to the *Name* field and enter the name you wish to give this custom user role.

6   If your agency is using the Active Directory Integration feature, go to the *AD Group Name* field and select the Active Directory group that is associated with this user role.

– OR –

If your agency is *not* using the Active Directory Integration feature, proceed to the next step.

7   If you want to keep the Session Timeout setting[*] at 45 minutes (default), proceed to the next step.

– OR –

If you want to increase/decrease the Session Timeout setting[*], go to the *Session Timeout (minutes)* field and enter a new value.

8   Go to the left column (Available) and click on each of the permissions you wish to assign to this user role. If a permission you're looking for does not appear on-screen, use the navigation arrows at the top of the column to scroll through the permissions list.

For a detailed description of permissions, see "Permissions for User Roles" in the table on page 308.

_____

[*]   The number of idle-time minutes that must pass before the system automatically logs a user off the system.

9 Once you've highlighted the desired permissions, click the ▸ icon located between the two columns. The selected permissions display in the right column (Assigned).
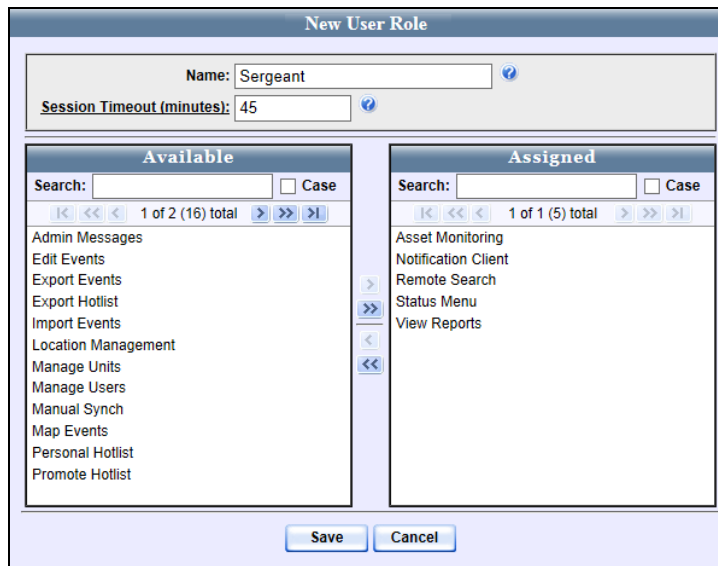
10 Click **Save**. The system analyzes your selections to make sure that they are logical. If there are any problems, the system will prompt you to make another selection.

Once you've saved the user role without any errors, a confirmation message displays.

**User Role Sergeant successfully saved.**

Changing a Custom User Role

This section describes how to change some or all of the following information for a custom user role:

❒ *User Role Name*
❒ *Session Timeout Minutes.*[*]
❒ *Permissions.* A user role's *permissions* determine what system functions a user will or will not be able to access. You can add/remove any number of permissions to/from a selected user role. For a list of permissions, see "Permissions for User Roles" in the table on page 308.

For more on user roles, refer to this chapter's introduction and/or "Custom User Roles" on page 316.
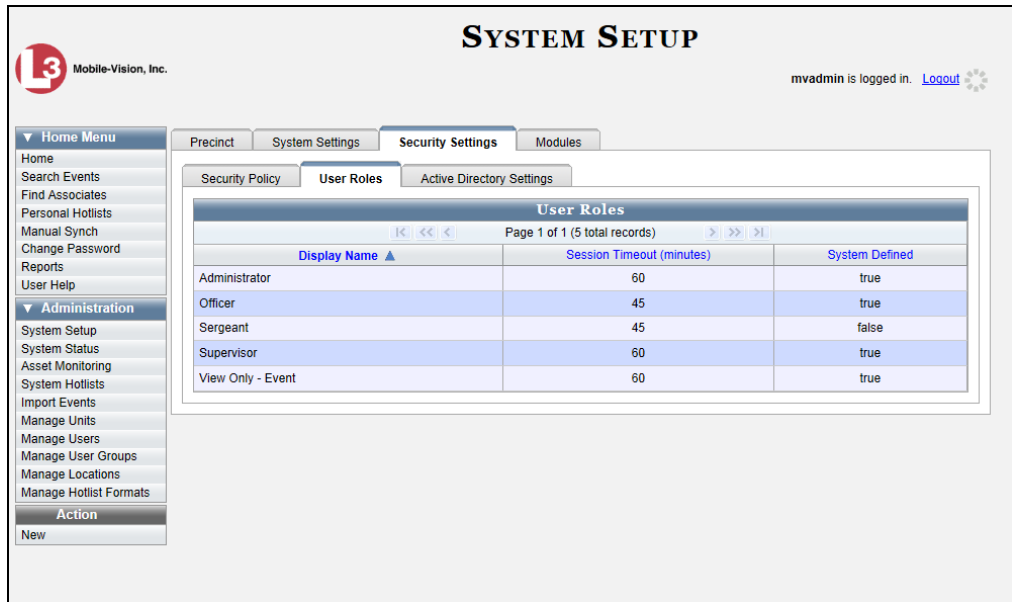
1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.
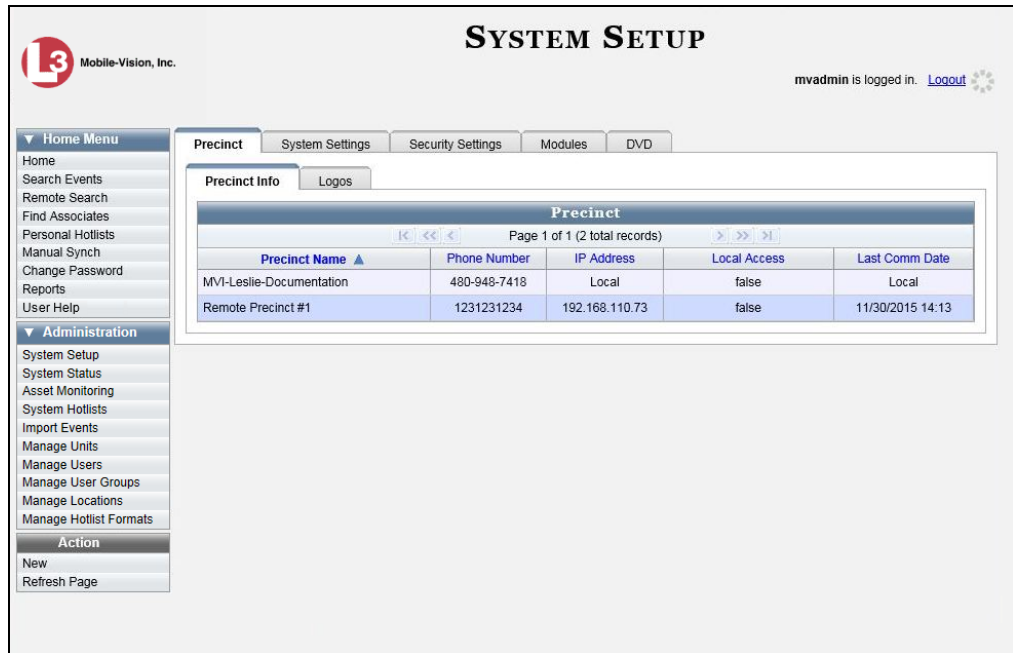
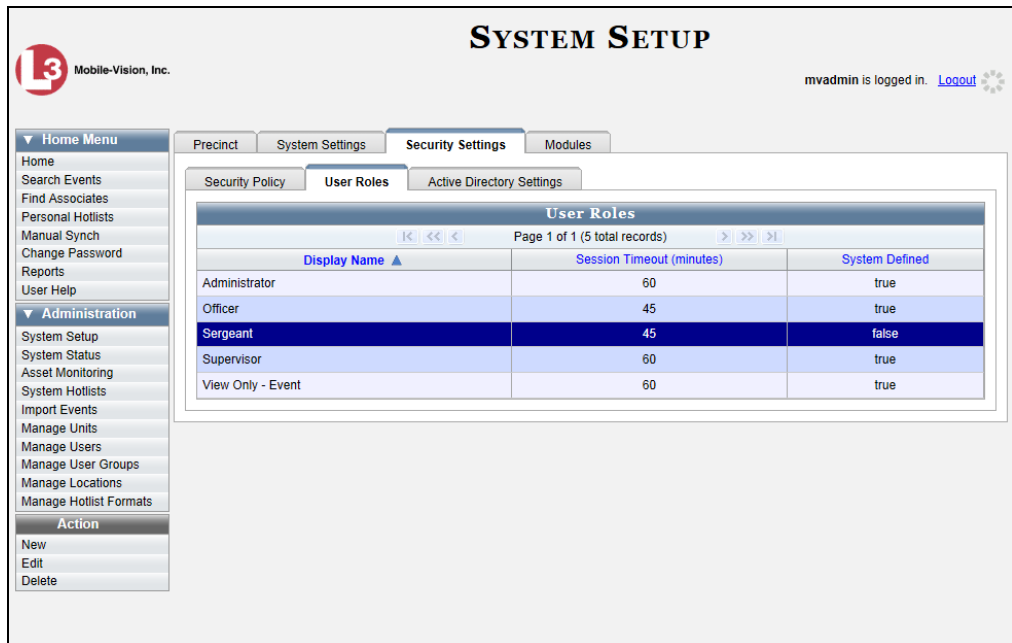**2** Click the **Security Settings** tab.
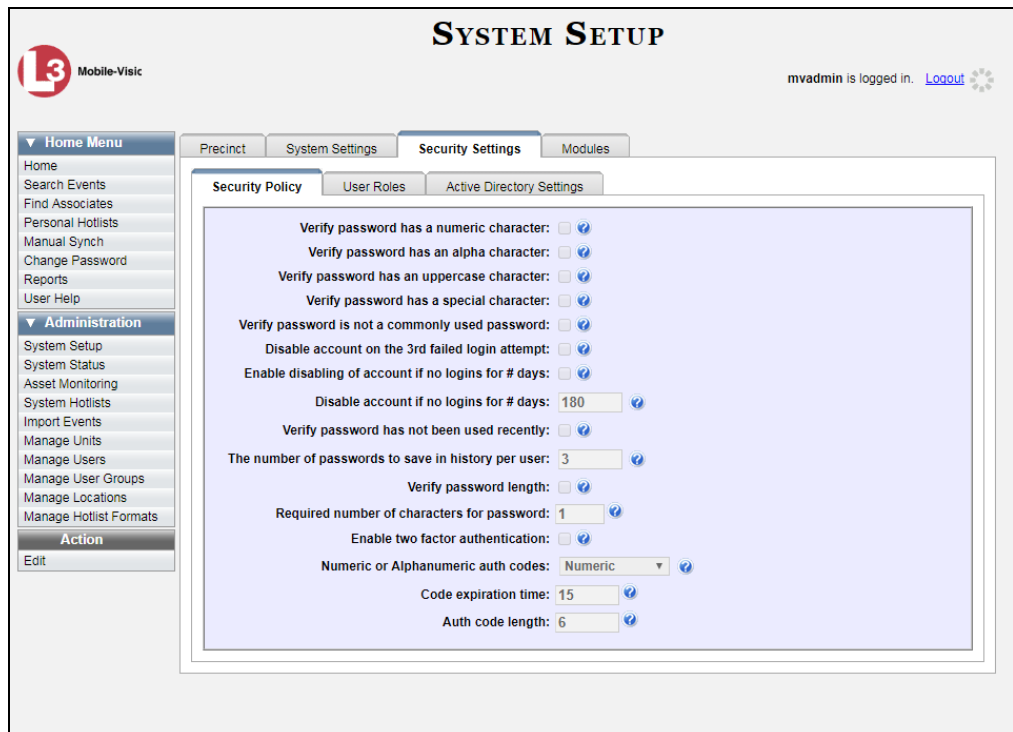
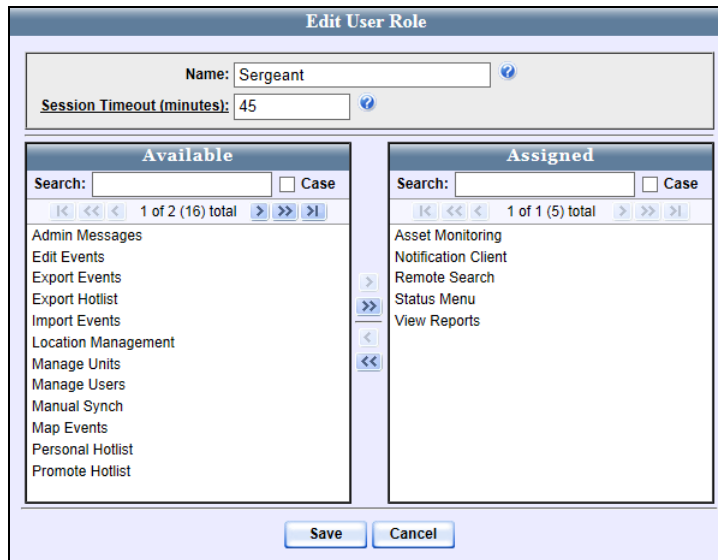**3** Click the **User Roles** tab. A list of User Roles displays.

For a description of the columns on this form, see the table on page 318.

**4** Click on the custom user role you wish to update.

5 Go to the Action column and click **Edit**.

– OR –

Right-click on the record, then select **Edit** from the popup menu.

The Edit User Role popup displays.

6 To change the name of this custom user role, enter a new value in the *Name* field. Otherwise proceed to the next step.

7 If your agency is using the Active Directory Integration feature, proceed to the next step. Otherwise skip to step 9.

8 To change the Active Directory group that is associated with this user role, select a new value from the *AD Group Name*. Otherwise proceed to the next step.

9 To change the Session Timeout setting[*] for this user role, proceed to the next step. Otherwise skip to step 11.

10 Enter a new value in the *Session Timeout (minutes)* field.

11 To add a permission to this user role, proceed to the next step. Otherwise skip to step 14.

12 Go to the left column (Available) and click on each of the permissions you wish to add. If a permission you're looking for does not appear on-screen, use the navigation arrows at the top of the column to scroll through the permissions list.

13 Once you've highlighted the desired permissions, click the ▸ icon located between the two columns. The selected permissions display in the right column (Assigned).

14 To *remove* permission(s) from this user role, proceed to the next step. Otherwise skip to step 17.

---

[*] The number of idle-time minutes that must pass before the system automatically logs a user off the system.

15 Go to the right column (*Assigned*) and click on each of the permissions you wish to remove.

16 Once you've highlighted the desired permissions, click the ◀ icon located between the two columns. The selected permissions are removed from the *Assigned* list.

17 Click **Save**. The system analyzes your selections to make sure that they are logical. If there are any problems, the system will prompt you to make another selection.
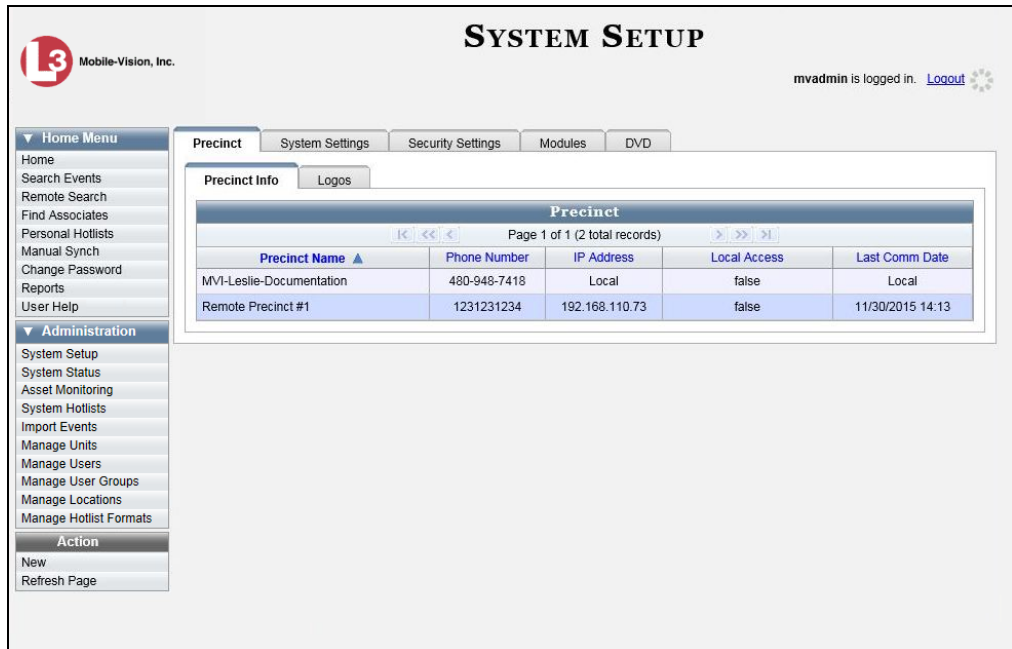
Once you've saved the user role without any errors, a confirmation message displays.

> **User Role Sergeant successfully saved.**

Deleting a Custom User Role

This section describes how to delete a custom user role that is not currently assigned to any users. If the user role you wish to delete *is* currently assigned to one or more users, you will have to change each user's role assignment first before you can perform this procedure, as described in chapter 8, "Changing a User."

1 Go to **▼ Administration** and click **System Setup**. The System Setup page displays.

2 Click the **Security Settings** tab.
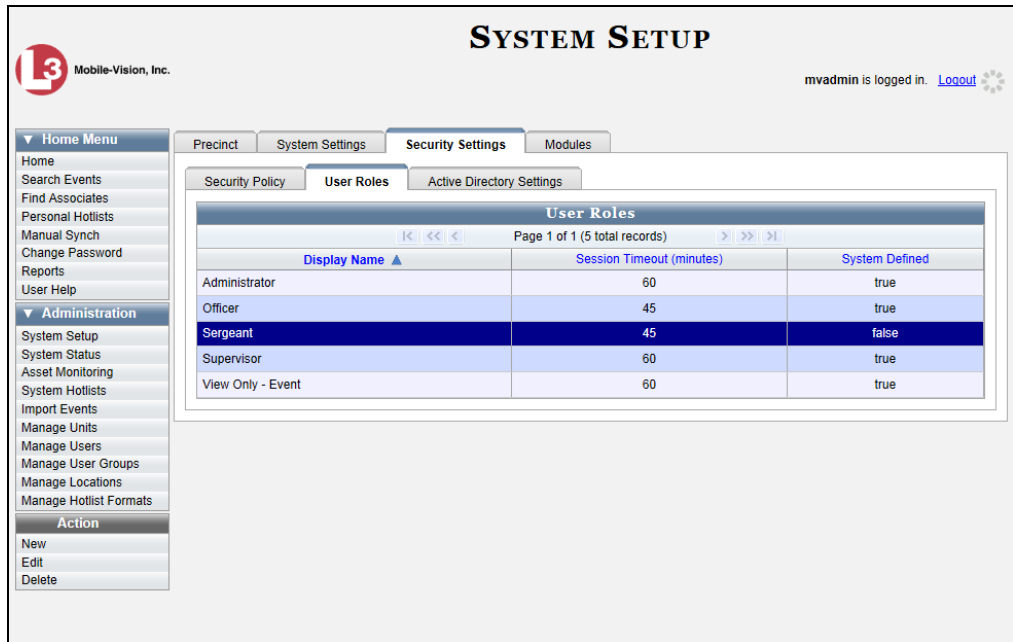
3 Click the **User Roles** tab. A list of User Roles displays.

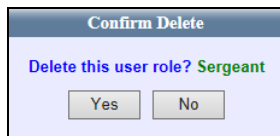**4** Click on the custom user role you wish to delete.

(Continued)

5 Go to the Action column and click **Delete**.

– OR –

Right-click on the record, then select **Delete** from the popup menu.
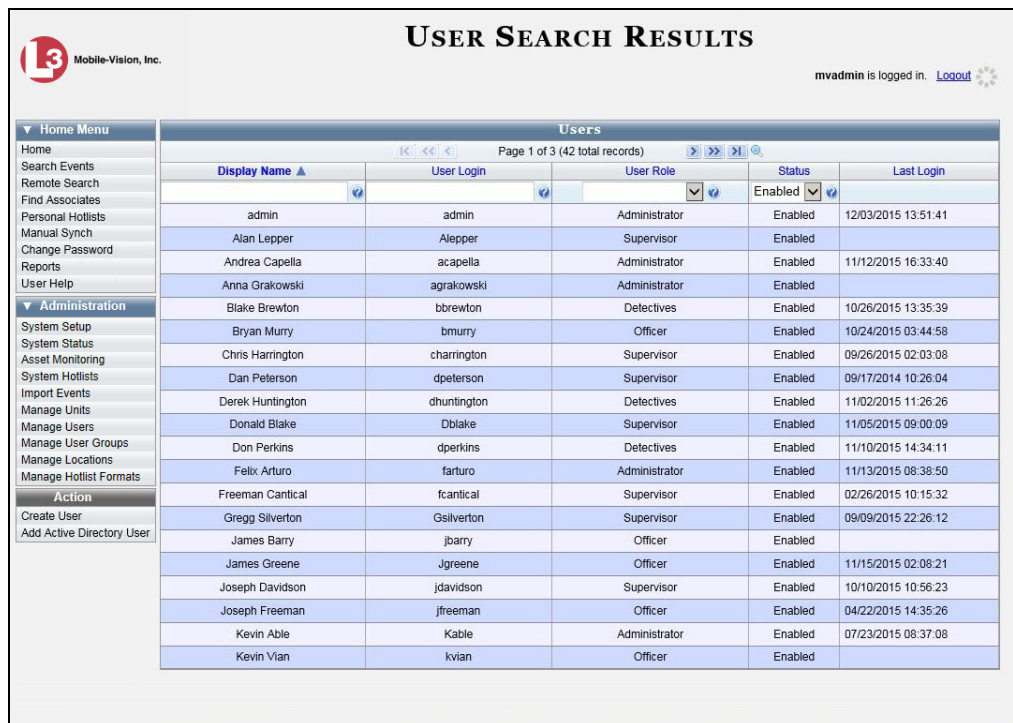
A confirmation message displays.

6 Click **Yes**. A confirmation message displays.

Assigning Permissions to a User

There are two ways in which you can assign permissions to a user. First, you can assign permissions at the same time you create a user. This method is described in chapter 8, "Adding a User." Second, you can assign permissions by changing an existing user's *role* and/or granting additional permissions to a user on an ad-hoc basis, as described in this section.

1 Go to ▼ Administration and click **Manage Users**. The User Search Results page displays.

2 If the user record you wish to update appears in the *Display Name* column, skip to step 4.

– OR –

If the user record you wish to update does *not* appear in the *Display Name* column, proceed to the next step.

3 Use the navigation arrows at the top of the form to scroll through the user list.

– OR –

Enter/select search criteria in the search field(s) provided. For detailed instructions, see "Searching for a User" in chapter 8.

4 Once the desired record appears in the *Display Name* column, click on it to select it.

5 Go to the Action column and click **Edit**.

– OR –

Right-click on the record, then select **Edit** from the popup menu.

The Edit User popup displays.

6 To change this user's *user role*, select a new role from the *User Role* drop-down list. Otherwise proceed to the next step.

7   Click the **Permissions** tab. A list of permissions displays.
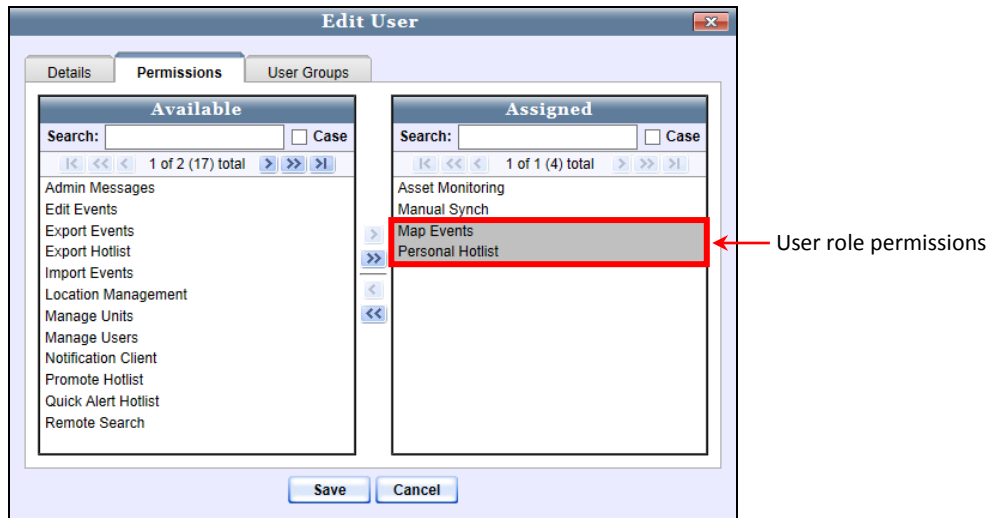
User role permissions

Please note that you cannot remove any of the permissions highlighted in gray. These are the permissions associated with the user's assigned *role*.
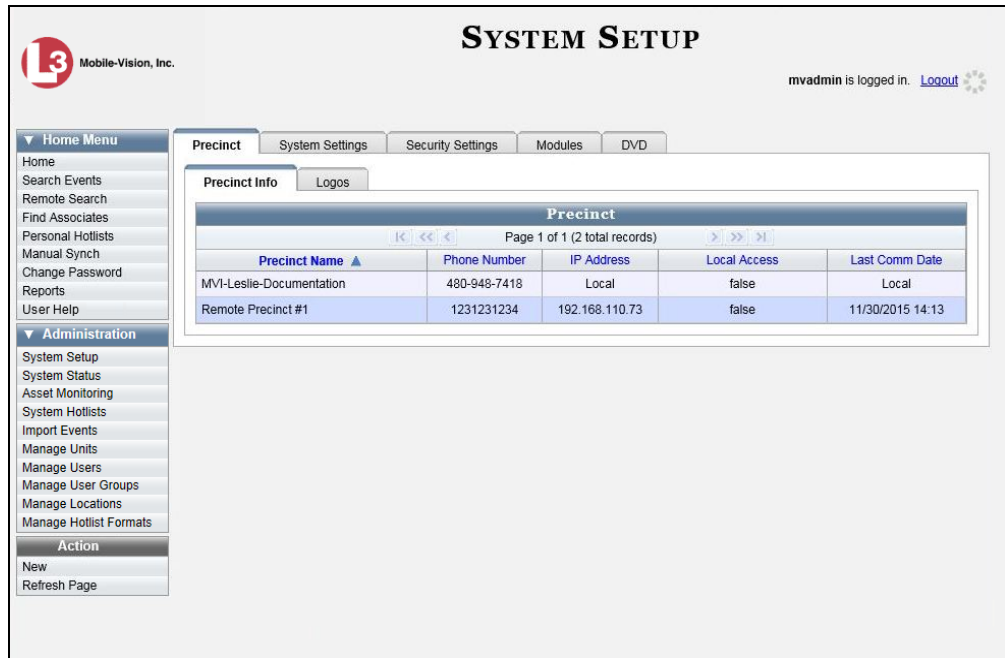
8   Review the current list of permissions for this user (highlighted in gray).

If you want to assign *additional* permissions to this user, proceed to the next step.

– OR –

If you do *not* want to assign additional permissions to this user (i.e., the default permissions are sufficient), skip to step 11.

9   Go to the left column (Available) and click on the additional permissions you wish to assign. If a permission you're looking for does not appear on-screen, use the navigation arrows at the top of the column to scroll through the permissions list.

10   Once you've highlighted the desired permissions, click the ▶ icon located between the two columns. The selected permissions display in the right column (Assigned).

11   Click **Save**. A confirmation message displays.

> **User dperkins successfully saved.**

Defining Password Policies

This section describes how to define the rules that apply to a user password. These include password length, password complexity, and the number of login attempts allowed before the system disables a password.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 Click the **Security Settings** tab.

3 Make sure that the **Security Policy** tab is selected.

4 Go to the Action column and click **Edit**. The Edit Security Policy popup displays.

The security options on this form are described in the table on the next page.

Edit Security Policy	
Security Option	**Description**
Verify password has a numeric character	When you select this checkbox, the system will check to make sure all new passwords contain at least one numeric character (e.g., 1 – 9).
Verify password has an alpha character	When you select this checkbox, the system will check to make sure all new passwords contain at least one alpha character (e.g., a – z).
Verify password has an uppercase character	When you select this checkbox, the system will check to make sure all new passwords contain at least one uppercase character (e.g., A – Z).
Verify password has a special character	When you select this checkbox, the system will check to make sure all new passwords contain at least one special character (e.g., ! @ # $ % &, etc.)
Verify password is not a commonly used password	When you select this checkbox, the system will check to make sure all new passwords do not match any of the passwords on the "common passwords" list. A copy of this list is found in the /fb/conf/word_list.txt file on the server. You can add more passwords to this file, if desired.
Disable account on the 3rd failed login attempt	When you select this checkbox, the system will lock a user out of the system after he has tried to login to the system three consecutive times using invalid User ID(s) and/or password(s).
Enable disabling of account if no logins for # days	This password function works in conjunction with the *Disable account if no logins for # days* field. It will disable a user's password if a user has not logged into AlertVU Back Office for **X** number of days, with **X** being the number entered in the *Disable account if no logins for # days* field.
Disable account if no logins for # days	This password function works in conjunction with the *Enable disabling of account if no logins for X days.* It indicates how many days of inactivity (i.e., no logins) must elapse before a user is locked out of the system.
Verify password has not been used recently	This password function works in conjunction with the *number of passwords to save in history per user* field. When you select this checkbox, the system will check to make sure that a password has not been used in **X** number of times, with **X** being the number entered in the *number of passwords to save in history per user* field.

Edit Security Policy (cont'd)	
Security Option	**Description**
The number of passwords to save in history per user	This password function works in conjunction with the *Verify password has not been used recently* field. It indicates the number of passwords to save in history per user. When a user is required to change their password, they will not be able to reuse any of the same passwords they have used since the last **X** number of times their password was changed.
Verify password length	This password function works in conjunction with the *Required number of characters for password* field. When you select this checkbox, the system will check to make sure that a password is **X** number of characters in length, with **X** being the number entered in the *Required number of characters for password* field.
Required number of characters for password	This password function works in conjunction with the *Verify password length* field. It indicates the required minimum length for each password. When you enter a number in this field, it means that all passwords must be a minimum of **X** characters in length.
Enable password expiration	When you select this checkbox, the system will prompt each user to reset their password **X** number of days after they last changed it, where **X** equals the number of days entered in the *Password expiration time* field. *To enable the Password Expiration feature, select this checkbox. To disable the Password Expiration feature, deselect this checkbox.*
Password expiration time	The number of days following a password change that a given password will expire. For example, if you enter **30** here, then every 30 days after a user changes his password, the system will prompt him to change it again. If he fails to do so, he will be locked out of the system. *Enter a number in the field provided.*
Enable two factor authentication	The *two factor authentication* feature prompts users to enter an Authentication Code each time they attempt to login to AlertVU Back Office. This Authentication Code is automatically generated by the system and sent to the email address associated with the officer's User ID. For this reason, agencies who use this feature *must* ensure that all user records include an email address. If one or more user records are *missing* an email address, the system will prevent those users from logging in. To implement two-factor authentication logins, first select this checkbox, then enter/select a value in the following fields: *(Continued)*

Edit Security Policy (cont'd)	
Security Option	**Description**
Enable two factor authentication (cont'd)	▪ Numeric or Alphanumeric auth codes ▪ Code expiration time ▪ Auth code length For specific instructions on logging into the system using the two-factor authentication feature, see "Logging into the System" in chapter 1`. *To <u>enable</u> Two Factor Authentication, select this checkbox. To <u>disable</u> Two Factor Authentication, deselect this checkbox.*
Numeric or Alphanumeric auth codes	The type of characters you wish to use for your Authentication Codes: *Numeric* (numbers only), or *Alphanumeric* (numbers and letters). *Select a value from the drop-down list.*
Code expiration time	The number of minutes that an Authentication Code will expire after the system has emailed it to a user. Once a code expires, a user can no longer use it to login. In that instance, the user must click the **Resend** button on the Authentication Code popup to generate a new code. *Enter a number in the field provided.*
Auth code length	The number of characters for your Authentication Code. System default is 6 characters. *Enter a number in the field provided.*

5 Review the first six security options and check those security features you wish to use.

6 If you want a user's account to be disabled after that user has not logged into the system for a certain number of days, proceed to the next step. Otherwise skip to step 9.

7 Select the *Enable disabling of account if no logins for # days* checkbox.

8 Proceed to the *Disable account if no logins for # days* field and enter the number of days of inactivity (i.e., no logins) that must elapse before a user is locked out of the system.

9 If you don't want your users to be able to re-use recent passwords, proceed to the next step. Otherwise skip to step 12.

10 Select the *Verify password has not been used recently* checkbox.

11 Proceed to the *number of passwords to save in history per user* field and enter the number of unique passwords that each user must save in history.

12 To set a minimum required length for passwords, proceed to the next step. Otherwise skip to step 15.

13 Select the *Verify password length* checkbox.

14 Proceed to the *Required number of characters for password* field and enter the minimum number of characters that your passwords must have.

15 If you wish to enable the Password Expiration feature, select the *Enable password expiration* checkbox (see *Enable password expiration* field on page 333). Proceed to the next step.

– OR –

If you do *not* wish to enable the Password Expiration feature, skip to step 17.

16 Proceed to the *Password expiration time* field and enter the frequency, in days, with which you want the system to prompt users to reset their passwords (e.g., **60** for *every 60 days*).

17 If you wish to enable the *two factor authentication* feature (see *Enable two factor authentication* field on page 333), select the *Enable two factor authentication* checkbox. Proceed to the next step.

– OR –

If you do *not* wish to enable the *two factor authentication* feature, skip to step 20.

WARNING: If you selected the *Enable two factor authentication* checkbox, you **must** have a valid email address saved to each officer's user record. Any user that does *not* have a valid email address will be locked out of the application. For more information, see "Changing a User" in chapter 8.
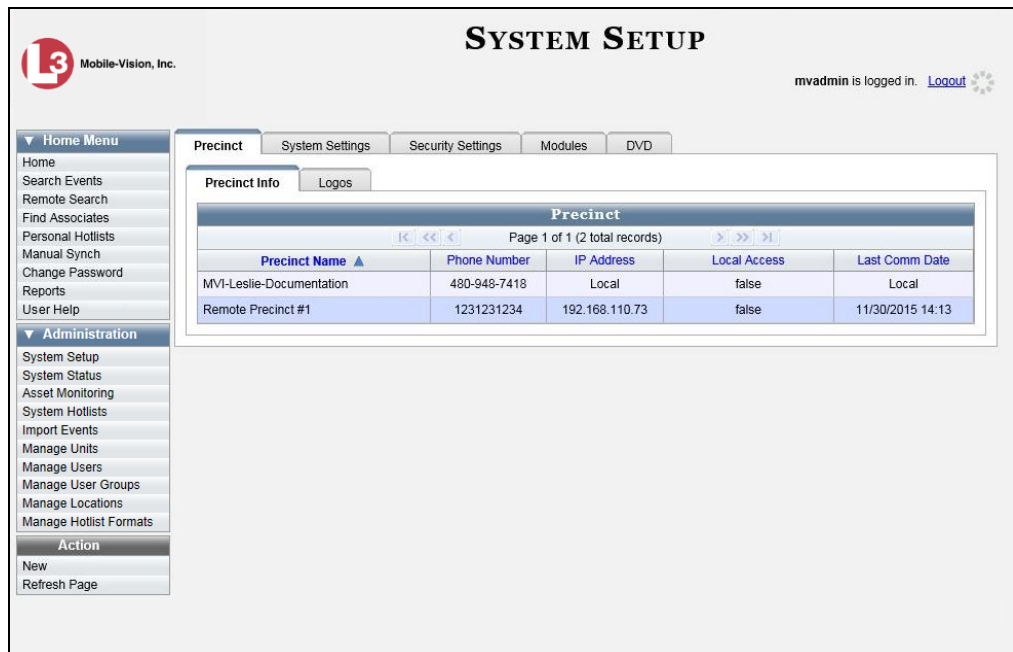
18 If you want your Authentication Codes to be comprised of numbers only (default), proceed to the next step.

– OR –

If you want your Authentication Codes to be comprised of numbers and letters, select **Alphanumeric** from the *Numeric or Alphanumeric auth codes* drop-down list.

19 Enter the number of minutes that an Authentication Code will expire after the system has emailed it to a user.

20 Click **Save**.

Changing Security Log Settings

Security logs are records that document various activities on the server, such as hotlist creation and event searches. These records tell you *what* activities were performed, *who* performed them, and *when* they were performed.

This section describes how to change the settings related to the capture and retention of security logs, including:

❒ The type of security logs that AlertVU will track (i.e., *system level* or *system level + user level*)
❒ The number of days that AlertVU will keep security logs on the server.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 Click the **System Settings** tab.

3 Click the **System Options** tab.

4 Go to the Action column and click **Edit**. The System Options popup displays.

(Continued)

5 To change the security log level, proceed to the next step. Otherwise skip to step 7.

6 Select a new value from the *Security Log Level* drop-down list:

All..............Log system-level activity *and* user-level activity
System.......Log system-level activity only

7 To change the number of days that you wish to keep security logs on the server, enter a new value in the *Days to Retain Security Logs* field. Otherwise proceed to the next step.

8 Click **Save**.

8 Users

There are two methods for entering and maintaining user records in AlertVU: *directly*, as described in "Maintaining Users in AlertVU" on page 341, or through your agency's existing internal network, as described in "Using the Active Directory Integration Feature" on page 365.

The Active Directory Integration feature enables you to integrate AlertVU with your agency's existing Windows Active Directory or Novell eDirectory. This feature allows for a single password authentication with your agency's internal network, eliminating the need to maintain two sets of User IDs and passwords. It also allows you to import existing network users into the system. If you choose to use this feature, your Systems Installation Specialist (SIS) will assist you in setting up your Active Directory. After that, you only have to update the user list periodically as needed.

AlertVU also includes a "user groups" option that enables you to group like users together (such as users that share the same role or are in the same department) and assign hotlists to those groups. This allows you to assign hotlists to multiple users at the same time.

For more information, see:

❒ Searching for a User, below
❒ Maintaining Users in AlertVU, page 341
❒ Managing User Groups, page 354
❒ Using the Active Directory Integration Feature, page 365
❒ Generating the User Activity Report, page 374.

Searching for a User

This section describes how to search for an existing user record by one or more of the following fields: *Display Name*, *User Login*, *User Role*, and/or *Status*.

1 Go to ▼ Administration and click **Manage Users**. The User Search Results page displays.

(Continued)

Note the search fields at the top of the page.

2 Enter/select the field values you wish to search on, as described below.

Search Field	Description
Display Name	Limits your search to those users who have this text in their display name.
User Login	Limits your search to those users who have this text in their User ID.
User Role	Limits your search to those users who are assigned this user role. For more on user roles, see chapter 7. *Select the appropriate user role from the drop-down list.*
Status	Limits your search to those users who have a status of either **Enabled** or **Disabled**. *Select the appropriate status from the drop-down list.*

After you enter a search value, the system will automatically display those records that match your search criteria.

3 If your search results are more than one page long, use the navigation buttons at the top of the user list to scan through the remaining search results.

Maintaining Users in AlertVU

This section describes how to add, change, and/or delete user records in AlertVU. These procedures only apply to those users who are *not* using the Active Directory Integration feature, which integrates AlertVU with your agency's existing internal network. If your agency *is* using the Active Directory Integration feature, see "Maintaining Users in Active Directory" on page 365 instead.

For specific instructions, see:

❒ Adding a User, below
❒ Changing a User, page 347
❒ Deleting a User, page 351.

Adding a User

This section describes how to enter a new user record in AlertVU. If your agency is using the Active Directory Integration feature, see "Maintaining Users in Active Directory" on page 365 instead.

Before you add users for the first time, it's important to define your user roles. For more information, see "User Roles" in chapter 7.

> **WARNING**: If your agency is using the two factor authentication login feature, you **must** enter a valid email address for each user. Any user that does *not* have a valid email address saved to their user record will be locked out of the application.

1 Go to ▼ Administration and click **Manage Users**. The User Search Results page displays.

USER SEARCH RESULTS

mvadmin is logged in. Logout

▼ Home Menu					
Home					
Search Events					
Remote Search					
Find Associates		**Users**			
Personal Hotlists	Page 1 of 3 (42 total records)				
Manual Synch	**Display Name ▲**	**User Login**	**User Role**	**Status**	**Last Login**
Change Password				Enabled	
Reports	admin	admin	Administrator	Enabled	12/03/2015 13:51:41
User Help	Alan Lepper	Alepper	Supervisor	Enabled	
▼ Administration	Andrea Capella	acapella	Administrator	Enabled	11/12/2015 16:33:40
System Setup	Anna Grakowski	agrakowski	Administrator	Enabled	
System Status	Blake Brewton	bbrewton	Detectives	Enabled	10/26/2015 13:35:39
Asset Monitoring	Bryan Murry	bmurry	Officer	Enabled	10/24/2015 03:44:58
System Hotlists	Chris Harrington	charrington	Supervisor	Enabled	09/26/2015 02:03:08
Import Events	Dan Peterson	dpeterson	Supervisor	Enabled	09/17/2014 10:26:04
Manage Units	Derek Huntington	dhuntington	Detectives	Enabled	11/02/2015 11:26:26
Manage Users	Donald Blake	Dblake	Supervisor	Enabled	11/05/2015 09:00:09
Manage User Groups	Don Perkins	dperkins	Detectives	Enabled	11/10/2015 14:34:11
Manage Locations	Felix Arturo	farturo	Administrator	Enabled	11/13/2015 08:38:50
Manage Hotlist Formats	Freeman Cantical	fcantical	Supervisor	Enabled	02/26/2015 10:15:32
Action	Gregg Silverton	Gsilverton	Supervisor	Enabled	09/09/2015 22:26:12
Create User	James Barry	jbarry	Officer	Enabled	
Add Active Directory User	James Greene	Jgreene	Officer	Enabled	11/15/2015 02:08:21
	Joseph Davidson	jdavidson	Supervisor	Enabled	10/10/2015 10:56:23
	Joseph Freeman	jfreeman	Officer	Enabled	04/22/2015 14:35:26
	Kevin Able	Kable	Administrator	Enabled	07/23/2015 08:37:08
	Kevin Vian	kvian	Officer	Enabled	

2 Go to the Action column and click **Create User**. The New User popup displays.

New User

Details	Permissions	User Groups

Display Name:

User Name:

Email Address:

User Password:

Repeat User Password:

Status: Enabled

User Role:

Notifications:

Inbox ☐

E-mail ☐

Live Alerts ☐

Save   Cancel

The fields on this form are described below.

New User Form	
Field	**Description**
Display Name	The name used to represent this user throughout the AlertVU application. This name will appear on application pages, reports, etc.
User Name	The user's login ID. This is the text that the user enters in the *User Name* field to login to the application.
Email Address	The user's email address. If your agency is using the two-factor authentication login feature, this field is required.
User Password	The user's login password. This is the text that the user enters in the *Password* field to login to the application. For security reasons, this value does not display on the screen as you type it. **Note**: After a new user logs into the application for the first time, he should change his user password, as described in chapter 1, "Changing Your Password."
Repeat User Password	Same as *User Password* above. The system requires that you type the password a second time to verify your entry.
Status	The current status of this user: ▪ *Enabled*. The user is allowed to login to the application. ▪ *Disabled*. The user is *not* allowed to login to the application.
User Role	The name of the permissions group that is assigned to this user. This designation determines what system features the user will or will not be able to access. For more on user roles, see "User Roles" in chapter 7.
Notifications	The type(s) of notifications that this user will receive when an AlertVU unit receives a hit on a license plate that's on either one of the user's personal hotlists *or* a system hotlist for which the user has Notification rights. You may select more than one notification type. ▪ *Inbox*. A message sent to the user's *Inbox Messages* list on the Home page. ▪ *E-mail*. A message sent to the user's regular email account. In order to receive this type of alert, you must supply the system with information on your agency's SMTP mail server, as described in chapter 6, "Forwarding System Messages to Your Regular Mailbox." *(Continued)*

| New User Form (cont'd)	
Field	**Description**
Notifications (cont'd)	▪ *Real Time Alerts* (system alerts only). A real-time popup which displays on the user's PC desktop. In order to receive this type of notification, the user must activate the Live Alert Utility on his PC whenever he logs in, as described in "Activating the Live Alert Utility" in chapter 3.
	For more on alerts and how they are set up at the hotlist level, see "Alerts" in chapter 3.
	WARNING: If you select the *Inbox* and/or *Email* notifications, please be aware that you may receive dozens or even hundreds of notifications per day. You will have to review and delete these notifications daily.

3 Enter an officer display name in the *Display Name* field. This is the name that will display throughout the application.

4 Enter a user login ID in the *User Name* field.

5 Enter the user's email address in the *Email Address* field.

6 Enter the user's initial login password in the *User Password* field. This is password that the user will use to login to the application for the first time.

7 Re-enter the user's initial login password in the *Repeat User Password* field.

8 If you want this user to be able to login to the application immediately (default), proceed to the next step.

– OR –

If you do *not* want this user to be able to login to the application immediately, select **Disabled** from the *Status* drop-down list. If you do so, remember that the account must be enabled before the user will be allowed to login.

9 Select a user role from the *User Role* drop-down list. For more information on user roles and how they are created/modified, see chapter 7.

10 Go to the *Notifications* column and select the type(s) of system alerts that this user will receive. For a description of these alerts, see *Notifications* on page 343.

11 Click the **Permissions** tab. A list of grayed-out permissions displays in the right column. These are the permissions associated with the user's assigned *user role*. (i.e., the role you just selected from the *User Role* drop-down list). You cannot remove any of these permissions. However, you *can* assign additional permissions to the user.

L3 Mobile-Vision, Inc.
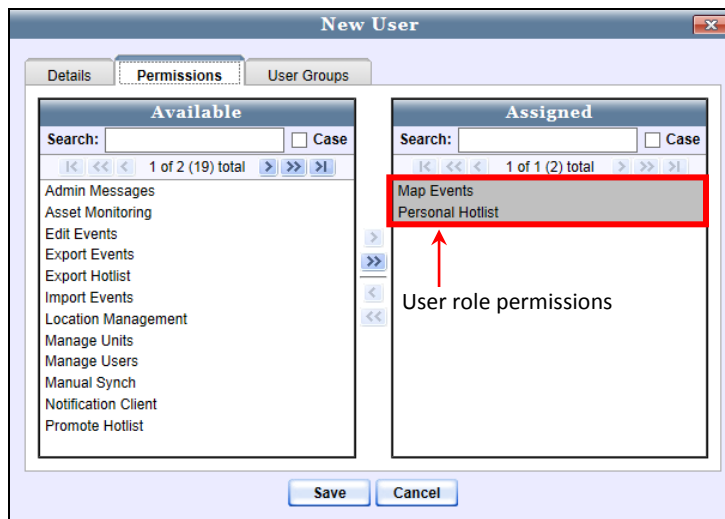
12 Review the current list of permissions for the new user (highlighted in gray).

If you wish to assign *additional* permissions to this user, proceed to the next step.

– OR –

If you do *not* wish to assign additional permissions to this user (i.e., the permissions displayed in the right column are sufficient), skip to step 15.

13 Go to the left column (Available) and click on the additional permissions you wish to assign. If you don't see a permission you're looking for, use the navigation arrows at the top of the column to scroll through the list.

14 Once you've highlighted the desired permissions, click the ▶ icon located between the two columns. The selected permissions display in the right column (Assigned).
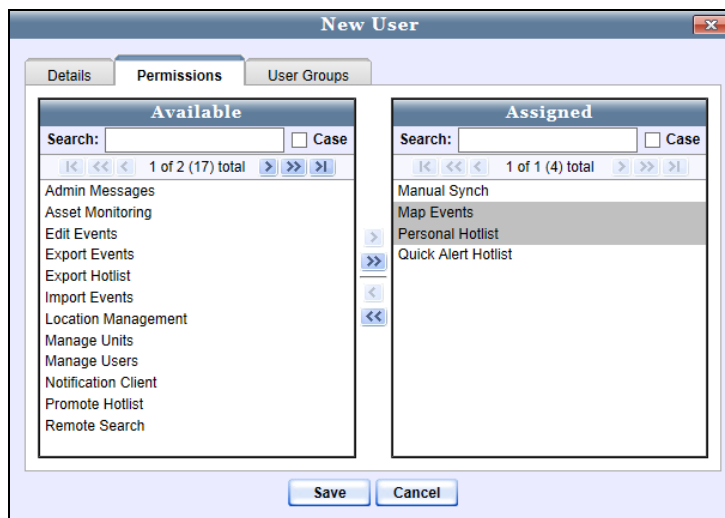
15 To assign this user to a predefined user group, proceed to the next step. Otherwise skip to step 19.

16 Click the **User Groups** tab.
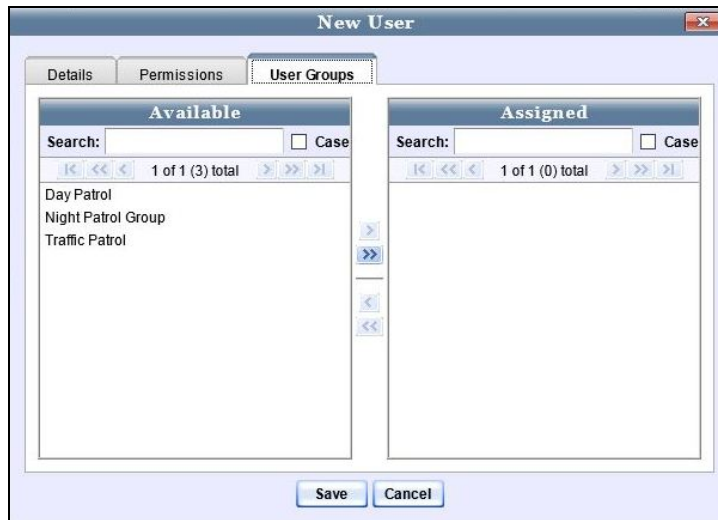
17 Go to the left column (Available) and click on the user group that you wish to assign this user to.

18 Click the ▷ icon located between the two columns. The selected user group displays in the right column (Assigned).
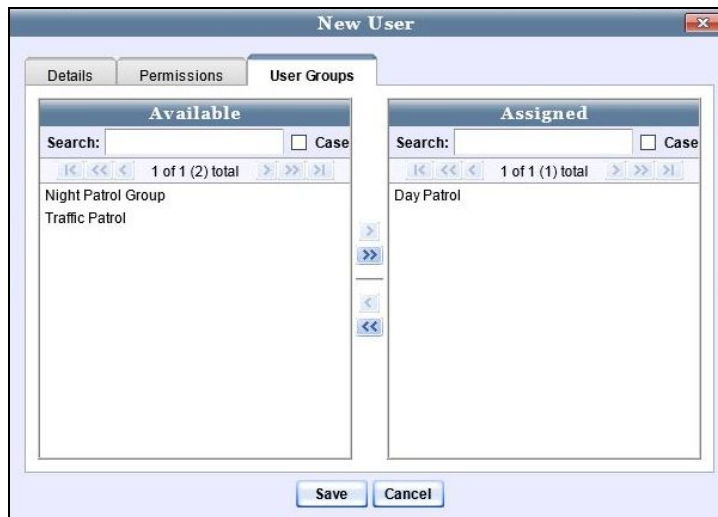
19 Click **Save**. A confirmation message displays.

> **User Officer McDonnell successfully saved.**

Changing a User

This section describes how to change an existing user record in AlertVU. If your agency is using the Active Directory Integration feature, see "Maintaining Users in Active Directory" on page 365 instead.

1 Go to ▼ Administration and click **Manage Users**. The User Search Results page displays.

2 If the user record you wish to update appears in the *Display Name* column, skip to step 4.

– OR –

If the user record you wish to update does *not* appear in the *Display Name* column, proceed to the next step.

3 Use the navigation arrows at the top of the form to scroll through the user list.

– OR –

Enter/select search criteria in the search field(s) provided. For detailed instructions, see "Searching for a User" on page 339.

4 Once the desired record appears in the *Display Name* column, click on it to select it.

5 Go to the [Action] column and click **Edit**.

– OR –
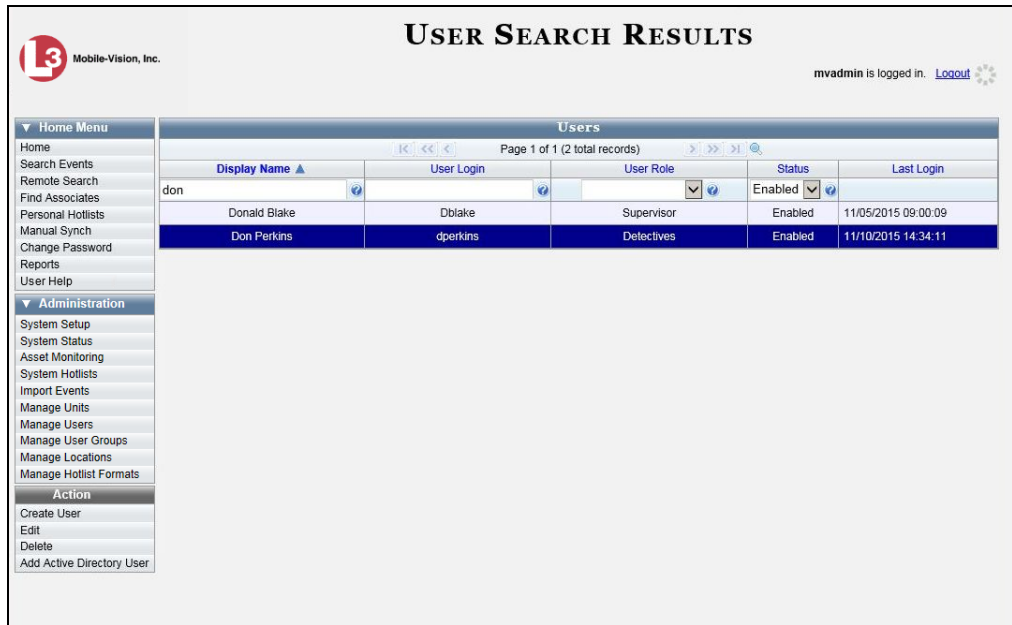
Right-click on the record, then select **Edit** from the popup menu.

The Edit User form displays.

The fields on the Edit User form are described in the table on page 343.

6 Enter/select your changes in the appropriate field(s).

⚠️ **WARNING:** If you select the *Inbox* and/or *Email* notifications, please be aware that you may receive dozens or even hundreds of notifications per day. You will have to review and delete these notifications on a daily basis.

7 To assign additional permissions to this user, proceed to the next step. Otherwise skip to step 11.

8 Click the **Permissions** tab. A list of permissions displays.
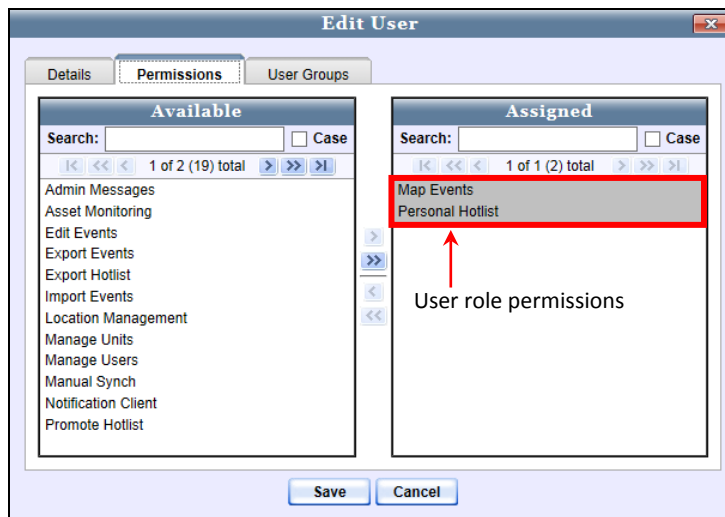
Please note that you cannot remove any of the permissions highlighted in gray. These are the permissions associated with the user's assigned *user role*.

9 Go to the left column (Available) and click on the new permissions you wish to assign. If a permission you're looking for does not appear on-screen, use the navigation arrows at the top of the column to scroll through the permissions list.

10 Once you've highlighted the desired permissions, click the ▶ icon located between the two columns. The selected permissions display in the right column (Assigned).

(Continued)
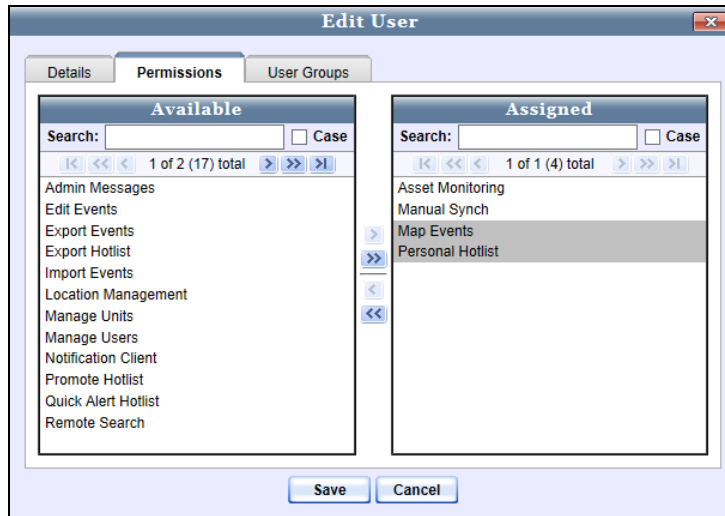
11 To assign this user to a predefined user group, proceed to the next step. Otherwise skip to step 15.

12 Click the **User Groups** tab.
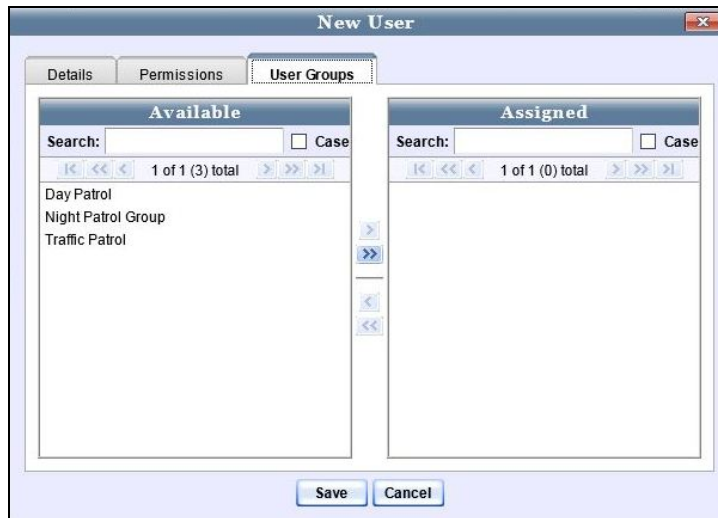
13 Go to the left column (Available) and click on the user group that you wish to assign this user to.

14 Click the ▶ icon located between the two columns. The selected user group displays in the right column (Assigned).
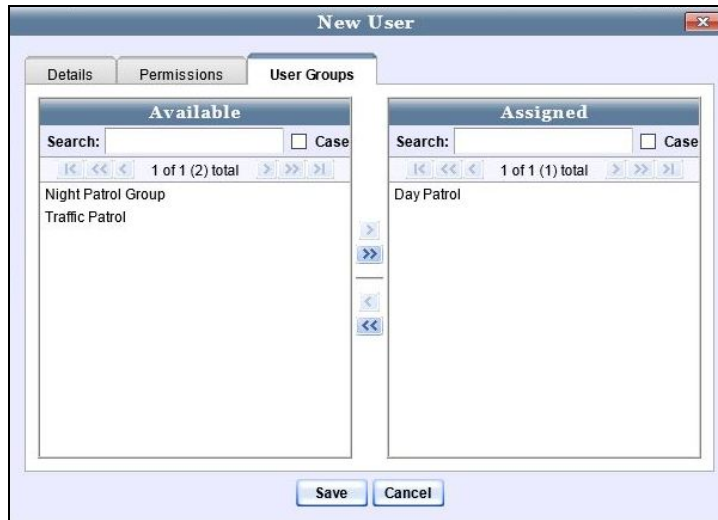
15 Click **Save**. A confirmation message displays.

User Marcus Welby **successfully saved.**

Deleting a User

This section describes how to delete an existing user record in AlertVU. If your agency is using the Active Directory Integration feature, see "Maintaining Users in Active Directory" on page 365 instead.

NOTE: For security purposes, if a user has any logged activity, they cannot be deleted.

1 Go to ▼ Administration and click **Manage Users**. The User Search Results page displays.

(Continued)

USER SEARCH RESULTS

mvadmin is logged in. Logout

Display Name ▲	User Login	User Role	Status	Last Login
admin	admin	Administrator	Enabled	12/03/2015 13:51:41
Alan Lepper	Alepper	Supervisor	Enabled	
Andrea Capella	acapella	Administrator	Enabled	11/12/2015 16:33:40
Anna Grakowski	agrakowski	Administrator	Enabled	
Blake Brewton	bbrewton	Detectives	Enabled	10/26/2015 13:35:39
Bryan Murry	bmurry	Officer	Enabled	10/24/2015 03:44:58
Chris Harrington	charrington	Supervisor	Enabled	09/26/2015 02:03:08
Dan Peterson	dpeterson	Supervisor	Enabled	09/17/2014 10:26:04
Derek Huntington	dhuntington	Detectives	Enabled	11/02/2015 11:26:26
Donald Blake	Dblake	Supervisor	Enabled	11/05/2015 09:00:09
Don Perkins	dperkins	Detectives	Enabled	11/10/2015 14:34:11
Felix Arturo	farturo	Administrator	Enabled	11/13/2015 08:38:50
Freeman Cantical	fcantical	Supervisor	Enabled	02/26/2015 10:15:32
Gregg Silverton	Gsilverton	Supervisor	Enabled	09/09/2015 22:26:12
James Barry	jbarry	Officer	Enabled	
James Greene	Jgreene	Officer	Enabled	11/15/2015 02:08:21
Joseph Davidson	jdavidson	Supervisor	Enabled	10/10/2015 10:56:23
Joseph Freeman	jfreeman	Officer	Enabled	04/22/2015 14:35:26
Kevin Able	Kable	Administrator	Enabled	07/23/2015 08:37:08
Kevin Vian	kvian	Officer	Enabled	

Page 1 of 3 (42 total records)

2 If the user record you wish to delete appears in the *Display Name* column, skip to step 4.

– OR –

If the user record you wish to delete does *not* appear in the *Display Name* column, proceed to the next step.

3 Use the navigation arrows at the top of the form to scroll through the user list.

– OR –

Enter/select search criteria in the search field(s) provided. For a description of these fields, see the table on page 343.

4 Once the desired record displays in the *Display Name* column, click on that record to select it.
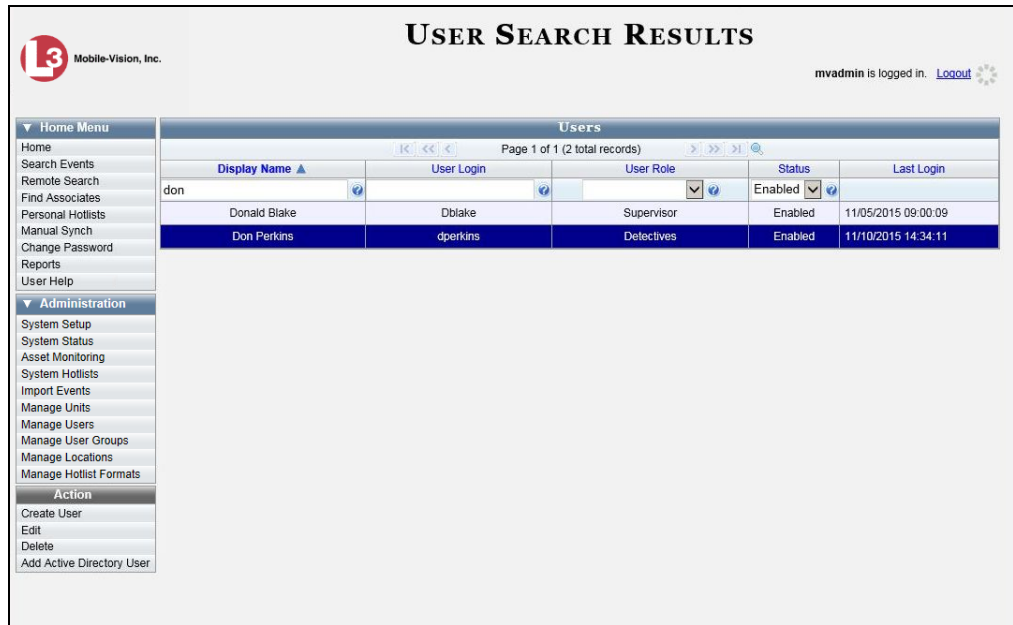
5 Go to the Action column and click **Delete**.

– OR –

Right-click on the record, then select **Delete** from the popup menu.

A confirmation message displays.

6 Click **Delete**. The selected user record is removed from the system.

Managing User Groups

The *user groups* feature allows you to combine like users for the purpose of assigning hotlists to them. For example, you might create a "Patrol Officer" group, then assign three hotlists to that group. The advantage of using user groups is that they enable you to assign hotlists to multiple users at the same time. To narrow the hotlist hit pool, you can also assign unit(s) to a user group. That will enable a user group's assignees to receive hotlist hits on *some*, but not *all* units For example, if user group "Patrol Officer" is assigned hotlist "ABC" and unit "XYZ", then the users assigned to that group will only receive hotlist alerts for hits on hotlist "ABC" that are captured from unit "XYZ."
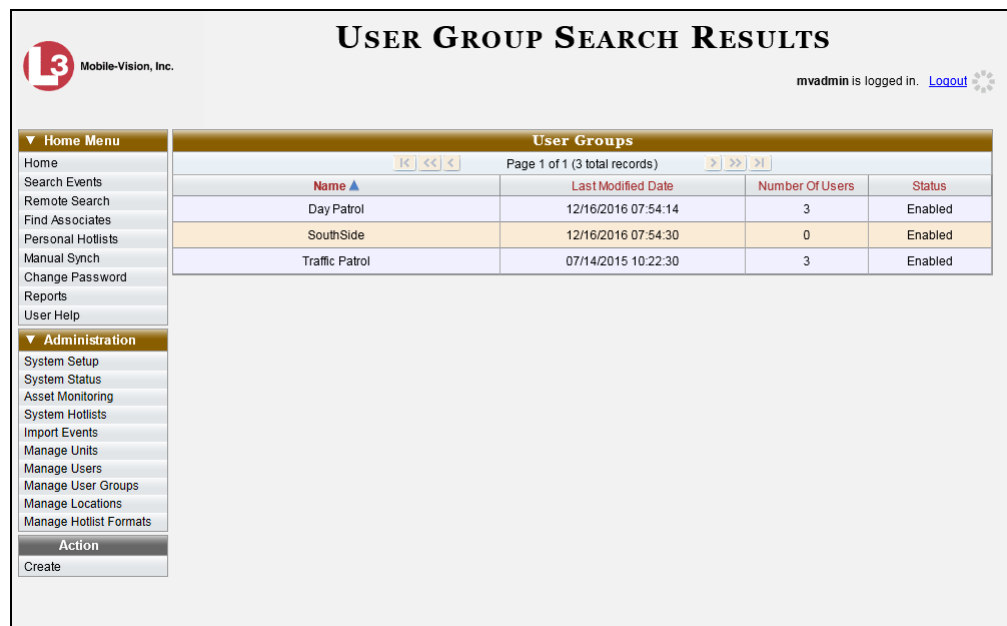
For more information, see:

❒ Adding a User Group, below
❒ Changing a User Group, page 359
❒ Deleting a User Group, page 364.

Adding a User Group

This section describes how to enter a new user group. For more on user groups and how they are used in AlertVU, see the previous section, "Managing User Groups."
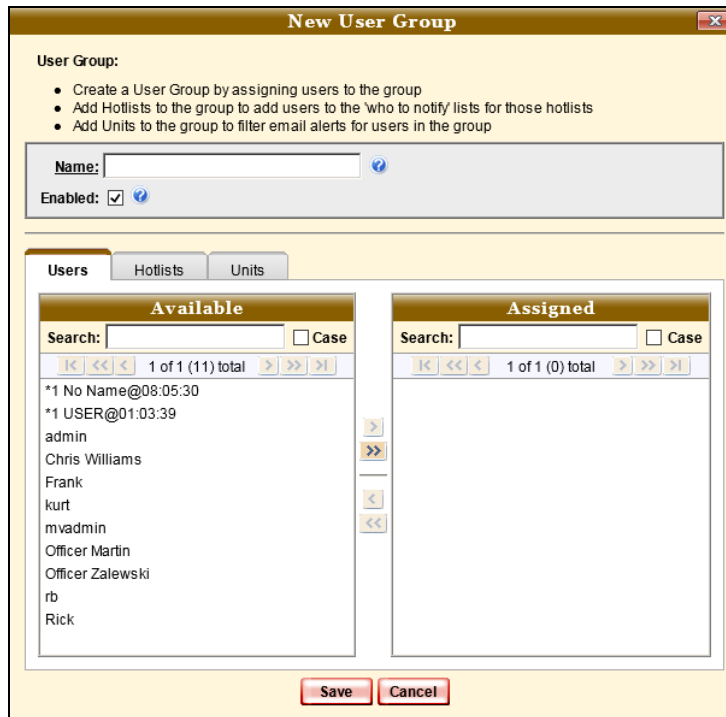
1 Go to ▼ Administration and click **Manage User Groups**. The User Group Search Results page displays.

This page lists your existing user groups, if applicable.

2 Go to the Action column and click **Create**. The New User Group form displays.

3 Enter a name for the new user group in the *Name* field.

4 Go to the left column (Available) and click on each of the users you wish to assign to this group. If a user you're looking for does not appear onscreen, use the *Search* field and/or navigation arrows at the top of the column to scroll through the user list.

5 Once you've highlighted the desired users, click the ▶ icon located between the two columns. The selected users display in the right column (Assigned).

(Continued)
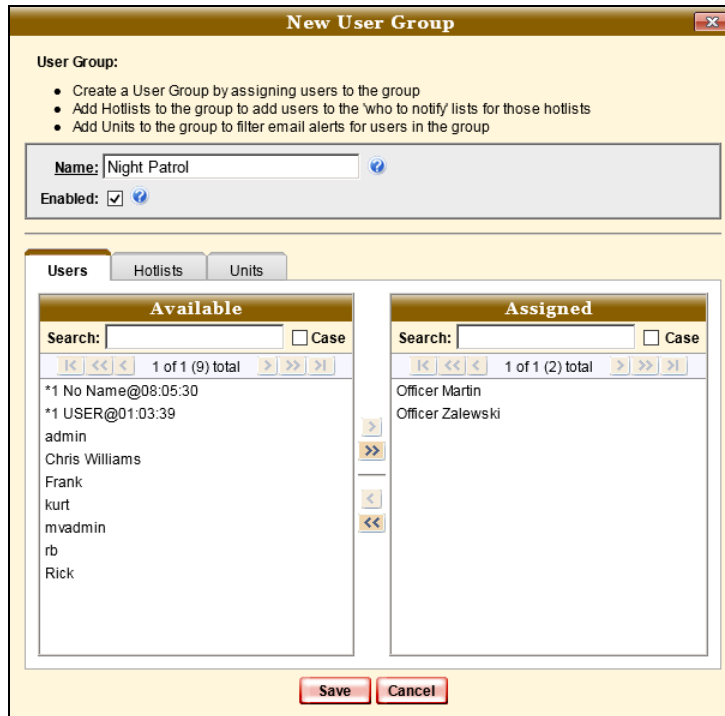
Next, you need to assign hotlists to the new user group.

6 Click the **Hotlists** tab. A list of all system hotlists displays in the left column (Available).

L3 Mobile-Vision, Inc.
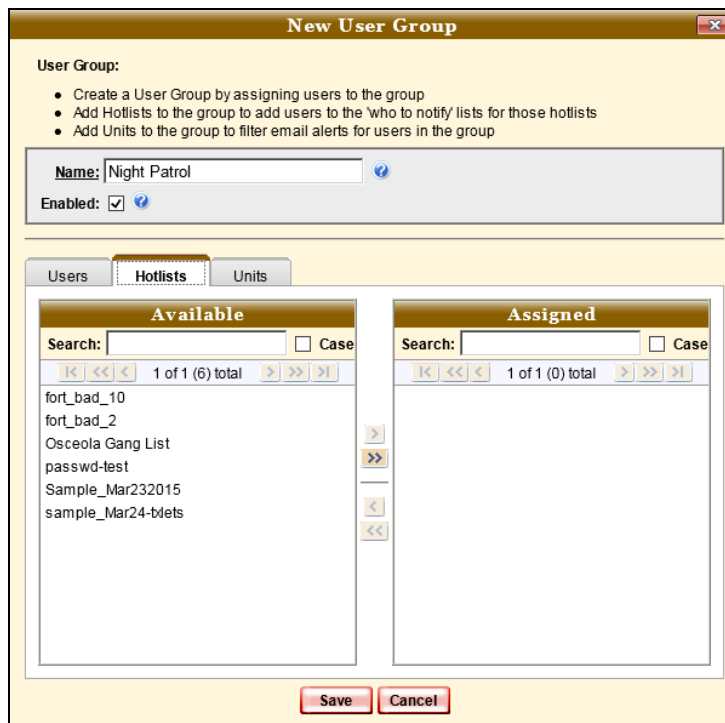
7 Go to the left column (Available) and click on each of the hotlists you wish to assign to this user group. If a hotlist you're looking for does not appear onscreen, use the *Search* field and/or navigation arrows at the top of the column to scroll through the list.

8 Once you've highlighted the desired hotlists, click the ▶ icon located between the two columns. The selected hotlists display in the right column (Assigned).

New User Group

User Group:
- Create a User Group by assigning users to the group
- Add Hotlists to the group to add users to the 'who to notify' lists for those hotlists
- Add Units to the group to filter email alerts for users in the group

Name: Night Patrol

Enabled: ☑

Users	**Hotlists**	Units

Available	**Assigned**
Search: ☐ Case	Search: ☐ Case
|< << < 1 of 1 (5) total > >> >|	|< << < 1 of 1 (1) total > >> >|
fort_bad_10	Osceola Gang List
fort_bad_2	
passwd-test	
Sample_Mar232015	
sample_Mar24-txlets	

Save   Cancel
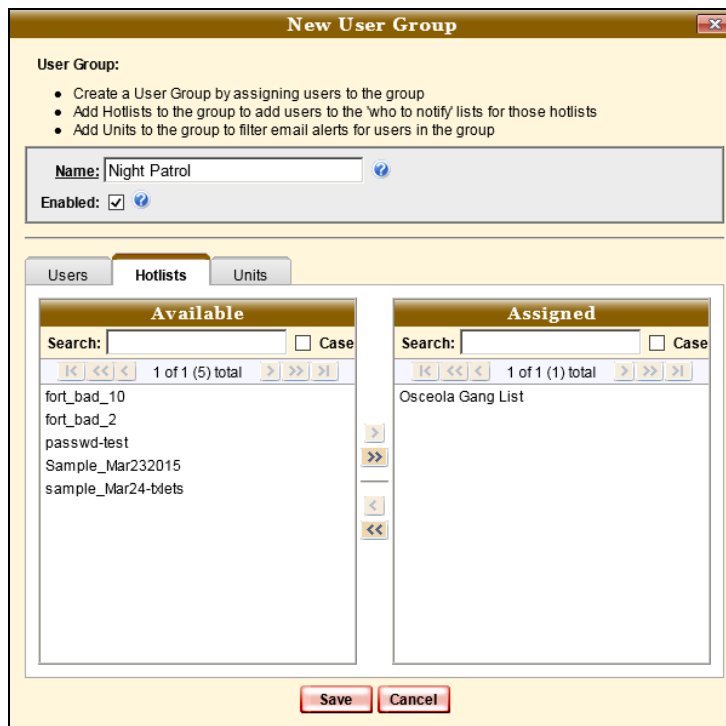
9 If you want this user group's assignees to receive hotlist hits on all units, skip to step 13.

– OR –

If you want this user group's assignees to receive hotlist hits on *some*, but not *all* units, proceed to the next step.

10 Click the **Units** tab. A list of all active AlertVU units displays in the left column (Available).

(Continued)
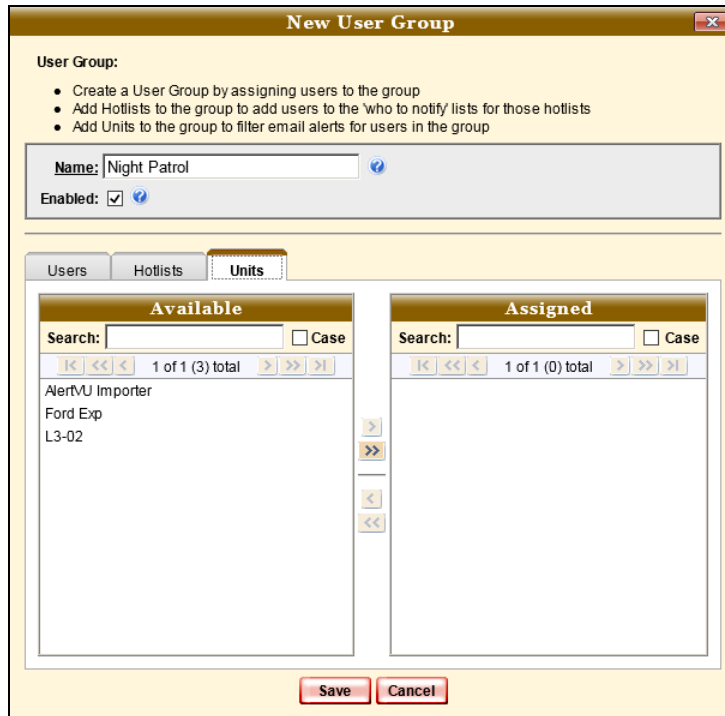
11 Go to the left column (Available) and click on each of the units you wish to assign to this user group. If a unit you're looking for does not appear onscreen, use the *Search* field and/or navigation arrows at the top of the column to scroll through the list.

12 Once you've highlighted the desired units, click the ![icon] icon located between the two columns. The selected units display in the right column (Assigned).
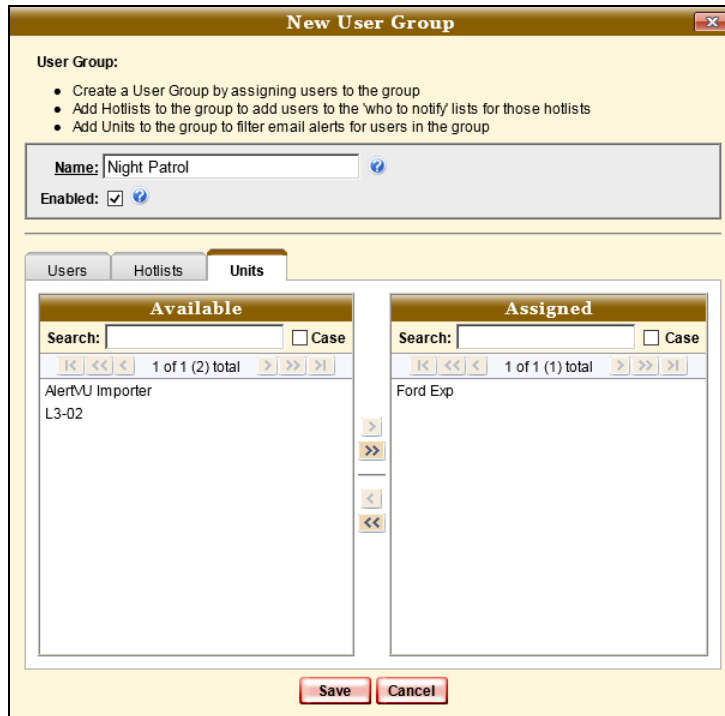
13 Click **Save**. A confirmation message displays.

> **User Group Night Patrol successfully saved.**

Changing a User Group

This section describes how to update an existing user group. For more on user groups and how they are used in AlertVU, see "Managing User Groups" on page 354.

Specifically, this section describes how to:

☐ Add a user to a user group
☐ Remove a user from a user group
☐ Add a hotlist to a user group
☐ Remove a hotlist from a user group

1 Go to ▼ Administration and click **Manage User Groups**. The User Group Search Results page displays.

(Continued)
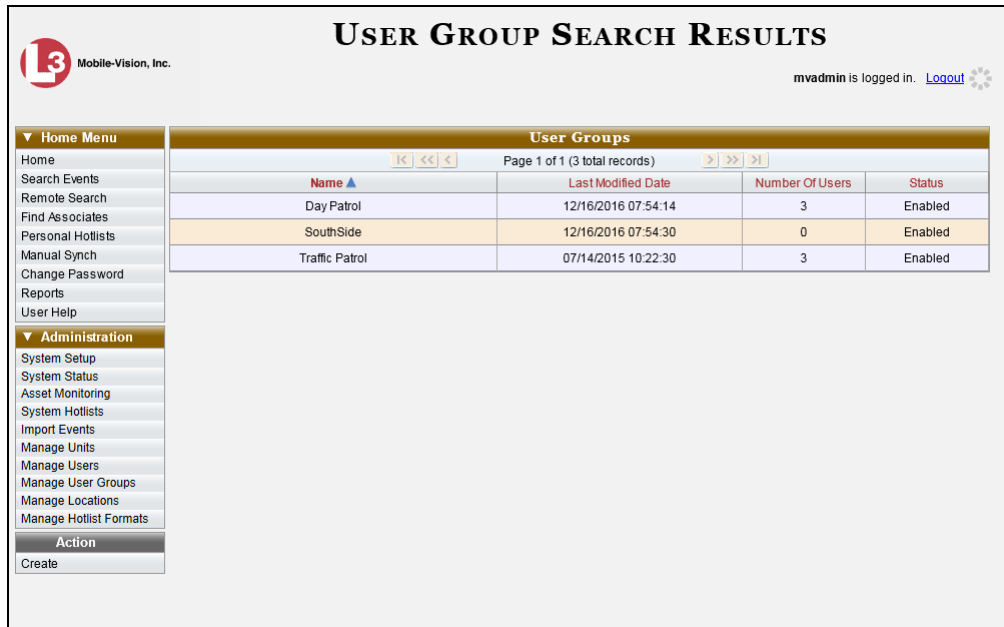
2 Click on the user group you wish to update.

3 Go to the Action column and click **Edit**.

– OR –

Right-click on the record, then select **Edit** from the popup menu. The Edit User Group popup displays.
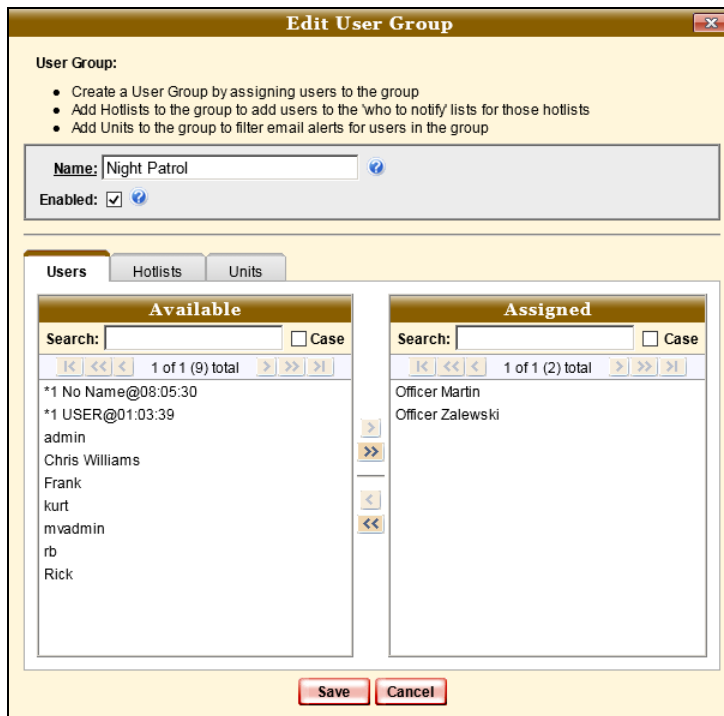
4 To add or remove users from this user group, proceed to the next step. Otherwise skip to step 11.

5 To *add* one or more users to this user group, proceed to the next step.

– OR –

To *remove* one or more users from this group, skip to step 9.

6 Go to the left column (Available) and click on each of the users you wish to add to this user group. If a user you're looking for does not appear onscreen, use the *Search* field and/or navigation arrows at the top of the column to scroll through the user list.

7 Once you've highlighted the desired users, click the ▶ icon located between the two columns. The selected users display in the right column (Assigned).

8 To *remove* one or more users from this group, proceed to the next step. Otherwise skip to step 11.

9 Go to the right column (Assigned) and click on each of the users you wish to remove from this user group. If a user you're looking for does not appear onscreen, use the *Search* field and/or navigation arrows at the top of the column to scroll through the user list.

10 Once you've highlighted the desired users, click the ◀ icon located between the two columns. The selected users are removed from the *Assigned* list.

11 To add or remove hotlists from this user group, proceed to the next step. Otherwise skip to step 19.

12 Click the **Hotlists** tab.

(Continued)
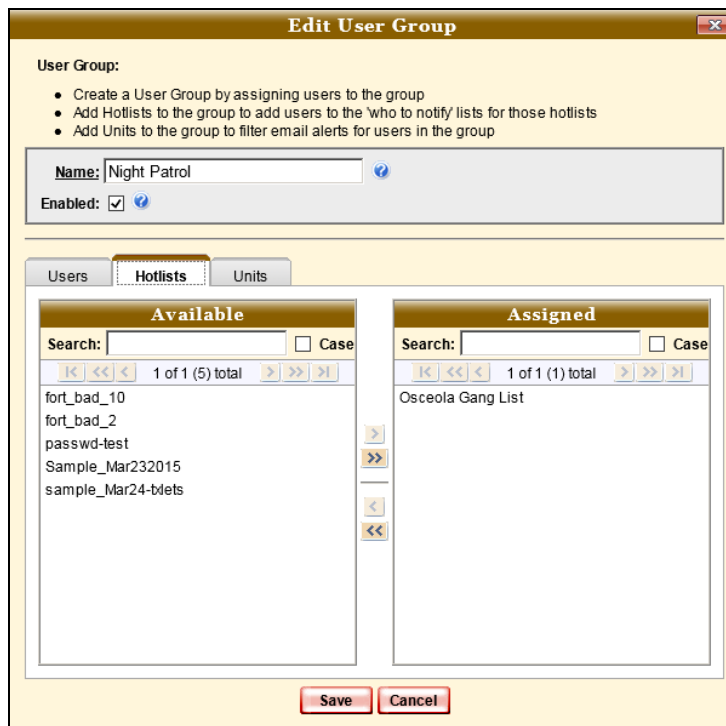
13 To *add* one or more hotlists to this user group, proceed to the next step.

– OR –

To *remove* one or more hotlists from this group, skip to step 17.

14 Go to the left column (Available) and click on each of the hotlists you wish to add to this user group. If a hotlist you're looking for does not appear onscreen, use the *Search* field and/or navigation arrows at the top of the column to scroll through the list.

15 Once you've highlighted the desired hotlist(s), click the ▶ icon located between the two columns. The selected hotlist(s) display in the right column (Assigned).

16 To *remove* one or more hotlists from this group, proceed to the next step. Otherwise skip to step 19.

17 Go to the right column (Assigned) and click on each of the hotlists you wish to remove from this user group. If the hotlist you're looking for does not appear onscreen, use the *Search* field and/or navigation arrows at the top of the column to scroll through the list.

18 Once you've highlighted the desired hotlist(s), click the ◀ icon located between the two columns. The selected hotlist(s) are removed from the *Assigned* list.

19 To add or remove units from this user group, proceed to the next step. Otherwise skip to step 27.

20 Click the **Units** tab.
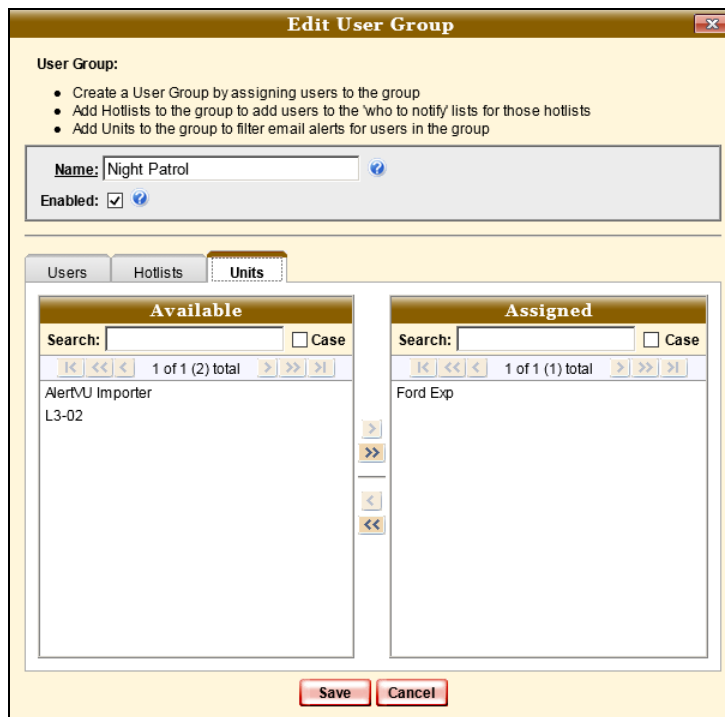
21 To *add* one or more units to this user group, proceed to the next step.

– OR –

To *remove* one or more units from this group, skip to step 25.

22 Go to the left column (Available) and click on each of the units you wish to add to this user group. If a unit you're looking for does not appear onscreen, use the *Search* field and/or navigation arrows at the top of the column to scroll through the list.

23 Once you've highlighted the desired unit(s), click the ▶ icon located between the two columns. The selected unit(s) display in the right column (Assigned).

24 To *remove* one or more units from this group, proceed to the next step. Otherwise skip to step 27.

25 Go to the right column (Assigned) and click on each of the units you wish to remove from this user group. If the unit you're looking for does not appear onscreen, use the *Search* field and/or navigation arrows at the top of the column to scroll through the list.

26 Once you've highlighted the desired unit(s), click the ◀ icon located between the two columns. The selected unit(s) are removed from the *Assigned* list.
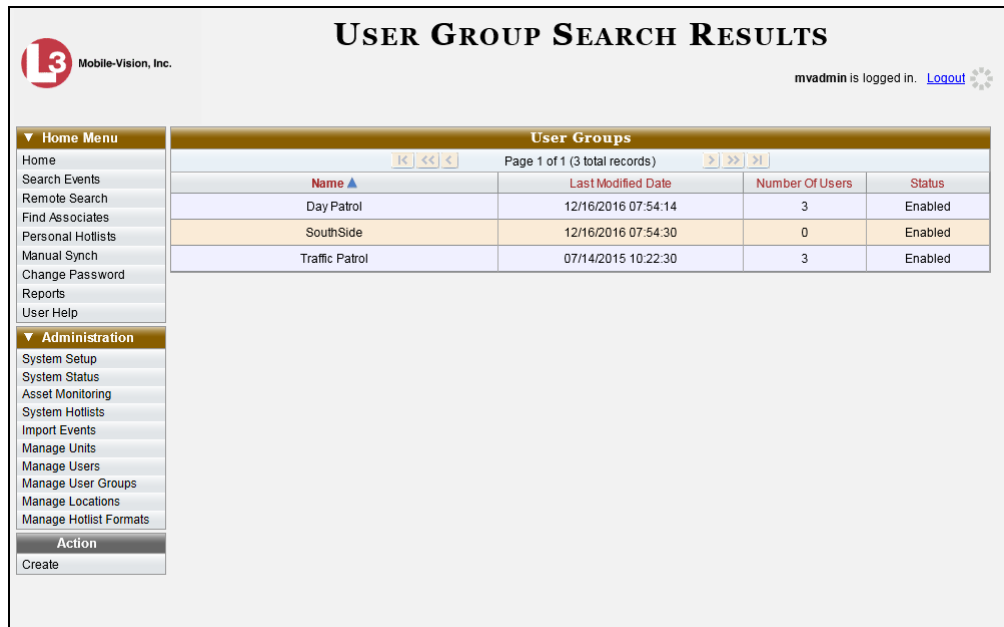
27 Click **Save**. A confirmation message displays.

> **User Group Night Patrol successfully saved.**

Deleting a User Group

This section describes how to delete an existing user group. For more on user groups and how they are used in AlertVU, see "Managing User Groups" on page 354.

1 Go to ▼ Administration and click **Manage User Groups**. The User Group Search Results page displays.

2 Click on the user group you wish to delete.

3 Go to the Action column and click **Delete**.

– OR –

Right-click on the record, then select **Delete** from the popup menu.

A confirmation message displays.

4 Click **Delete**. The selected user group is removed from the User Groups list.

L3 Mobile-Vision, Inc.

Using the Active Directory Integration Feature

If desired, you can link AlertVU to your agency's existing Windows Active Directory or Novell eDirectory. This feature, called *Active Directory Integration*, allows for a single password authentication with your agency's internal network, eliminating the need to maintain two sets of User IDs and passwords. This feature also allows you to import existing network users.

Your Systems Installation Specialist (SIS) will assist you in setting up your Active Directory for the first time. After that, you need only update the user list as needed.

For specific procedures used to integrate your Active Directory with AlertVU, see Appendix A.

For more information, see:

❐ Maintaining Users in Active Directory, below
❐ Updating the Active Directory Settings, page 371.

Maintaining Users in Active Directory

There are two methods for updating the Active Directory user list:

❐ *Method 1: Auto-Create Users Upon Login*. This method will automatically create a new user record in AlertVU whenever a new user logs into AlertVU Back Office for the first time. This method is fully automated. It is the "set it and forget it" option.
❐ *Method 2: Manually Add Users En Mass*. This method is used to manually update your user list on a periodic basis.

For specific instructions, see:

❐ Method 1: Auto-Creating Active Directory Users Upon Login, below
❐ Method 2: Manually Adding Active Directory Users En Mass, page 368.

Method 1: Auto-Creating Active Directory Users Upon Login

This section describes how to set up the system so that it automatically creates a new user record in AlertVU whenever a new user logs in for the first time. This procedure only applies to those customers who are using the Active Directory Integration feature.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

(Continued)

This document consists of general capabilities information that is not defined as controlled technical data under ITAR part 120.10 or EAR
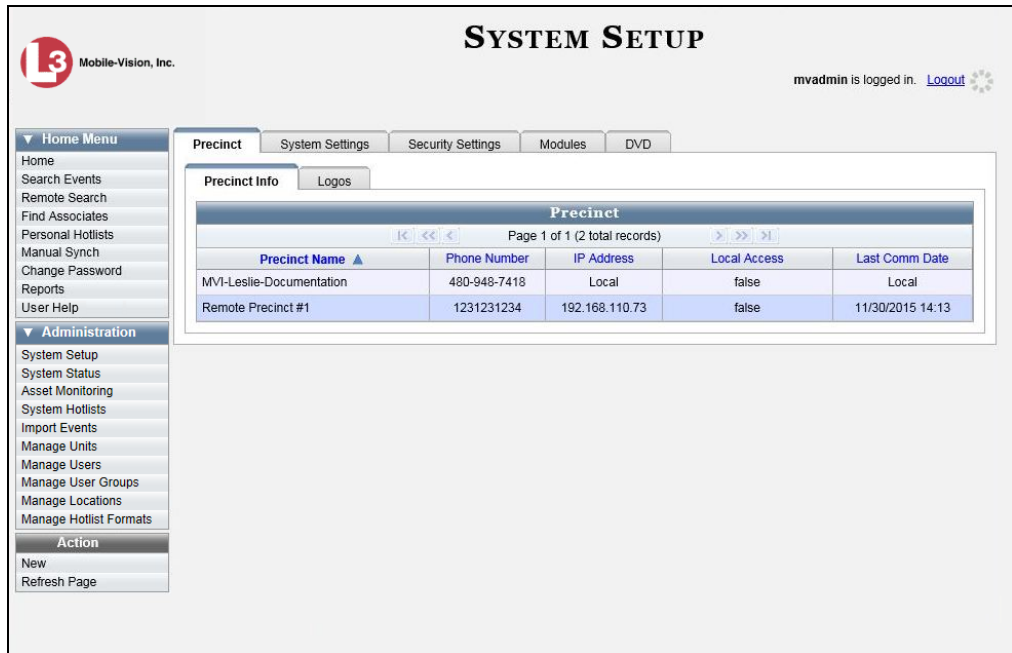
2 Click the **Security Settings** tab.
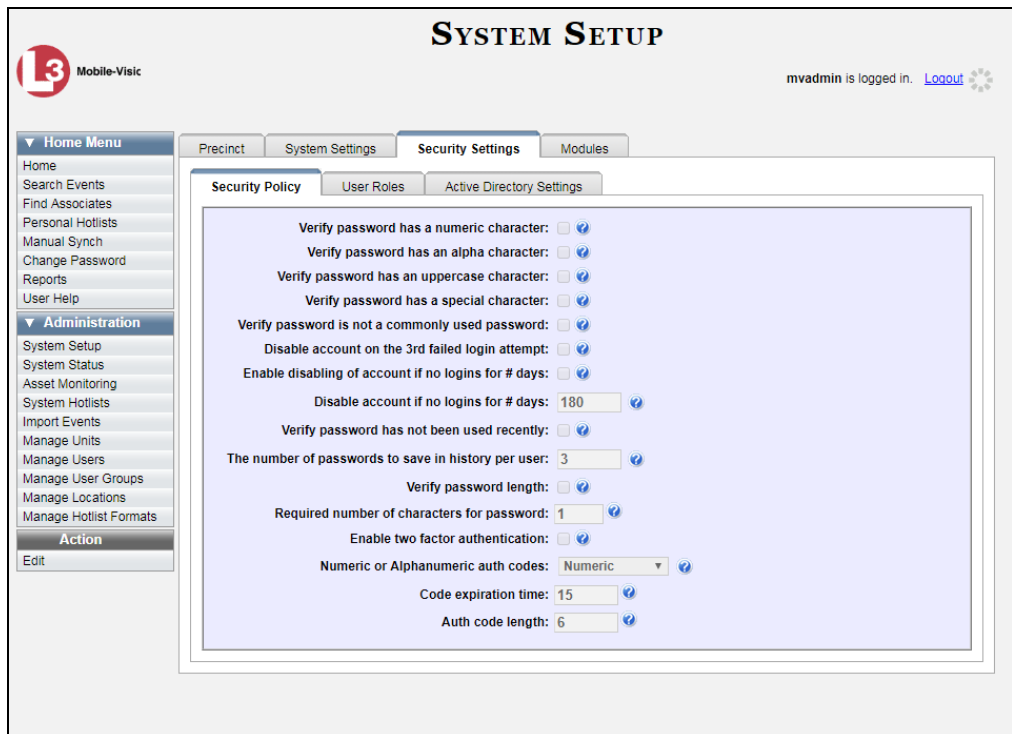
3 Click the **Active Directory Settings** tab. The Active Directory form displays.
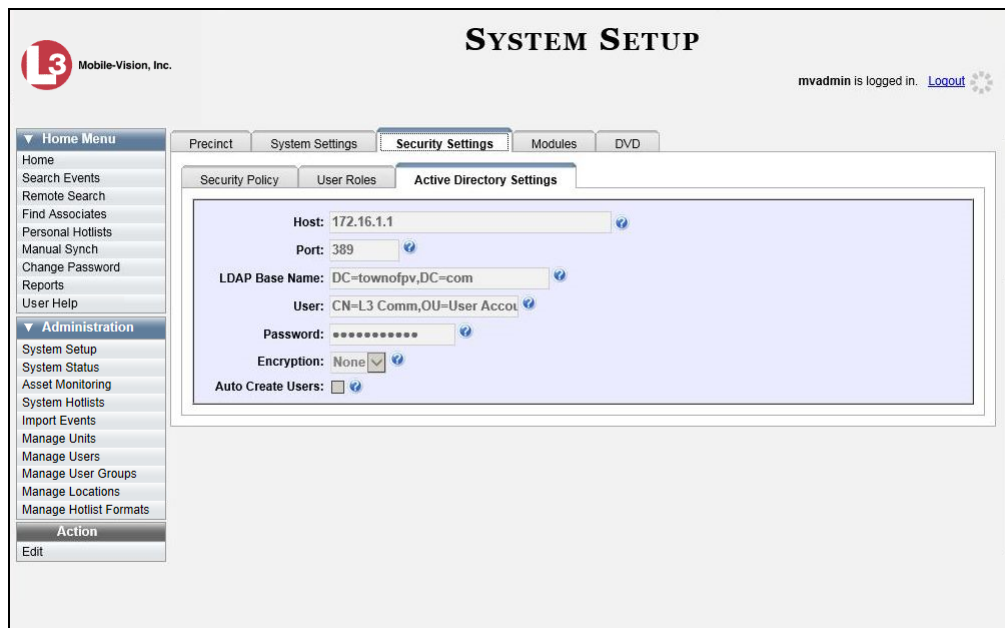
4 Go to the Action column and click **Edit**. The Edit LDAP Active Directory Settings popup displays.
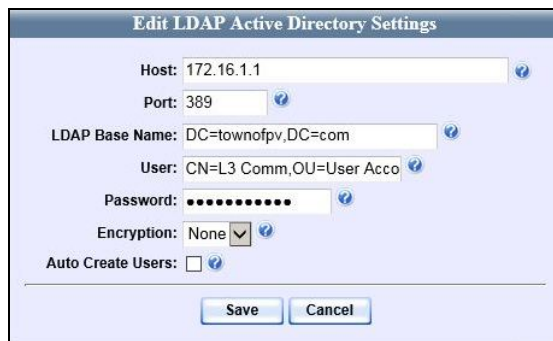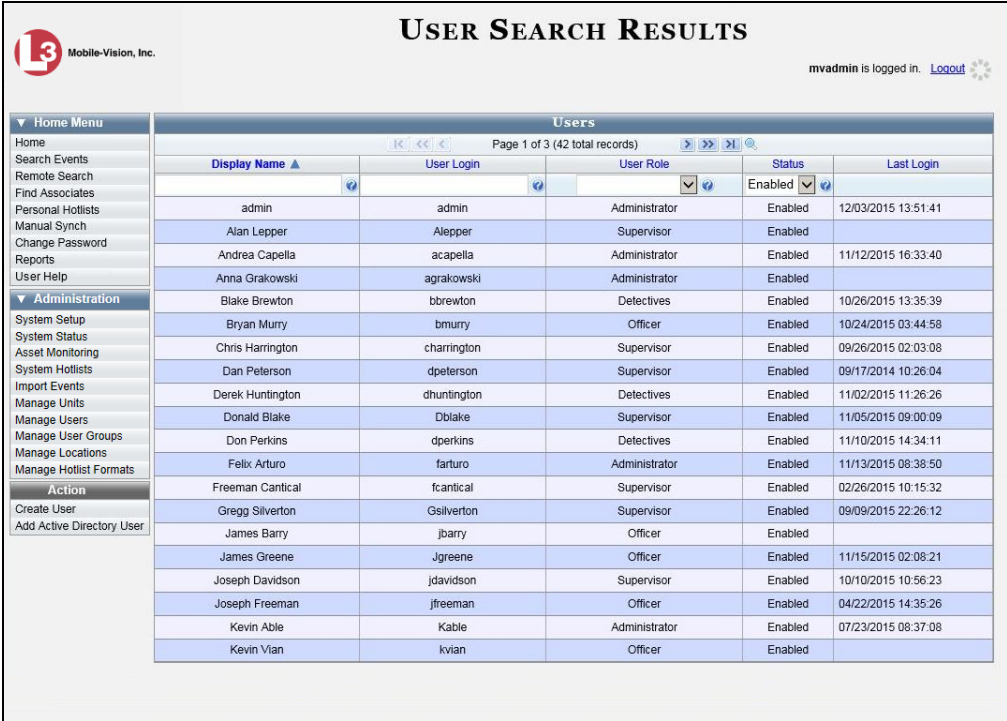
The fields on this popup are described in the table on page 373.

5 Select the *Auto Create Use*rs checkbox.

6 Click **Save**.

Method 2: Manually Adding Active Directory Users En Mass

This section describes how to manually update your user list on a periodic basis. This procedure only applies to those customers who are using the Active Directory Integration feature.

1 Go to ▼ Administration and click **Manage Users**. The User Search Results page displays.

2 Go to the Action column and click **Add Active Directory User**. The Active Directory Users page displays.

Use the Active Directory Users page to search for and select the active directory users that you wish to add to the system, as described below.

3 Go to the *Top Level OU* drop-down list and select the organization unit in which you wish to search for users.

4 Go to the *Search by* drop-down list and select the field name wish to search by.
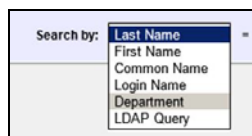
5 Go to the blank field to the right of *Search by* field and enter the field value you wish to search by. This value should correspond to the selected *Search by* value. For example, if you entered **Department** in the *Search by* field, you might enter **Information Services** in the search field.

6 Go to the Action column and click **Search**.

The system displays all user records that match your selection criteria.

(Continued)
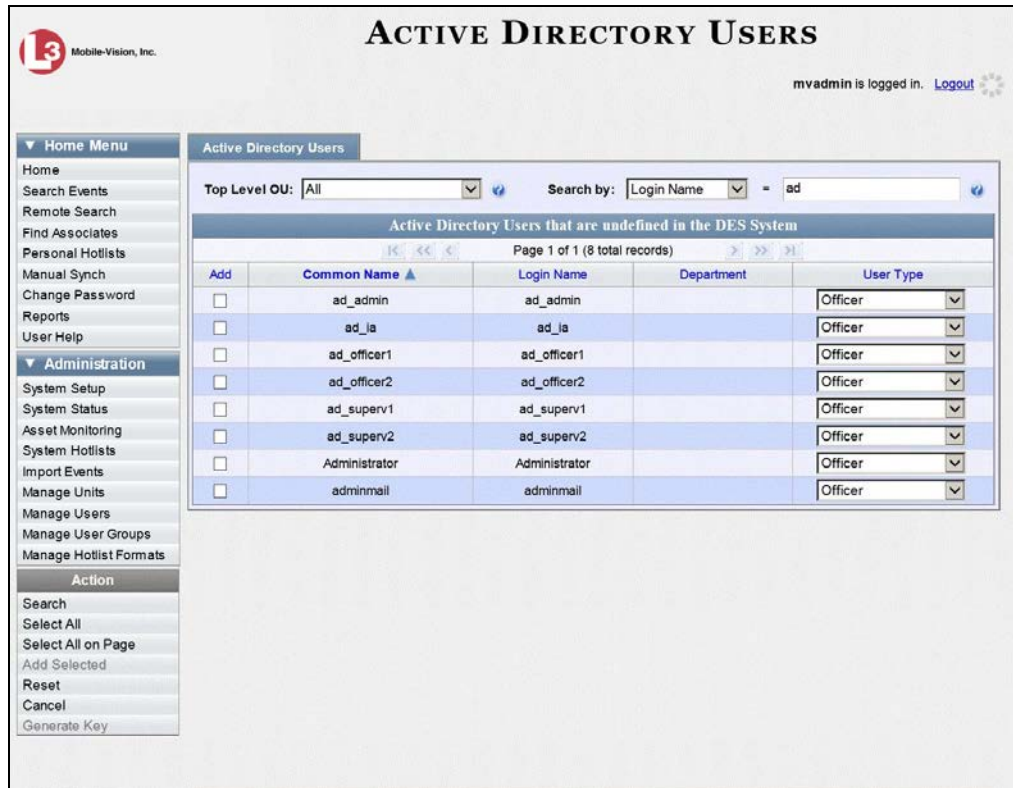
7 Select all of the users you wish to add:

Go to the Action column and click **Select All**.

– OR –

Go to the Action column and click **Select All on Page**.

– OR –

Go to the *Add* column and manually select the appropriate checkboxes. If necessary, use the navigation arrows at the top of the page to scroll through the full user list.

8 Go to the *User Type* column and select a role for each user from the drop-down list provided.

9 Once the correct users are selected, go to the Action column and click **Add Selected**. A confirmation message displays.

> **9 user(s) successfully saved.**

The selected users are added to your AlertVU users list.

Updating the Active Directory Settings

This section describes how to update your Active Directory settings.

1 Go to ▼ Administration and click **System Setup**. The System Setup page displays.

2 Click the **Security Settings** tab.

3 Click the **Active Directory Settings** tab. The Active Directory form displays.

4 Go to the Action column and click **Edit**. The Edit LDAP Active Directory Settings popup displays.

The fields on this popup are described in the following table.

L3 Mobile-Vision, Inc.

Edit LDAP Active Directory Settings	
Field	**Description**
Host	The address of the host active directory server.
Port	The port to use when connecting to the Active Directory server. Default values are: ▪ No encryption – 389 ▪ SSL encryption – 636
LDAP Base Name	The LDAP string which represents the base distinguished name of the Active Directory server. This is usually a full distinguished name path, such as: DC=MVI,DC=MyCompany,DC=com
User	The name of the user to connect to the Active Directory server. If you use our setup instructions to create the user (recommended), you may use the user's name, such as "Mark Jones." Otherwise you **MUST** use a full distinguished name, such as: CN=JasonSkipper,OU=Florida,DC=MVI,DC=MyCompany,DC=com
Password	The security password that matches the *User* name above.
Encryption	The type of encryption used on the Active Directory server: **None** or **SSL**. *Select this value from the drop-down list provided.*
Auto Create Users	A checkbox used to indicate whether or not the system will automatically create users. If this box is selected, the system will automatically create users at login time if the user's credentials authenticate against the Active Directory server.

5 Enter or select your changes in the appropriate field(s).
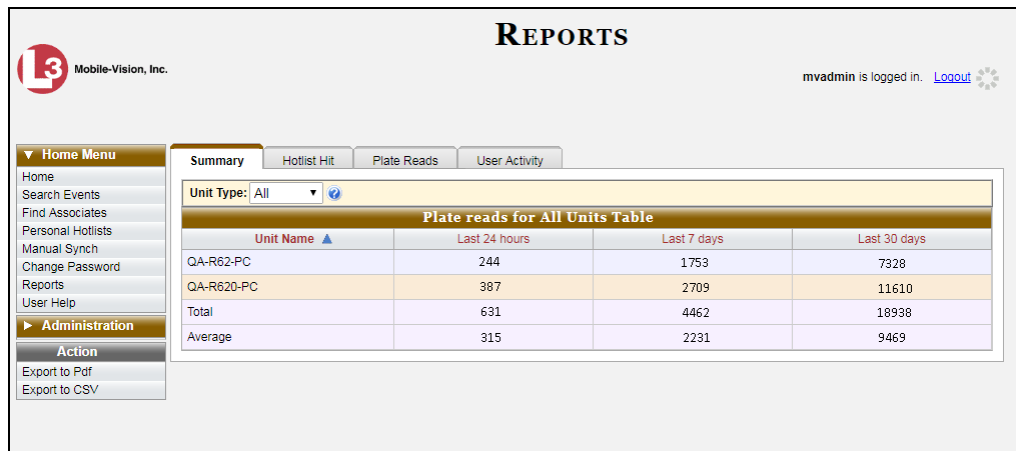
6 Click **Save**.

Generating the User Activity Report

This section describes how to export all your user activity to a spreadsheet or PDF file. This is referred to as the *User Activity* report. It includes information such as which user records have been added, changed, and/or deleted, and by whom. The system automatically updates this report once every day.

The User Activity report includes all user activity from the time your agency upgraded to AlertVU Back Office version 3.12 to the present.
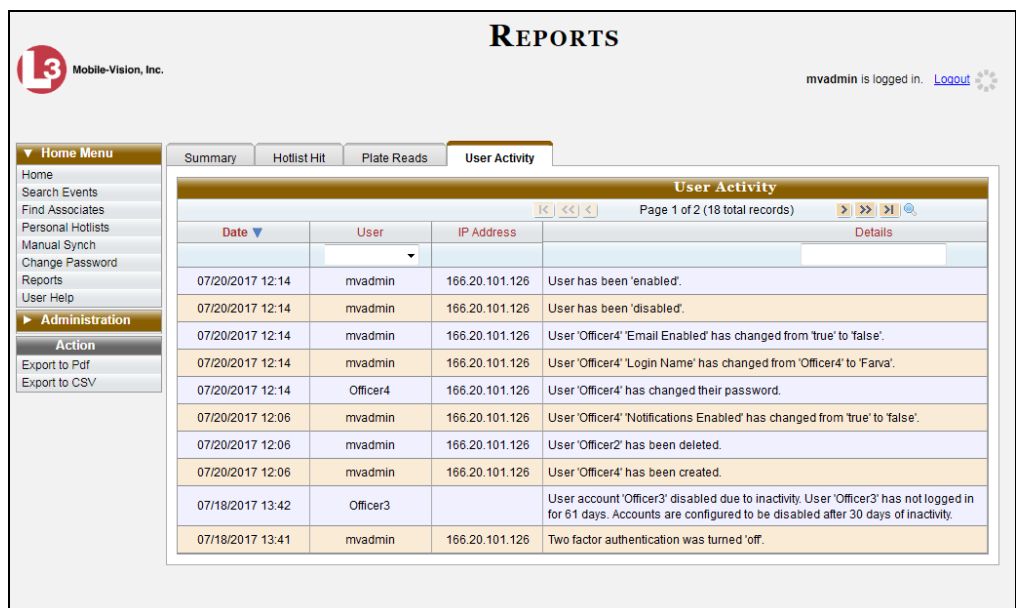
1 Go to ▼ Home Menu and click **Reports**. The Reports page displays.

2 Click the **User Activity** tab.

3 To report on *all* users (default), proceed to the next step.

– OR –

To report on only *one* user, select that user from the *User* drop-down list.

4 To narrow your report criteria to those activities that contain a particular word or phrase (for example—*password*, *created*, *deleted*, *changed*, *supervisor*, *administrator*, *officer*, *two factor authentication*, etc.), enter that word or phrase in the *Details* box. Otherwise proceed to the next step.

5 To export this report to a *pdf* file, go to the Action column and click **Export to pdf**.

– OR –

To export this report to a *csv* spreadsheet file, go to the Action column and click **Export to CSV**.

A Windows download message displays. The appearance of this message may vary slightly depending on the version of Windows that you have.

PDF Download Messages

Do you want to open or save **report-1448999380696.pdf** from **166.20.101.93**?   Open   Save ▼ Cancel ×

report-150153386....pdf ^

CSV Download Messages

Do you want to open or save **report-1448999409287.csv** (205 bytes) from **166.20.101.93**?   Open   Save ▼ Cancel ×

report-150153411....csv ^
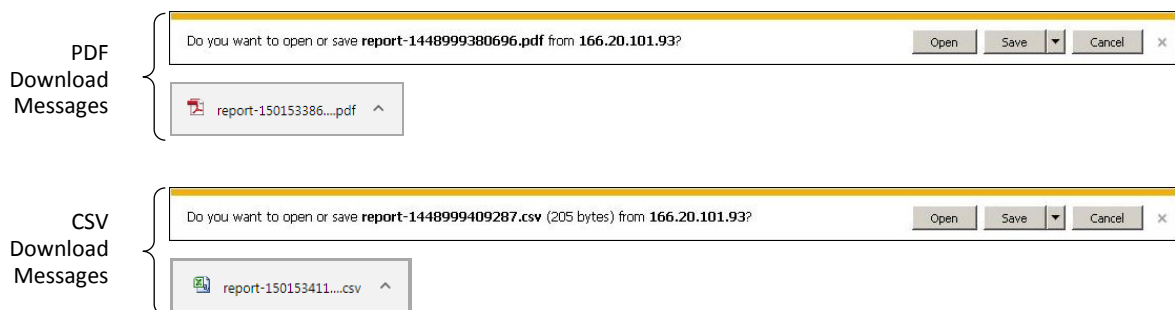
6 Click **Open**.

– OR –

Double-click on the download tab.

(Continued)

⇒ If you selected the **Export to pdf** option, the report displays in Adobe Reader.

PDF file in Acrobat

User Activity

Date	User	IP Address	Details
07/20/2017 12:14	mvadmin	166.20.101.126	User has been 'enabled'.
07/20/2017 12:14	mvadmin	166.20.101.126	User has been 'disabled'.
07/20/2017 12:14	mvadmin	166.20.101.126	User 'Officer4' 'Email Enabled' has changed from 'true' to 'false'.
07/20/2017 12:14	mvadmin	166.20.101.126	User 'Officer4' 'Login Name' has changed from 'Officer4' to 'Farva'.
07/20/2017 12:14	Officer4	166.20.101.126	User 'Officer4' has changed their password.
07/20/2017 12:06	mvadmin	166.20.101.126	User 'Officer4' 'Notifications Enabled' has changed from 'true' to 'false'.
07/20/2017 12:06	mvadmin	166.20.101.126	User 'Officer2' has been deleted.
07/20/2017 12:06	mvadmin	166.20.101.126	User 'Officer4' has been created.
07/18/2017 13:42	Officer3		User account 'Officer3' disabled due to inactivity. User 'Officer3' has not logged in for 61 days. Accounts are configured to be disabled after 30 days of inactivity.
07/18/2017 13:41	mvadmin	166.20.101.126	Two factor authentication was turned 'off'.
07/18/2017 13:37	Officer3		User account 'Officer3' has has its password expired. User 'Officer3' has not changed their password in for 35 days. Passwords are configured to expire after 30 days.
07/18/2017 12:47			User account 'Officer3' disabled due to inactivity. User 'Officer3' has not logged in for 35 days. Accounts are configured to be disabled after 30 days of inactivity.

⇒ If you selected the **Export to CSV** option, the report displays in Microsoft Excel.

CSV file in Excel

Date	User	IP Address	Details
7/20/2017 12:14	mvadmin	166.20.101.126	User has been 'enabled'.
7/20/2017 12:14	mvadmin	166.20.101.126	User has been 'disabled'.
7/20/2017 12:14	mvadmin	166.20.101.126	User 'Officer4' 'Email Enabled' has changed from 'true' to 'false'.
7/20/2017 12:14	mvadmin	166.20.101.126	User 'Officer4' 'Login Name' has changed from 'Officer4' to 'Farva'.
7/20/2017 12:14	Officer4	166.20.101.126	User 'Officer4' has changed their password.
7/20/2017 12:06	mvadmin	166.20.101.126	User 'Officer4' 'Notifications Enabled' has changed from 'true' to 'false'.
7/20/2017 12:06	mvadmin	166.20.101.126	User 'Officer2' has been deleted.
7/20/2017 12:06	mvadmin	166.20.101.126	User 'Officer4' has been created.
7/18/2017 13:42	Officer3	null	User account 'Officer3' disabled due to inactivity. User 'Officer3' has not logged in for 61 days. Accounts are configured to be disabled after 30 days of inactivity.
7/18/2017 13:41	mvadmin	166.20.101.126	Two factor authentication was turned 'off'.
7/18/2017 13:37	Officer3	null	User account 'Officer3' has has its password expired. User 'Officer3' has not changed their password in for 35 days. Passwords are configured to expire after 30 days.
7/18/2017 12:47	0	null	User account 'Officer3' disabled due to inactivity. User 'Officer3' has not logged in for 35 days. Accounts are configured to be disabled after 30 days of inactivity.
7/18/2017 12:46	0	null	User account 'Officer3' disabled due to inactivity. User 'Officer3' has not logged in for 35 days. Accounts are configured to be disabled after 30 days of inactivity.
7/14/2017 12:41	0	null	User account 'Officer3' disabled due to inactivity. User 'Officer3' has not logged in for 31 days. Accounts are configured to be disabled after 30 days of inactivity.
7/14/2017 12:38	0	null	User account 'Officer3' disabled due to inactivity. User 'Officer3' has not logged in for 31 days. Accounts are configured to be disabled after 30 days of inactivity.
7/14/2017 11:06	0	null	User account 'Officer3' disabled due to inactivity. User 'Officer3' has not logged in for 30 days. Accounts are configured to be disabled after 30 days of inactivity.
7/14/2017 11:05	0	null	User account 'Officer3' disabled due to inactivity. User 'Officer3' has not logged in for 30 days. Accounts are configured to be disabled after 30 days of inactivity.
7/14/2017 10:55	0	null	Two factor authentication was turned 'off'.

7 When you're finished viewing/printing the report, click the ☒ in the upper right corner of the report to exit Acrobat or Excel.

G Glossary

Alert

A notification that the system sends you any time an AlertVU <u>unit</u> receives a possible hit on a license plate that's on either one of your <u>personal hotlists</u> or a <u>system hotlist</u> for which you have notification rights.

Associate

An <u>event</u> that was captured in the same region and within the same time frame as another event. The Associates search function allows you to link a suspect with other possible suspects or associates who happened to be in the same region at the same time as your suspect.

Backup PC

A computer used to process DVD burn requests. AlertVU comes with an optional backup facility that automatically sends backup burn requests to a <u>robotic DVD burner</u>. The resulting archive discs, termed <u>Certified Backup Discs</u>, contain system <u>events</u> and <u>hotlists</u>. Because the process of burning DVDs is resource-intensive, one PC is dedicated to this task. If you are using a Bravo robotic DVD burner, then the backup PC is a separate computer workstation connected to the disc burner. If you are using a Rimage DVD/Blu-Ray burner that combines a disc burner with a computer, the Backup PC refers to the computer component of the Rimage.

Certified Backup Disc (CBD)

An archive disc. When the archive function is enabled, the system automatically sends CBD burn requests to the <u>Backup PC</u> without any action on your part. These discs contain the <u>event</u> records and <u>hotlists</u> that were previously stored on the <u>server</u>.

Custom Hotlist Format

The predefined and user-defined formats that can be changed. The predefined formats include: Florida Crime Information Center (FCIC), Arkansas National Law Enforcement Telecommunication System (AR NLETS), Maryland Motor Vehicle Administration (MD MVA), Texas Law Enforcement Telecommunication System (TXLETS), and California Law Enforcement Web Stolen Vehicle Systems (CLEW SVS).

Delimited Hotlist Format

A type of file format that separates each piece of data with a comma, semicolon, or space.

Derivative Hotlist

A [hotlist](#) that is a subset of another, larger, hotlist.

Event

The file that's created when an AlertVU [unit](#) captures the digital image of a license plate. Because the same license plate can be read multiple times, some license plate numbers have more than one event record associated with them.

Event Exporter

A system feature that enables you to automatically copy your incoming [event](#) data into zip files or "packages" and place them in the Packages folder of the Event Exporter's Home Directory. This makes it possible for you to import your event data into third-party applications, such as another license plate reader system.

Fixed Field Hotlist Format

A type of file format where each data element is in a column of a specific length, such as eight characters wide.

Fuzzy Search

A search that looks for characters that are similar looking to other characters. This type of search addresses the problem of misreads from the capture device. For example, to the AlertVU capture device, a 3 might look like an 8, a 4 might look like an A, a C might look like an O, etc. If, for instance, there's an [event](#) in the system with a plate of R342KCY, then fuzzy search results would include not only the exact match to that plate but R842KCY, R8A2KCY, R8A7KCY, R8A7KOY, etc.

GeoHotlist

A type of Hotlist that is defined in part by a predefined geographic region. GeoHotlists only issue Alerts on hits that occur within their assigned [Location](#) or [Location Group](#).

Hotlist

A list of wanted license plates, such as BOLOs, Amber Alerts, persons of interest, etc.

Hotlist Format

A record that stores the information that AlertVU needs to parse, or divide and analyze, the data that's contained in each hotlist type. For example, if the XYZ hotlist consists of five columns and the second column contains the license plate number, the system needs to know that.

Location

A predefined geographic region that you can apply to a personal hotlist or system hotlist. When you assign a Location to a hotlist, it narrows that hotlist's criteria to plates that are scanned within the Location's geographic region.

Location Group

A record that combines multiple Locations into one group, making it easier to apply multiple locations to a hotlist at the same time.

MDC

Mobile Data Computer

Mobile Unit

An AlertVU license plate reader that is installed in a vehicle, such as a patrol car. The AlertVU connects to a Mobile Data Computer, which controls and transmits plate reads to the server via the AlertVU PC applications. Each AlertVU mobile unit has a corresponding record entered in AlertVU Back Office. These records store all the information required for successful communication between your AlertVU mobile units and the server. They are created automatically by the system whenever it discovers a new (i.e., unknown) device on the network.

Notifications List

A list of users who will receive an Inbox, email, or real-time "popup" alert whenever an AlertVU unit captures a plate that's on a system hotlist.

Personal Hotlist

A list of license plates that only you have access to. If desired, you can have the system notify you whenever an AlertVU unit captures a license plate that is on one of your personal hotlists.

Quick Alert

A one plate "Amber Alert" style hotlist that you can transmit to all your AlertVU units.

RAID

Redundant Array of Independent Disks—a storage device that contains multiple disk drive components.

Robotic DVD Burner

A disc duplicator that burns and labels your Certified Backup Discs. L3 Mobile-Vision sells two types of burners: the Bravo, a stand-alone unit, and the Rimage, a combination disc burner/computer. If you have a Rimage, you do not need a separate Backup PC. Rimage units can burn CDs, DVDs, and Blu-Ray discs. Most Bravo

units can burn CDs and DVDs. The higher-end Bravos can burn Blu-Ray discs as well.

Server

The network computer that hosts the AlertVU Back Office application and stores all of your event and hotlist data.

Session Timeout Setting

The number of idle-time minutes that must pass before the system automatically logs a user off the system.

System Hotlist

A list of license plates that you can share with other users and transmit to all your AlertVU units. If desired, you can have the system notify selected users whenever an AlertVU unit captures a license plate that's on a system hotlist.

System-defined Hotlist Format

The predefined formats that cannot be changed. These include CSV (Comma separated text file) and NCIC (National Crime Information Center).

Unit

The license plate reader that's installed either in a vehicle, such as a patrol car (mobile unit), or on a stationary device, such as a pole (fixed unit). The AlertVU cameras capture digital license plate images and transfer those files to a storage server over a wireless network.

User Group

A container that allows you to combine like users for the purpose of assigning hotlists to them.

User Role

A group of permissions that you can assign to one or more users.

A   Appendix: End-User License Agreement

IMPORTANT-READ CAREFULLY: This License AGREEMENT (the "AGREE-MENT") is a legal AGREEMENT between you (either an individual or single entity, including, but not limited to a Corporation, LLC, LLP, Partnership, Sole Proprietorship) ("LICENSEE") and L3 Mobile-Vision, Inc. ("LICENSOR").

By accepting delivery of the L3 Mobile-Vision software you are agreeing to become bound by the terms of this agreement, which includes the software license, maintenance terms and software disclaimer of warranty. If licensee does not agree to these terms and conditions, do not accept delivery, copy, or use the software. This limited warranty does not cover any other system components sold or installed by L3 Mobile-Vision, Inc. Please refer to applicable warranty documents for coverage details on related L3 Mobile-Vision products.

Software License

The SOFTWARE is protected by copyright laws and international copyright treaties, as well as other intellectual property and trade-secret laws and treaties. **The SOFTWARE is being licensed, not sold**.

GRANT OF LICENSE. This License AGREEMENT grants Licensee the following non-exclusive rights:

1. In consideration of payment of the LICENSE fee, LICENSOR grants to you, the LICENSEE, a non-exclusive right to use and display this copy of the software program in object code form only (hereinafter called the SOFTWARE) as per the usage limitations specified by the invoice at a single location. LICENSOR reserves all rights not expressly granted to LICENSEE.
2. As the LICENSEE, you own the magnetic or other physical media, on which the SOFTWARE is originally or subsequently recorded or fixed, but LICENSOR retains title and ownership of the SOFTWARE recorded on the original disk copy or copies, and all subsequent copies of the SOFTWARE, regardless of the form or media in or on which the original or other copies may exist. THIS LICENSE IS NOT A SALE OF THE ORIGINAL SOFTWARE OR ANY COPY OR COPIES OF IT.
3. Certain SOFTWARE licensed by LICENSOR to LICENSEE requires that LICENSEE must purchase one named user of SOFTWARE for each Digital Video Recorder, per physical location. Where named users are not utilized, the total number of licensed Digital Video Recorders cannot exceed the total number of licensed users of SOFTWARE per physical location. Non-compliance of this license restriction is strictly forbidden and shall be considered a material breach of this AGREEMENT and among all other remedies available to LICENSOR, including but not limited to immediate payment to LICENSOR for all license fees due and owing to LICENSOR, shall cause this AGREEMENT to immediately

terminate in accordance with the TERMINATION provisions stated in this AGREEMENT.

4. This SOFTWARE and the accompanying written materials are copyrighted. Unauthorized copying of the SOFTWARE, including SOFTWARE that has been modified, merged, or included with other software, or of the written materials, is expressly forbidden. You may be held legally responsible for any copyright infringement that is caused or encouraged by your failure to abide by the terms of this license. Subject to these restrictions, and if the SOFTWARE is not copy-protected, you may make one (1) copy of the SOFTWARE, solely for backup purposes. You must reproduce and include the copyright notice on the backup copy. The SOFTWARE is licensed as a single product. Its component parts may not be separated for use on more than one computer.

5. As the LICENSEE, you may not physically transfer the SOFTWARE from one computer to another. The SOFTWARE is licensed for one computer only. You may not electronically transfer the SOFTWARE from one computer to another over an internal or external network of any kind. You may not distribute copies of the SOFTWARE or accompanying written materials to others or modify, adapt, translate, reverse engineer, decompile, disassemble or create derivative works based on the written materials accompanying the SOFTWARE without the prior written consent of LICENSOR.

6. LICENSEE may not use the SOFTWARE for the benefit of a third party, not rent, timeshare or use the SOFTWARE in service bureau processing. LICENSEE may not transfer, export, install or use the SOFTWARE without the prior written permission of LICENSOR.

7. Without prejudice to any other rights, LICENSOR may terminate this License AGREEMENT if LICENSEE fails to comply with the terms and conditions of this License AGREEMENT. In such event, LICENSEE must destroy all copies of the SOFTWARE and all of its component parts.

8. LICENSOR may create, from time to time, updated versions of the SOFTWARE. At its option LICENSOR will make such updates available to LICENSEE only if LICENSEE is covered under Annual Maintenance by paying the Annual Maintenance fee. Maintenance is mandatory for the first year and will be automatically invoiced to LICENSEE on an annual basis from the anniversary date of LICENSOR'S first maintenance invoice to LICENSEE. LICENSEE agrees to pay this fee, within the terms stated on the invoice, unless LICENSEE notifies LICENSOR in writing of its intention not to renew at least ninety (90) days in advance of being invoiced, or the anniversary date of the AGREEMENT, or purchase SOFTWARE. Should LICENSEE choose not to renew maintenance in any given year LICENSOR may terminate this License AGREEMENT pursuant to the provisions stated in this License Agreement. See the LICENSOR'S Maintenance Agreement for further details on Annual Maintenance. Should LICENSEE choose not to renew maintenance any given year, and then wishes to renew at a later date, and LICENSOR has elected not to terminate the License Agreement, LICENSEE shall be charged for all back maintenance, which was not renewed, plus the maintenance fee at current rate. In addition, 20% of the total sum of back maintenance and current maintenance fee may be added as a surcharge for an interruption in maintenance. A copy of the terms of the Annual Software Maintenance Agreement is included in this package.

Termination

1. Following termination of this Agreement for any reason, the LICENSEE shall pay LICENSOR all amounts due to LICENSOR within 15 days. Any amounts due LICENSOR which are not paid within this period shall accrue the highest applicable rates allowed by law up to 2% per month. LICENSEE SHALL BE SOLELY RESPONSIBLE TO REIMBURSE TO LICENSOR ALL FEES, INCLUDING, BUT NOT LIMITED TO, COLLECTION AGENCY, LICENSOR TIME AND EXPENSE, AND REASONABLE ATTORNEY FEES AND EXPENSES INCURRED BY LICENSOR IN THE COLLECTION OF ANY AMOUNTS NOT PAID TO LICENSOR UNDER THIS AGREEMENT.
2. LICENSEE shall immediately discontinue all use of the SOFTWARE and shall remove SOFTWARE and any derivative works and/or computer code from LICENSEE's computer systems. All copies of SOFTWARE must be destroyed, or returned to LICENSOR immediately at LICENSEE's sole expense.
3. All of LICENSOR'S Proprietary Rights and the LICENSEE'S obligations regarding these Rights as detailed in this AGREEMENT shall survive the termination of this AGREEMENT.

Limited Warranty and Limitation of Liability

1. **Limited Warranty**. LICENSOR warrants that the SOFTWARE, when used in accordance with the procedures specified in the appropriate documentation (the "Documentation"), shall perform as specified therein.
2. **Limited Warranty Term**. This limited warranty as described in this Paragraph, shall be valid for any period during which LICENSEE has purchased and is a currently covered under maintenance services from LICENSOR for the SOFTWARE pursuant to terms and restrictions stated in LICENSOR'S maintenance agreement. This warranty shall apply only to the then-current release of the SOFTWARE for use on computer systems then recommended by LICENSOR. This limited warranty covers only the SOFTWARE installed by L3 Mobile-Vision. This warranty does not cover defects or errors pertaining to customer supplied hardware up to and including operating systems and network configurations. This limited warranty does not cover any other components sold or installed by L3 Mobile-Vision.
3. **Modifications Not Warranted**. The limited warranty described in this Paragraph shall be limited in such a way that LICENSOR shall not be liable for any malfunction or error resulting from a modification made by any person or organization other than LICENSOR with or without the prior written explicit approval of LICENSOR. Should LICENSEE employ and/or contract with any person and/or any business entity including but not limited to a third party individual, corporation, LLC, partnership, joint venture, sole proprietorships, not-for-profit organizations and/or former or current employees of LICENSOR, to work on and/or perform any services on, or with the Licensed SOFTWARE, LICENSOR can elect at its sole option to terminate this license AGREEMENT.
4. **Limited Warranty Remedy**. For a claim of breach of this limited warranty by the LICENSEE, LICENSEE'S sole and exclusive remedy, and LICENSOR's sole and exclusive liability, will be for LICENSOR, at LICENSOR's option, to

either: (i) provide services to correct any inconsistencies between the SOFTWARE and the Documentation which cause the SOFTWARE to fail to conform to the limited warranty set forth in this Paragraph, which shall include LICENSOR's right to add, modify, or delete portions of the SOFTWARE and/or the Documentation; or (ii) terminate the license, including all rights granted hereunder and refund the license fees, which shall be amortized over a five (5) year period from date of purchase.

5. **Disclaimer of Warranty**. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS OTHERWISE SET FORTH IN THIS AGREEMENT, THE SOFTWARE, DOCUMENTATION AND ANY SERVICES PROVIDED BY LICENSOR ARE PROVIDED "AS IS." THE FOREGOING LIMITED WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES, EITHER ORAL OR WRITTEN, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, EVEN IF LICENSOR OR ANY OF ITS PARENTS, AFFILIATES OR SUBSIDIARIES HAVE BEEN MADE AWARE OF SUCH PURPOSE, AND THE WARRANTY AGAINST INFRINGEMENT OF PATENTS OR OTHER INTELLECTUAL PROPERTY RIGHTS.

6. **Limitation of Liability**. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL LICENSOR, ITS PARENTS, AFFILIATES AND SUBSIDIARIES OR THEIR DISTRIBUTORS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS OR CONSEQUENTIAL, SPECIAL OR INCIDENTAL DAMAGES, ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. NOTWITHSTANDING ANY DAMAGES THAT LICENSEE MAY INCUR FOR ANY REASON WHATSOEVER (INCLUDING, WITHOUT LIMITATION, ALL DAMAGES REFERENCED ABOVE AND ALL DIRECT OR GENERAL DAMAGES), THE ENTIRE LIABILITY OF LICENSOR AND ITS PARENTS, AFFILIATES AND SUBSIDIARIES UNDER ANY PROVISION OF THIS AGREEMENT AND LICENSEE'S EXCLUSIVE REMEDY FOR ALL OF THE FOREGOING SHALL BE LIMITED TO AN AMOUNT EQUAL TO THE LICENSE FEES ACTUALLY PAID BY LICENSEE FOR THE SOFTWARE. THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY FAILS ITS ESSENTIAL PURPOSE.

7. **Miscellaneous**. This License AGREEMENT is the entire AGREEMENT between LICENSEE and LICENSOR and supersedes any other communications, advertisements or understandings, whether oral or written, with respect to the SOFTWARE. This License AGREEMENT is not assignable by LICENSEE in whole or in part without the prior written permission of LICENSOR; LICENSOR may assign this License AGREEMENT or any obligation thereof. This License AGREEMENT may be amended only in writing, signed by both parties. The construction, interpretation and enforcement of this License AGREEMENT, as well as any and all tort claims arising from this License AGREEMENT or arising

from any of the proposals, negotiations, communications or understandings regarding this License AGREEMENT, shall be governed by and construed in accordance with the laws of the State of New Jersey, applicable to contracts made entirely within New Jersey, without regard to the conflict of laws provisions thereto. The sole jurisdiction and venue for any litigation arising out of this License AGREEMENT shall be an appropriate federal or state court located in the State of New Jersey, except that LICENSOR may seek injunctive relief in any venue of its choosing. All remedies available to either party for breach of this License AGREEMENT are cumulative and may be exercised concurrently or separately, and the exercise of any one remedy shall not be deemed an election of such remedy to the exclusion of other remedies. The failure of either party at any time to require performance by the other party of any provision hereof shall not affect the full right to require such performance at any time thereafter, nor shall the waiver by either party of a breach of any provision hereof be taken or held to be a waiver of any succeeding breach of such provision or as a waiver of the provision itself. If any provision or portion thereof of this License AGREEMENT is found by a court of competent jurisdiction to be invalid or unenforceable, the License AGREEMENT shall be construed in all respects as if the invalid or unenforceable provision or portion thereof had been omitted and all other terms and conditions are fully enforceable, and in such case this License AGREEMENT may be modified, amended, and limited, reflecting the intentions of the parties, if and only if such changes are necessary to render the License AGREEMENT valid and enforceable. The headings or titles of the Paragraphs or Subparagraphs of this License AGREEMENT are for convenience only and shall not be used as an aid in construction of any provision hereof. If LICENSEE breaches this License AGREEMENT, LICENSOR shall be entitled, in addition to any other rights available at law or in equity, to immediate injunctive relief without any requirement to post a bond or other security. LICENSEE acknowledges and agrees that LICENSEE had a full and ample opportunity to consult legal counsel regarding this License AGREEMENT, has freely and voluntarily entered into this License AGREEMENT, has read, understood, agreed with and acknowledged each and every provision, including, but not limited to, LICENSEE'S rights, obligations, and applicable terms and conditions as set forth herein. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods is specifically excluded from application to this License AGREEMENT. The SOFTWARE and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer L3 Mobile-Vision, Inc, 400 Commons Way, Suite F, Rockaway, NJ 07866.

END OF SOFTWARE LICENSE AGREEMENT

Third Party Software Licenses

For a list of third party software licenses, please click on the following link:

http://s6.parature.com/FileManagement/Download/e387d3538564423fbdbdc7057a64c820

This document consists of general capabilities information that is not defined as controlled technical data under ITAR part 120.10 or EAR

Index

E

J

K

L

M

U

View (cont'd)
    Minimum Days Online setting, 67
    Plate Reads report, 61
    Product manuals, 282
    RAID, 278
    Rear of vehicle, 37
    Software version, 209
    Summary report, 54
    System logs, 259
    System messages, 270, 299
    System Status page, 262
    Units' status list, 234
    Version of transmission software, 211
View Only – Event user, 309

W

Web address, importing a hotlist from, 110, 121
Web service port, 224
Wildcards, 18
Windows Active Directory. *See* Active Directory Integration Feature
Workstation, backup. *See* Backup PC

Z

Zip file, exporting events to, 70
Zip password, 112