



NLSS Unified Security Suite 2.2

User Manual

Copyright © 2009-2011 by Next Level Security Systems, Inc.

Gateway-20110823

Contents

- Chapter 1: Introduction** 10
 - KEY FEATURES 10
 - COMPONENTS OF THE NLSS UNIFIED SECURITY PLATFORM..... 11
 - NLSS Gateway 11
 - NLSS Unified Security Suite 11
 - Access Control Devices 11
 - Cameras 11
 - NLSS HD Media Decoder 12
 - NLSS External Storage 12
 - Generic Computers 12
 - Generic HD Monitors 12
 - ABOUT SUPERUSERS, OPERATORS, AND CARDHOLDERS 13
- Chapter 2: Installation** 14
 - SYSTEM REQUIREMENTS 14
 - PC Requirements for NLSS Discovery Utility 14
 - PC Requirements for Configuration and Operation 14
 - HARDWARE INSTALLATION 14
 - SOFTWARE INSTALLATION 15
 - Install Security Certificate 15
 - Install Cameras 17
 - Install NLSS Gateways 17

PART 1: OPERATIONS

- Chapter 3: Getting Started** 20
 - LOG IN 20
 - Local Login 20
 - Automatic Log Outs* 21
 - Remote Login 21
 - THE MAIN MENU 21
 - Operations Menu 22
 - Events Menu 22
 - Configuration Menu 22
 - Local Display Menu 23

Chapter 4: Controlling Cameras	24
SELECTING CAMERAS	24
MONITORING CAMERAS	26
Monitor Cameras from the Operations Menu	26
Monitor Cameras from the Local Display Menu	26
Use the Camera Toolbar	27
<i>Video Information</i>	27
<i>Hide Toolbar</i>	28
<i>PTZ (Pan, Tilt, Zoom)</i>	28
<i>Digital Zoom</i>	31
<i>Manual Camera Output</i>	31
<i>Video Analytics</i>	31
<i>Filmstrip</i>	46
<i>Date & Time Selection</i>	47
<i>Rewind and Fast Forward</i>	47
<i>Play/Pause</i>	47
<i>Live/Recorded Toggle</i>	48
<i>Camera Events Toggle</i>	48
<i>Event Bookmark</i>	48
<i>Snapshot</i>	48
<i>Save a Clip</i>	49
<i>Local Microphone Control</i>	49
<i>Volume / Mute</i>	49
<i>Full Screen Toggle</i>	49
<i>Time Sliders</i>	50
Additional Camera Controls	51
<i>Select Stream</i>	51
<i>Camera Events</i>	51
<i>Camera Reports</i>	53
Chapter 5: Displaying Video	54
CREATE AND DISPLAY VIEWS	55
Views: Parameters	55
Views: Actions	56
<i>Create Views</i>	56
<i>Edit Views</i>	56
<i>Delete Views</i>	56
<i>Display Views</i>	57
<i>About Camera Presets, Patrols, and Video Analytics</i>	57
CREATE AND DISPLAY SEQUENCES	57
Sequences: Parameters	58
Sequences: Actions	58
<i>Create New Sequences</i>	58
<i>Delete Sequences</i>	58
<i>Edit a Sequence</i>	59
<i>Display Sequences</i>	59
PUSH VIEWS AND SEQUENCES TO DECODERS	60
<i>Display Views via Decoders</i>	60
<i>Display Sequences via Decoders</i>	61
Chapter 6: Using Floor Plans	62
CREATE FLOOR PLANS	62

Create New Floor Plans	63
Configure Floor Plans	63
USE FLOOR PLANS.....	64
Navigate Floor Plans.....	64
Select and Edit Floor Plans	64
Select Devices in Floor Plans.....	64
<i>Select a Decoder</i>	64
<i>Select a Camera</i>	64
<i>Select a Door</i>	64
Monitor Events on the Floor	65
Deleting a Floor Plan.....	65
Chapter 7: Operations with Reports.....	66
GENERATING REPORTS	66
Systemic Reports	67
Device-Specific Reports.....	67
CATEGORIES OF SYSTEMIC REPORTS.....	68
Access Control Reports	68
Camera Reports.....	68
Cardholder Reports.....	68
Door Reports.....	68
User Reports	68
Video Analytics Reports	68
Chapter 8: Operations with Doors	69
MOMENTARILY UNLOCK A DOOR.....	69
ASSOCIATE CAMERAS AND DOORS	69
Associate Cameras with Doors	70
Disassociate Cameras from Doors.....	70
Display Camera Streams Associated with Doors.....	70
OPEN CAMERA AUDIO FOR AN ASSOCIATED DOOR.....	71
LIST EVENTS FOR INDIVIDUAL DOORS	72
GENERATE REPORTS FOR INDIVIDUAL DOORS	73
Chapter 9: Operations with Cardholders	74
ACTIONS WITH CARDHOLDERS	74
Information on the Cardholder	75
Photo of this Cardholder	75
Activate / Deactivate Cards	75
List Events for this Cardholder	75
Generate Reports for this Cardholder	76
Chapter 10: Monitoring and Handling Events	77
MONITORING EVENTS	77

- Realtime View 78
- Event Log 79
 - Event Log List*..... 79
- EVENT DETAILS 82
 - Event Details Actions 82
 - Event State*..... 82
 - Shunt Toggle* 83
 - Lock State Toggle* 83
 - Written Note Editor* 83
 - Recorded Event* 83
 - Current Snapshot*..... 83
 - Profile Picture* 83
 - Exporting the Event* 84
 - Exit*..... 84
 - Emergency Events 84

PART 2: SYSTEM CONFIGURATIONS

- Chapter 11: General Configuration Functions**..... 86
 - SEARCHING TABLES 86
- Chapter 12: Global Configurations**..... 87
 - CONFIGURE RMS..... 88
 - CONFIGURE CUSTOMER 88
 - Customer Details..... 88
 - Customer: Actions 88
 - CONFIGURE SITES 89
 - Site Details 89
 - Editing Site Details 89
 - CONFIGURE NLSS GATEWAYS..... 89
 - Gateways: General Tab 89
 - General Parameters* 90
 - General Actions* 90
 - Gateways: Wired Network Tab..... 94
 - Gateways: Email Tab 95
 - CONFIGURE HOLIDAYS 95
 - Holidays Table 95
 - Holiday Details 95
 - Holidays: Actions..... 96
 - Add New Holidays*..... 96
 - Edit Holidays* 96
 - Delete Holidays*..... 96
 - CONFIGURE SCHEDULES..... 96
 - Schedules Table 97
 - Schedule Details 97
 - Schedules: Actions..... 98
 - Create New Schedules* 98

<i>Cardholders: General Tab</i>	114
<i>Cardholders: Credentials Tab</i>	115
<i>Cardholders: Access Levels Tab</i>	116
<i>Cardholders: Contacts Tab</i>	117
<i>Cardholders: Organizational Tab</i>	118
<i>Cardholders: User Defined Tab</i>	118
<i>Cardholders: Options Tab</i>	118
CONFIGURE CARDHOLDER-USER DEFINED FIELD LABELS	119
User Defined: Parameters	119
User Defined: Actions	119
CONFIGURE USERS	120
Users Table	120
User Details	120
Users: Actions	120
<i>Create New Users</i>	121
<i>Edit Users</i>	121
<i>Delete Users</i>	121
Chapter 14: Configure Access Control	122
ADDING, EDITING AND DELETING ITEMS	122
Adding Items	122
<i>Edit Items</i>	123
<i>Delete Readers</i>	123
CONFIGURE CONTROLLERS	123
Associating a Mercury Controller with an NLSS Gateway	124
Controller Details	125
<i>Controller Details: General Tab</i>	125
<i>Controller Details: Diagnostics Tab</i>	126
CONFIGURE READER INTERFACES	127
Reader Interface Details	127
<i>Reader Interfaces Details: General Tab</i>	127
<i>Reader Interfaces: Aux Input Tab</i>	128
<i>Reader Interfaces: Aux Output Tab</i>	129
Reader Interfaces: Actions	130
<i>Add Reader Interfaces Manually</i>	130
<i>Delete Reader Interfaces</i>	130
CONFIGURE READERS	131
Reader Details	131
Readers: Actions	132
CONFIGURE DOORS	133
Door Details	133
<i>Door Details: General Tab</i>	133
<i>Doors Details: Strike Tab</i>	134
Doors: Actions	134
CONFIGURE I/O INTERFACES	135
I/O Interface Details	135
<i>I/O Interfaces: General Parameters</i>	135
<i>I/O Interface Details: Aux Input Tab</i>	136
<i>I/O Interface Details: Aux Output Tab</i>	136
I/O Interfaces Actions	137
CONFIGURE I/O LINKAGES	137

I/O Linkages Details	138
I/O Linkages: Actions	138
Chapter 15: Configure Video, Storage, & Decoders	139
CONFIGURE CAMERAS AND STREAMS	139
Cameras Table.....	139
Camera Details: General Tab.....	140
<i>Editable Parameters</i>	140
<i>Read-Only Parameters</i>	141
Cameras: General Actions	141
<i>Connect with a Camera</i>	141
<i>Edit Camera Details</i>	142
<i>Add Cameras</i>	142
Camera Details: Stream Tab.....	143
<i>List of Streams</i>	143
<i>Video Stream Parameters</i>	143
<i>Audio Stream Parameters</i>	144
<i>Cameras: Enabling a Stream</i>	144
Camera Details: Recording Tab	144
<i>Stream Settings</i>	144
<i>Camera Settings</i>	145
<i>Cameras: Recording Configuration</i>	145
CONFIGURE EXTERNAL STORAGE DEVICES	146
Storage Table.....	146
Storage Details.....	146
Storage: Actions	147
<i>Add USB Storage Devices</i>	147
<i>Add eSATA Storage Devices</i>	147
<i>Add iSCSI Storage Devices</i>	147
<i>Add NAS Storage Devices</i>	148
<i>Delete a Storage Device</i>	148
CONFIGURE NLSS HD MEDIA DECODERS	149
Decoder Table.....	149
Decoder Details.....	149
<i>Parameters You Can Edit</i>	149
<i>Read-Only Parameters</i>	149
Decoders: Actions	150
Chapter 16: Remote Management Services	151
RMS HIERARCHY	151
LOGGING IN TO THE CUSTOMER PORTAL.....	152
RMS MAIN MENU.....	152
SITES.....	153
MULTISITE DISPLAY	154
Displaying a View	154
Creating a New View.....	154
Editing a View	155
Deleting a View	155
FULL SCREEN	155

Preface

PURPOSE, SCOPE, AND AUDIENCE OF THIS MANUAL

This document explains how to install, configure, and operate the NLSS Unified Security Suite. The **Operation** part of this document is intended for anyone with basic familiarity with PCs, web browsers, and security concepts. The **Administration** procedures require a slightly greater than average knowledge of these topics, while the **Configuration** procedures require some IT knowledge.

Except for access control devices, the NLSS devices in the Unified Security Suite use common connectors such as AC plugs, and Ethernet and HDMI cables. For instructions on wiring NLSS hardware and third party access control devices, refer to the separate *NLSS Hardware Installation Guide*, which is available on the [NLSS web site](#).

PARTNERS AND THIRD PARTIES

This document refers directly to various devices made by partners and other third parties. All references to makes, models, and trademarks mentioned in this document are the property of their respective owners.

Chapter 1: Introduction

The *NLSS Unified Security Suite* is software that runs on the NLSS Gateway appliance. This software is a unified platform for video surveillance, video analytics, and access control.

The NLSS Unified Security Suite software connects with third party video cameras and access control devices over an IP network. Specifically, it collects data from separate access control devices, video cameras, and a database of users and schedules. The software then organizes and distributes this data via the *NLSS Web Interface*. Users of this software can operate and configure their systems via the NLSS Web Interface.

Users with a single site can use the NLSS Web Interface (in a standard browser) to directly access the NLSS Gateway to operate and configure their systems. Users with multiple sites can use the browser to access *RMS (Remote Managed Services)*, and access the NLSS Gateway at any of their sites.

This document describes how to use the NLSS Web Interface.

1.1 KEY FEATURES

The NLSS Unified Security Suite can be configured and operated via the NLSS Web Interface, which is accessed through most browsers on any PC. NLSS software also provides the following features and benefits:

- **Unified Simplicity:** organizes data from the traditionally separate subsystems of access control, intrusion detection, and video surveillance.
- **Easy to Install and Update:**
 - Comes with the NLSS Discovery Utility, which discovers all NLSS devices on the same layer two network.
 - Most discovered devices can be configured easily and updated in the system without disrupting operations.
 - Can be administered and operated through a browser via the intuitive NLSS Web Interface.
- **Remote Access:** the entire system can be configured, monitored, and administered from a single local or remote location.
- **High Performance**
 - *Modularity:* the basic system requires only one NLSS Gateway at a site. A more robust system can include numerous Gateways with multiple cameras, access points, and users at many physical sites.
 - *Video:* can auto-discover Onvif standard IP cameras, including 1080p HD cameras. Can also display and record video streams from remote encoders and local files that adhere to standard RTSP and HTTP protocols.

- *Intelligence*: Video Analytics are fully integrated and are tracked as events. Video Analytics include Line Crossing, People Count, Directional People Count, Face Capture, Activity Detection, Perimeter Detection, Dwell, Direction, Object Taken, and Object Moved. See [Video Analytics](#) for more information.
- **Remote Monitoring and Backups**: video recordings and other data can be saved on internal hard drives in NLSS Gateways, as well as on external storage devices.
- **Remote Management Service (RMS)**: provides a single entry point to manage multiple sites. Provides the ability to access, configure and operate multiple systems from anywhere, at any time, via a web browser or a mobile device. (RMS is available as an additional service.)

1.2 COMPONENTS OF THE NLSS UNIFIED SECURITY PLATFORM

Along with network and a browser, one NLSS Gateway is the minimum required to configure, administer, and operate the NLSS Security Platform.

1.2.1 NLSS Gateway

The NLSS Unified Security Suite software is embedded in each NLSS Gateway, with *no software licenses*. Each NLSS Gateway is essentially a network device that collects and processes information. The software suite organizes and displays this information for users to monitor and act upon. Each Gateway includes a web server that generates the NLSS Web Interface to access the software suite.

1.2.2 NLSS Unified Security Suite

The NLSS Unified Security Suite software gives you an easy, yet powerful means to monitor, manage and act on data from video cameras and access control devices attached to the same network as the host NLSS Gateway. Using a browser, you can log into the NLSS Web Interface generated by this software.

1.2.3 Access Control Devices

The NLSS Unified Security Suite supports many access controllers, reader interfaces, and readers from Mercury Security, HID, and Assa Abloy. For a complete list of currently supported devices, check the NLSS web site at www.NLSS.com.

1.2.4 Cameras

The NLSS Unified Security Suite supports security cameras that conform to ONVIF standards, as well as most cameras from major manufacturers, including many Arecont, Axis, Bosch, IQInVision, Panasonic, Pelco, and Sony cameras. For a complete list of currently supported cameras, check the NLSS web site at www.NLSS.com.

1.2.5 NLSS HD Media Decoder

Independent Mode software is embedded on each *NLSS HD Media Decoder* so it can operate in a stand-alone mode. When it is part of an NLSS Security Platform, each decoder operates as a slave to an NLSS Gateway. The Gateway manages the decoder.

NLSS strongly recommends the use of NLSS HD Media Decoders for long-term, continuous monitoring of video. Although you can also monitor video in the NLSS Web Interface, you are dependent on a web browser to do so. Due to the complexities and shortcomings of various web browsers, NLSS cannot guarantee the performance, stability, or functionality of video displayed in a web browser.

1.2.6 NLSS External Storage

External Storage devices provide an optional extension of the hard drive space for NLSS Gateways. To increase the Gateway's storage capacity, connect a USB, eSATA, NFS, or iSCSI external storage device directly to a Gateway and configure the drive.

1.2.7 Generic Computers

The NLSS Web Interface is used to control and configure the system, according to user permissions. The interface can be accessed via a browser running on Windows, Linux, Macintosh or Android-based operating systems.

Browsers such as Firefox 3.0+, IE 8.0+, Chrome 12.0+, or Safari 3.0+ can log into any NLSS Gateway in the system.

Adobe Flash Player 10.3 or greater is recommended.

Any computer can access the NLSS Web Interface. As with any software, faster processors and additional RAM can improve performance.

1.2.8 Generic HD Monitors

Video streams processed by the system are rendered in the Gateway and displayed in a browser with the NLSS Web Interface.

The minimum recommended resolution is 1024x768, or greater.

1.3 ABOUT SUPERUSERS, OPERATORS, AND CARDHOLDERS

A *User* is a person with an assigned role, either *Superuser* or *Operator*, who configures and/or operates parts or all of the NLSS Unified Security Suite at a site. A user's role defines his or her software *permissions*, which determines specific administrative rights on the system.

The NLSS Security Platform supports two types of User roles with different permissions.

- *Superusers* can manage all elements of the system.
- *Operators* can:
 - View cameras, configure video analytics, add video PTZ presets, manually control PTZ (pan, tilt, zoom) cameras, view video event, run forensics, run event reports, and export video clips to the FLV format.
 - Configure decoders.
 - Import JPEG floor plans and add devices such as cameras, doors, and decoders.
 - Run and print a variety of reports.
 - Associate doors to cameras and send momentary unlock commands to the door.
 - View cardholder data and activate/deactivate access cards.
 - Create views and sequences.

Notes about Users:

- A *role*, such as Superuser or Operator, contains privileges in the system to perform various functions.
- Only two roles are available: Superuser with all rights, and Operator with limited rights.
- Each User must have a unique ID (email) and password.
- The system comes pre-configured with a Superuser account that cannot be deleted. However, the password to this Superuser account can be customized.

Chapter 2: Installation

This chapter provides instructions for using the NLSS Unified Security Suite software to discover your cameras and access control devices. (Installing hardware is documented separately.)

2.1 SYSTEM REQUIREMENTS

Using the NLSS Web Interface to decode and display video streams in a browser requires hardware and software that meets the following minimum requirements.

2.1.1 PC Requirements for NLSS Discovery Utility

The NLSS Discovery Utility discovers NLSS equipment, Gateways and Decoders.

- Windows XP or more recent operating system
- Windows .NET Framework
- Network connection on a LAN (local area network)

2.1.2 PC Requirements for Configuration and Operation

- Network connection on a LAN.
- The latest version of Firefox 3.0+, IE 8.0+, Chrome 12.0+, or Safari 3.0+
- The latest version of Adobe Flash Player (10.3 or above)

Important: In whichever browser you are using, disable hardware acceleration for Flash.

- See [Generic Computers](#) for hardware and operating system specifications.

2.2 HARDWARE INSTALLATION

For instructions on physically installing NLSS Gateways and HD Media Decoders, see the separate *NLSS Gateway: Quick Start Guide*, which you can download from [NLSS.com](#).

For instructions on physically installing IP cameras and access control hardware, refer to instructions provided by the manufacturers of those devices.

2.3 SOFTWARE INSTALLATION

The installation of your NLSS Unified Security Platform is done in three phases.

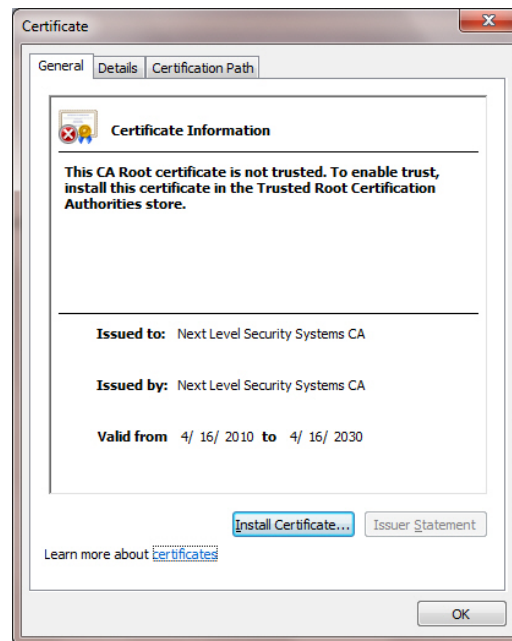
- [Install Security Certificate](#)
- [Install Cameras](#)
- [Install NLSS Gateways](#)

2.3.1 Install Security Certificate

CA certificates are an important component of secure connections using the HTTPS protocol, which NLSS Gateways use for security purposes.

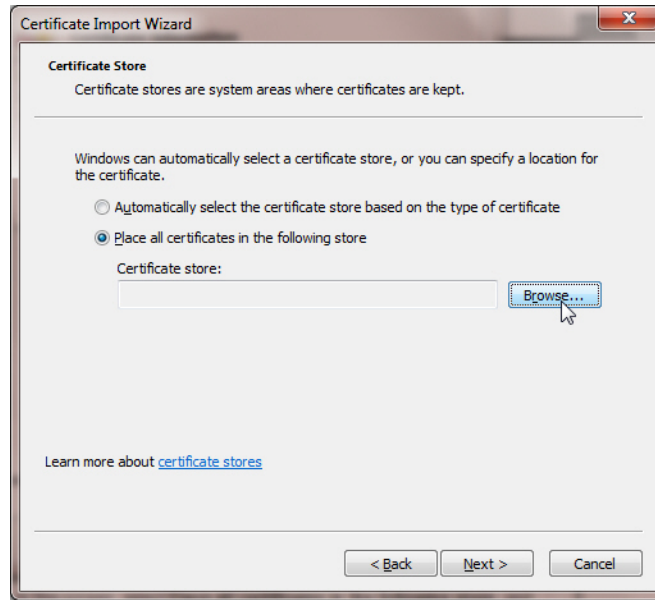
Note: The following instructions for installing the NLSS CA certificate in your browser are only for Internet Explorer (8.0 or above). For other browsers, consult their documentation for instructions on manually installing a CA certificate.

1. Using Internet Explorer, go to <http://www.nlss.com/support.html>. Click the [Downloads](#) link to access a page for downloading NLSS CA certificates.
2. Download the [NLSS Certificate](#), and save it to your desktop.
3. Double-click the certificate file on your desktop to display the Certificate dialog (see the figure below).

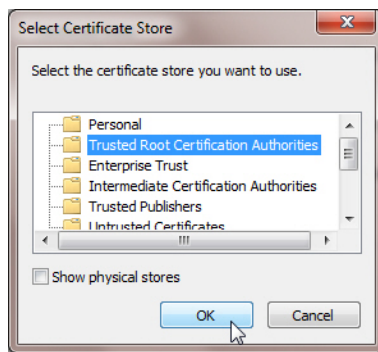


4. In the General tab of the Certificate dialog, click **Install Certificate**. The *Certificate Import Wizard* appears.
5. In the Wizard:
 - a. Click **Next** to display the Certificate Store page.
 - b. Select **Place all certificates in the following store**.

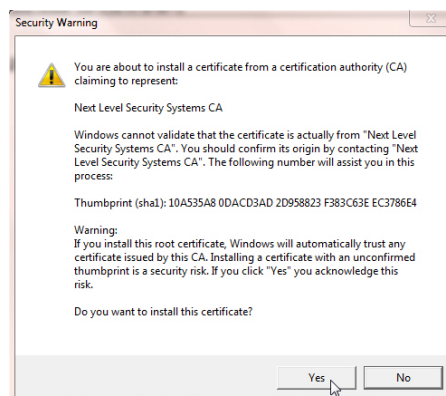
- c. Click **Browse** to display the Select Certificate Store page.



6. In the *Select Certificate Store* page, select **Trusted Root Certificate Authorities**.



7. Click **OK**.
8. Click **Next** and **Finish** to close the Wizard.
9. To complete the installation of the Certificate, click **Yes** in the Security Warning page if it appears.



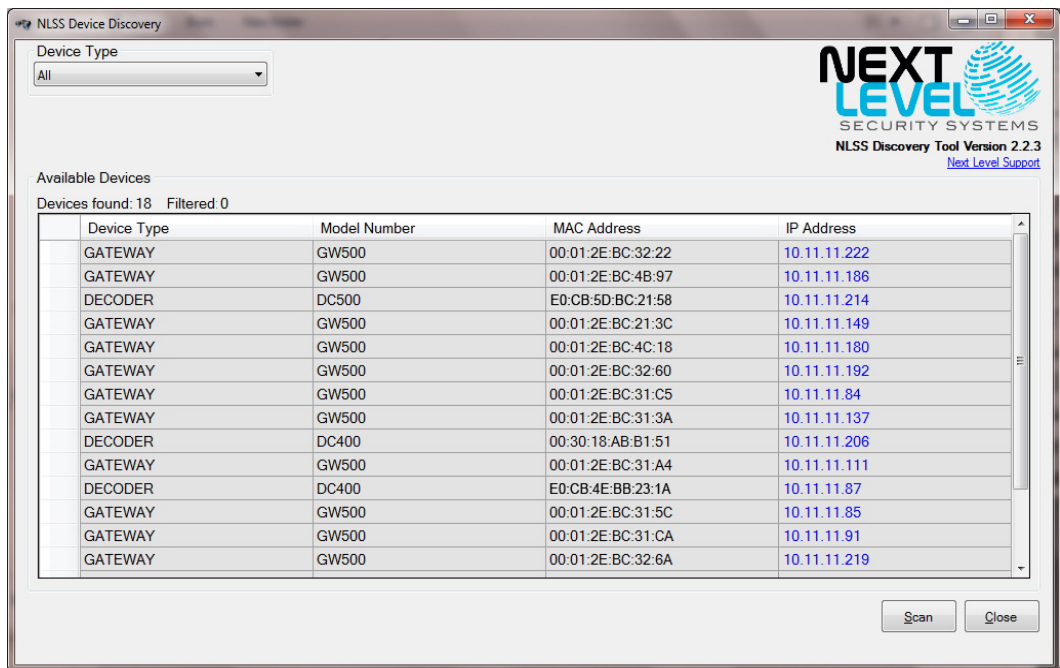
2.3.2 Install Cameras

For ease of discovery, ensure that your IP cameras are installed and powered on a LAN before installing an NLSS Gateway on the same LAN.

Note: For best results, use the same password for all IP cameras. As needed, change the passwords on the cameras according to instructions provided by the manufacturers.

2.3.3 Install NLSS Gateways

1. Physically connect your NLSS Gateway to the local network.
 After the NLSS Gateway is connected to the network, use a computer running a supported operating system and browser to configure and control the system.
 - Ensure the computer has a supported browser, with Adobe Flash Player 10.3 or above plug-in installed. See [Generic Computers](#).
 - Ensure the computer has a high speed Internet connection to support streaming video, and is connected to the same network as the Gateway.
2. Insert the supplied **NLSS Discovery Utility CD** into the computer’s disc drive, or download the software from the NLSS web site (www.nlss.com).
3. Copy the **NLSS Discovery Utility** file to your computer’s hard drive.
4. Run the **NLSS Discovery Tool**.
5. In the *NLSS Device Discovery* screen, click **Scan**. The Utility discovers all the NLSS Gateways and NLSS HD Media Decoders on the same LAN.



The list can be sorted by clicking on a column header.

The scan results of the NLSS Discovery Utility provide both the IP address and MAC address of each NLSS device. Either address can be used with a browser to navigate to the NLSS Web Interface generated by the target NLSS device.

In the discovered device list, the IP addresses are hyper-linked to the respective NLSS Gateways.

6. Click an IP address to open the NLSS Web Interface login screen in the default browser.

Note: An alternate method of connecting to the Gateway is by using the local host name. This host name is based upon the Gateway's MAC address.

Use the following URL to connect to the Gateway with host name:

`http://nlss-gateway-macaddress.local`

where *gateway* is the NLSS device and *macaddress* is the MAC address of the target Gateway.

For example, if the MAC address of a *Gateway 500* is 90:E6:BA:B2:F7:C8, enter:

`http://nlss-gw500-90e6bab2f7c8.local`

(note the removal of colons)

7. Accept other installation prompts, such as plug-ins, etc. Bypass certificate errors, if any.

The NLSS Gateway's login screen is displayed in the browser. This login screen provides access to the NLSS Web Interface generated by the target NLSS Gateway. SuperUser permissions are needed to complete the final steps.

8. Log in as described in [Local Login](#).
9. In the NLSS Web Interface, navigate to the *Configuration > Global > Gateways* screen, and click the **Check Update** button to see if new firmware is available for your NLSS Gateway. If so, update the firmware to the latest version. For instructions, see [Configure NLSS Gateways](#).

PART 1: OPERATIONS

Operations includes instructions and background information on operating every component of the NLSS Security Platform via the NLSS Web Interface. Operators who have limited user permissions may not have access to all functionality discussed in Operations.

Chapter 3: Getting Started

3.1 LOG IN

The NLSS Web Interface can be accessed from the same local network as the NLSS Gateway, or remotely via VPN or a similar service.

3.1.1 Local Login

Using a supported browser running on a computer in the same network as your NLSS system, navigate to any NLSS Gateway in your system. You can enter either the IP address or the local host name of the target NLSS Gateway.

Note: The MAC address of an installed Gateway never changes. If DHCP is used to assign an IP address to the Gateway, then that IP address can change. The NLSS Discovery Utility provides both MAC and IP addresses.

Here is an example of using the IP address to locate a specific NLSS Gateway:

```
https://10.11.11.91/
```

When your browser connects to the target Gateway, a login screen is displayed. Log in with the username and password that your Administrator configured for you.

If you are an Administrator logging into a new Gateway for the first time, you can log in using the following master username and password. These credentials provide unlimited access to configuration, administration, and operation of the system.

- **User: superuser**
- **Password: superuser**

After you log into your Gateway for the first time, we recommend changing the default password for the *Superuser* and *Operator*.

Once the discovery process begins, it may take a few minutes to locate all compatible cameras and access control devices on your network and list them in the NLSS Web Interface.

After devices are discovered by the NLSS Gateway, a status of *Preprovisioned* is listed in the device table. Preprovisioned means the device has been discovered, but has never been out into service with the Gateway. Devices are put into service by setting the **Administrative State** to **In Service** in the **Configuration** menu for the device type. This step is explained in the appropriate sections in this manual.

After a device is placed In Service, the Preprovisioned setting is no longer available. Use the **Out of Service** setting to remove a device from service.

3.1.1.1 AUTOMATIC LOG OUTS

If the NLSS Gateway detects no activity in the NLSS Web Interface for 60 minutes, then the system automatically logs out the User who logged in last. This security feature prevents unattended but logged in interfaces from being permanently available until the User manually logs out.

3.1.2 Remote Login

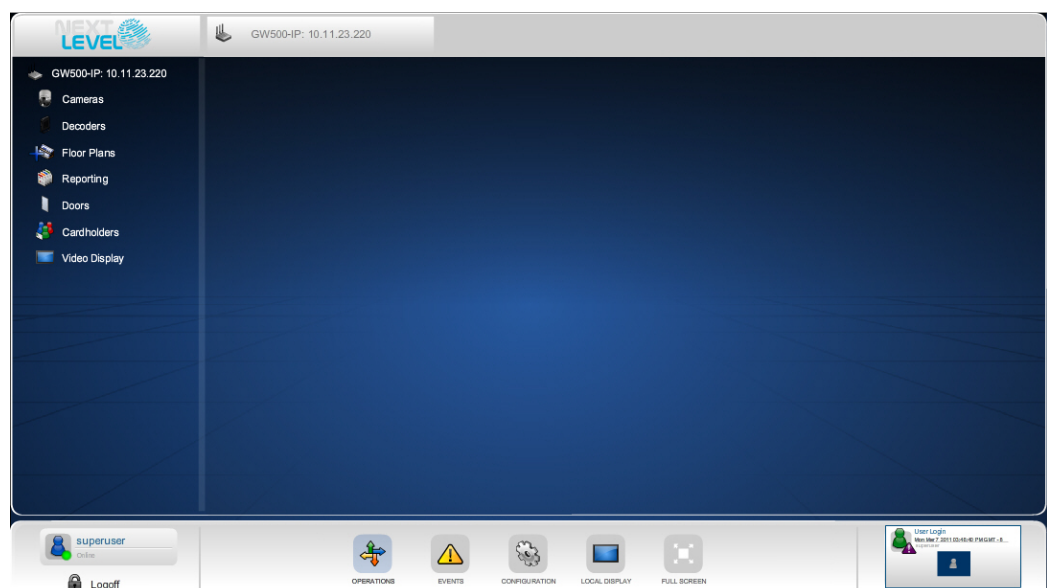
Logging into the system via the NLSS Web Interface is the same for remote users as for local users, except a VPN or another service is required to access the network on which the target NLSS Gateway is installed.

Once you are on the same network as the target NLSS Gateway, then you can enter the IP or MAC address of that Gateway into a browser, and log into the NLSS Web Interface using the [Local Login](#) instructions.

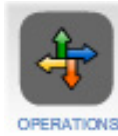
3.2 THE MAIN MENU

Depending on your permissions, you may or may not be able to access all the Main Menu items at the bottom of the screen. Users with unlimited permissions all menu options can access.

- **Logoff:** ends your session on the NLSS Web Interface.
- [Operations Menu](#)
- [Events Menu](#)
- [Configuration Menu](#)
- [Local Display Menu](#)
- **Full Screen:** toggles between full-screen and windowed modes.



3.2.1 Operations Menu



In the Operations menu on the left side of the screen contains most of the functions that Operators of the NLSS system regularly need. Operator accounts are typically configured with permission to access everything under the Operations menu. After you click the **Operations** button, a series of options is displayed in the left pane of the screen, under the Gateway's name.

- **Cameras:** controlling live cameras and accessing recordings. See [Chapter 4: Controlling Cameras](#) for instructions.
- **Decoders:** pushing Views and Sequences in video streams to NLSS HD Media Decoders for display on remote monitors. See [Push Views and Sequences to Decoders](#) for instructions.
- **Floor Plans:** creating and using Floor Plans that show the locations of individual cameras, decoders, and doors. See [Chapter 6: Using Floor Plans](#) for instructions.
- **Reporting:** run reports that summarize events, etc. See [Chapter 7: Operations with Reports](#) for instructions.
- **Doors:** locking and unlocking doors manually, as well as running individual door reports. See [Chapter 8: Operations with Doors](#) for instructions.
- **Cardholders:** tracing and deactivating individual Cardholders, as well as running individual cardholder reports. See [Chapter 9: Operations with Cardholders](#) for instructions.
- **Video Display Configuration:** creating Views for different camera scenes and Sequences for displaying those Views. These results are also used by the Local Display menu. See [Chapter 5: Displaying Video](#) for instructions.

3.2.2 Events Menu

The Events menu provides a timeline of all system events in both a Real Time view and an Event Log view. Users with *Operator* permissions typically have access to everything under the Events menu. For details, see [Chapter 10: Monitoring and Handling Events](#).

3.2.3 Configuration Menu



The Configuration menu allows users with Superuser permissions to configure everything in the system. Operators typically do not have permission to access options under the Configuration menu.

The Configuration menu provides the following options:

- **Global:** provides screens for configuring everything that's not covered in the other categories (see below). See [Chapter 12: Global Configurations](#) for instructions.
- **Identity:** provides screens for configuring cardholders and access levels. See [Chapter 13: Configure Identity and Credentials](#) for instructions.
- **Access Control:** provides screens for configuring access to doors and other entries that are monitored by your NLSS system. See [Chapter 14: Configure Access Control](#) for instructions.

- **Video:** provides screens for configuring installed cameras, NLSS HD Media Decoders, and external storage devices. See [Chapter 15: Configure Video, Storage, & Decoders](#) for instructions.

3.2.4 *Local Display Menu*

The Local Display turns your computer into a spot monitor. Using the Local Display menu, you can monitor Cameras, Views, and Sequences in full-screen mode. View and Sequence choices are created via the **Operations > Video Display Configuration** menu. See [Chapter 5: Displaying Video](#) for instructions.

Five options are available from the View Sources menu.

- **Cameras:** shows the cameras monitored by this Gateway. See [Monitor Cameras from the Local Display Menu](#) for instructions.
- **Views:** provides access to customized views. See [Method 2](#) under [Display Views](#) for instructions.
- **Sequences:** provides quick access to a sequence configured for a camera. See [Display Sequences](#) under [Sequences: Actions](#) for instructions.
- **Toolbar:** toggles to display or hide the Toolbar containing the Main Menu.
- **Show/Hide:** toggles to hide and display the View Sources menu.

Chapter 4: Controlling Cameras

This chapter provides instructions for controlling individual security cameras, as well as RTSP streams from local video files and HTTP streams from the web using a server push.

4.1 SELECTING CAMERAS

Cameras and video streams can be viewed and configured for monitoring from the Cameras menu. These cameras and video streams are discovered by the NLSS Gateway.

To be discovered, a camera has to be physically attached to the same local area network as the Gateway in your system, and the camera must be turned on.

Note: Discovering a camera is not enough to view its video stream. To play video streams from a camera, the system must also be able to connect to the camera, which requires configuring the camera to use its user name and password. See [Configure Cameras and Streams](#) for configuration instructions.

An embedded video player displays a camera or video stream when it is selected.

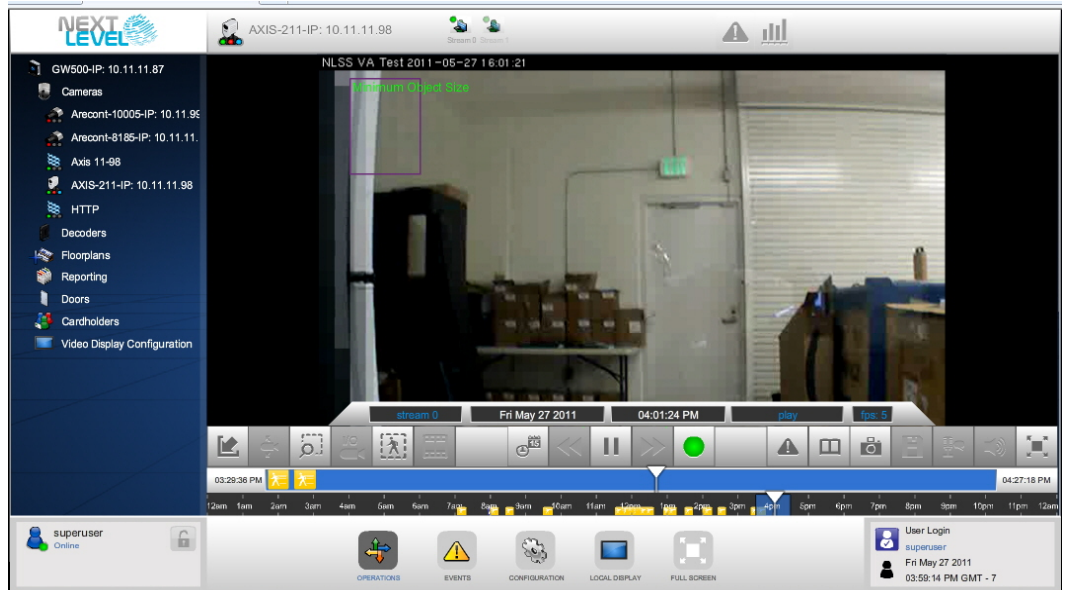
1. Select **Operations > Cameras** from the Main Menu of the NLSS Web Interface.
A list of cameras and other supported video streams is displayed in the left column.
2. Click the corresponding link to select a camera or video stream.

The video player is displayed in the center pane; and the Camera Toolbar is displayed under the video player. Stream, Events and Reports options are displayed above the player.

The NLSS Web Interface displays these video streams on the screen, and can push them to remote monitors supported by NLSS HD Media Decoders.

The NLSS Gateway supports all of the camera features listed in this chapter, some of which are not available on all cameras. Some cameras also may have features that are not supported by the NLSS Gateway at this time.

Note: Hardware configuration can be done only by Users with Superuser permissions.



In the Cameras list, the icon appearing next to each camera’s name indicates the operational state of the camera:

- Green dot: indicates the system is successfully connected to the camera.
- Red dot: indicates that the camera is currently recording.
- Blue dot: indicates that analytics are running.
- Red X: indicates a previously established connection with this camera has been lost.
- Spinning animation: indicates the system is attempting to connect with the camera.
- Streaming symbol: indicates an RTSP or HTTP video stream.



4.2 MONITORING CAMERAS

The ability of the NLSS system to display video in a web browser is intended to aid investigations with video surveillance, but is not intended to provide constant long-term surveillance. Due to the complexities and shortcomings of various web browsers, NLSS cannot guarantee the performance, stability, or functionality of video displayed in a web browser. For displaying video constantly over long periods, we recommend adding one or more *NLSS HD IP Media Decoders* in your system.

- [Monitor Cameras from the Operations Menu](#)
- [Monitor Cameras from the Local Display Menu](#)
- [Use the Camera Toolbar](#)
- [Additional Camera Controls](#)

4.2.1 Monitor Cameras from the Operations Menu

In the NLSS Web Interface, camera streams can be displayed from two locations under the Operations menu:

- **Operations > Cameras**
 - In the Camera list, select a camera to display it in the embedded video player.
 - If the camera outputs more than one stream, and these streams were enabled when the camera was configured. Select a stream from the options above the video player.
 - Use the toolbar under the video player to control the selected camera. See [Use the Camera Toolbar](#).
- **Operations > Video Display Configuration**
 - Select a View or Sequence to display it in the embedded video player. For details on configuring and using Views and Sequences. See [Chapter 5: Displaying Video](#).

Optionally, you can push streams to remote monitors via NLSS HD Media Decoders in your system. See [Push Views and Sequences to Decoders](#) for details.

4.2.2 Monitor Cameras from the Local Display Menu

You can monitor video in the Local Display menu using a web browser to access the NLSS Web Interface for a Gateway in your system.

1. Select **Local Display** from the Main Menu.
The View Sources menu is displayed in a blank pane.
2. Click either **Cameras**, **Views** or **Sequences**. A list of available items appears.
For example, if you select Views, a list of Views appears. Views and Sequences are discussed in [Chapter 5: Displaying Video](#).
3. Click the desired item from the list to display it on your screen.
For instance, if you selected Cameras in the previous step, select the desired camera to display its stream on your screen.

- To exit the Local Display screen, display the Toolbar, if it is hidden, and then select another option from the menu.

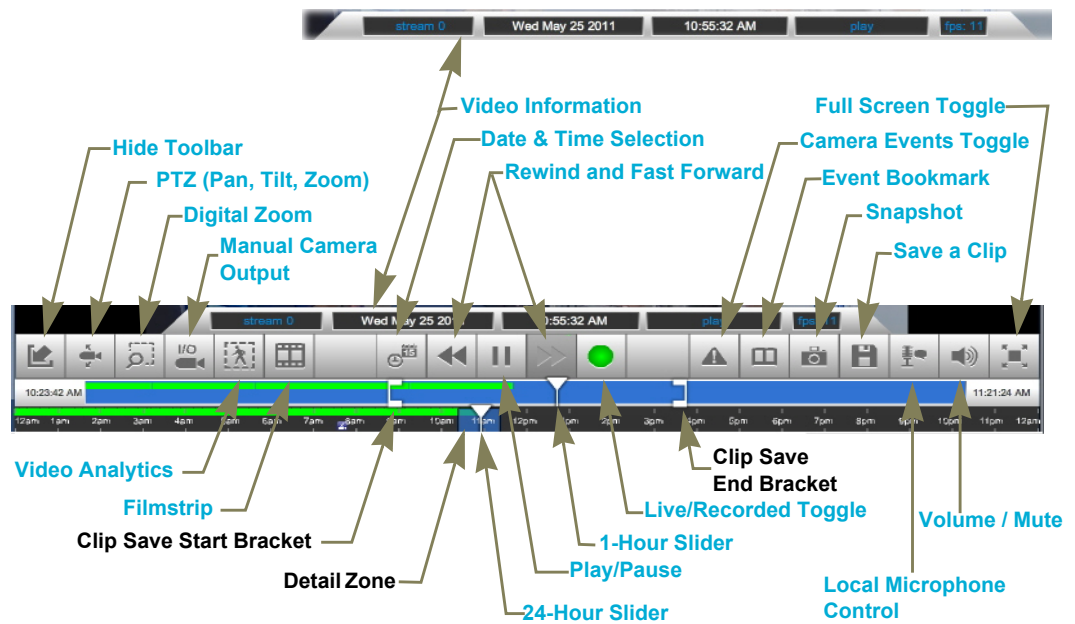
The View Sources menu can be moved on the screen by clicking and holding the Drag button on the left and moving the menu to the desired location.

4.2.3 Use the Camera Toolbar

If you select the **Operations > Cameras** menu, a list of discovered camera streams, RTSP streams and HTTP streams is displayed. Select a stream from this list to display it in the embedded video player.

The Camera Toolbar appears under the embedded video player for both live and recorded cameras, as well as other types of streams.

The Camera Toolbar contains video information, a series of controls, and a timeline.



4.2.3.1 VIDEO INFORMATION

The Camera Toolbar provides the information about the video playing for the selected camera, whether it is live or recorded.

- Stream:** the stream number from the camera, as selected above the video player. See [Select Stream](#).

Note: Some cameras output two or more separate streams simultaneously, each with a different codec or resolution.

- Date:** the date of the video stream that is playing.
- Time:** the time of day of the video stream that is playing.
- Status:** what the video player is currently doing: **play**, **rewind**, **fast forward**, etc.
- FPS:** frames per second of the video stream that is playing.

4.2.3.2 HIDE TOOLBAR

The Camera Toolbar can be temporarily hidden.

- Click the **Hide** button. The toolbar disappears.
- Click the **Show Toolbar** button in the lower left corner to display the Toolbar.

4.2.3.3 PTZ (PAN, TILT, ZOOM)

Cameras that support PTZ or just zoom can be controlled from the NLSS Web Interface. The controls function like a joystick for the selected camera, if that camera supports PTZ.

Click the **PTZ** button to display pan, tilt, and zoom controls.



- **Pan and Tilt:** click-hold anywhere over the video stream within the video player, and drag the mouse. The cursor becomes a small hand.
As an alternative, click-hold the virtual joystick and move it.
If the camera is capable of pan and tilt movements, it follows the mouse movements.
- **Zoom:** click-hold-drag the vertical zoom slider to zoom the camera.
- **Preset:** saves the current position of the selected camera. See [Using Presets](#) for details.
- **Patrol:** organizes two or more Presets into a *Patrol*. When the Patrol is activated, the camera moves to the first Preset, holds that position for a configured time then moves to the second Preset, and continues to cycle through the Presets. See [Using Patrols](#) for more information.

Click the **PTZ** button again to hide the controls.


4.2.3.3.1 Using Presets

A Preset saves the current position and zoom settings of the selected PTZ camera. Using the NLSS Web Interface, you can create, save, edit, and use numerous custom Presets, as well as one Home Preset.

1. Click the **PTZ** button to display the PTZ controls.

2. Navigate to the Cameras menu and select a PTZ-enabled camera. The video stream from that camera is displayed in the video player in your browser.
3. In the Camera Toolbar, click the **PTZ** button to access that function.
After PTZ is accessed, you can configure the Presets for that camera:
 - **Create and Use a Home Preset**
 - **Create Custom Presets**
 - **Use Custom Presets**
 - **Edit Presets**
 - **Delete Presets**


CREATE AND USE A HOME PRESET

1. Move and zoom the camera to the desired position for a Home Preset.
2. Click the **Update** button (green check ) next to the Home button to set this position as the Home Preset.

At any time, you can move the camera to the Home Preset by clicking the **Home** button.

CREATE CUSTOM PRESETS

In addition to a Home Preset, custom Presets can be added.


1. Move and zoom the camera to the desired position of the first Preset.
2. Click the **Preset** button in the upper left to display an **Add** button (plus (+) sign).
3. Click **Add (+)** button to display the *Add PTZ Preset* dialog.
4. In the dialog, enter a unique **Preset Name** and **Preset ID** number.
5. Click the **Update** button (green check ) next to the Preset to save the new setting.
 - Click the **Cancel** button (red X) to ignore the setting and close the dialog.
6. Repeat the steps above to create additional Presets.
7. Click the **Preset** button again to hide the **Add** button.

The *PTZ Preset List* for that camera is displayed under the Presets button.

USE CUSTOM PRESETS

1. Click the **Preset** button to display the PTZ Preset List.
2. In the PTZ Preset List, click a Preset to move the camera to the desired position.

EDIT PRESETS

1. Move and zoom the camera to the desired new position.
2. Click the **Preset** button to display the PTZ Preset List.
3. In the PTZ Preset List, click the **Update** button (green check ) next to the Preset you wish to update. The preset is updated with the current position of the camera.

Note: The previous Preset is lost when you click the check.

DELETE PRESETS

1. Click the **Preset** button to display the PTZ Preset List.
2. In the PTZ Preset List, click the **Trash Can** button next to the green check mark for the Preset that you want to delete.

4.2.3.3.2 Using Patrols

When you activate a Patrol, the affected camera moves from one Preset to the next in a defined order, pausing at each position for a configured time. Use the NLSS Web Interface, to create, save, edit and use custom Patrols.

1. Navigate to the Cameras menu and select a PTZ-enabled camera. The video stream from that camera is displayed in the video player in your browser.
2. In the Camera Toolbar below the video player, click the **PTZ** button to access the Patrol functionality:
 - **Create and Edit Patrols**
 - **Use Existing Patrols**
 - **Delete Patrols**

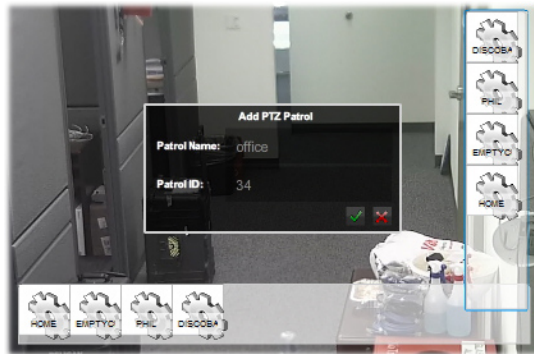
CREATE AND EDIT PATROLS

1. Click the **Patrol** button to display a blue plus (+) button in the video player.
2. Click the plus (+) button to display the *Add PTZ Patrol* dialog.
3. In the dialog, enter a **Patrol Name** and **Patrol ID**.
4. Click the **Update** button (green check ✓) to save the new Patrol.
Click the **Cancel** button (red X) to ignore the setting and close the dialog.

After a Patrol is created, it must be configured. The same procedure is used to edit a Patrol.

1. Click the **Patrol** button to refresh the list.
2. Click the desired Patrol in the list.

The *Edit PTZ Patrol* dialog is displayed. A list of Presets is displayed as icons in a vertical column on the right of the dialog. A blank horizontal column at the bottom of the dialog. Using these columns, Presets can be added, removed and reordered for a Patrol.



- To add a Preset to the Patrol, drag that Preset's icon from the vertical column to the horizontal column.
 - To reorder the Presets in a Patrol, drag the Preset icons in the horizontal list into the desired order.
 - To remove a Preset in the Patrol, drag that Preset's icon out of the horizontal list.
3. By default, the camera pauses for 5 seconds at a Preset, before moving to the next Preset in the list. To change this time:
 - a. Click the desired Preset in the horizontal list. The *Edit PTZ Patrol Item* dialog is displayed.
 - b. Enter the new pause time (in seconds).
 - c. Click the **Update** button (green check ✓) to save the new Patrol.
Click the **Cancel** button (red X) to ignore the setting and close the dialog.

USE EXISTING PATROLS

1. Click the **Patrol** button to display a list of existing Patrols.
2. Click the desired patrol in the list to activate that patrol.

DELETE PATROLS

1. Click the **Patrol** button to display a list of existing patrols.
2. To delete a patrol in the list, click the **Trash Can** button next to the target patrol.

4.2.3.4 DIGITAL ZOOM

1. Click the **Digital Zoom** button. The *Magnifying Glass* tool is opened.
2. Move the zoom slider up and down to zoom in and zoom out in the video player display.
3. Drag the Magnifying Glass over the small display of the video player display to take a closer look at a particular area.
4. Click the **Digital Zoom** button again to close the Magnifying Glass tool.

Note: The Digital Zoom does not move the camera or operate its zoom function. This tool only changes the video player display.

4.2.3.5 MANUAL CAMERA OUTPUT

Click this button in the toolbar to enable the camera's output port for five seconds.

4.2.3.6 VIDEO ANALYTICS

A *video analytic* recognizes certain movements and other behaviors within a video stream. When set thresholds are exceeded, an event is triggered.

The NLSS Unified Security Suite supports video analytics. You can configure multiple video analytics for each camera, but only one analytic can run on a camera at a time. The total number of video analytics that can run across your system is platform dependent.

Video analytics are the most processor intensive operations in the system, and therefore the number of analytics that run simultaneously is limited. Different analytics require different levels of processing power.

The system performance requirements of video analytics vary, depending upon the behavior, scene, activity in a scene, shadows, specific camera, frame rate, bit rate, etc.

A baseline level of **1** (one) is used to measure the impact of a video analytic behavior on the system. This table shows the relative impact level of different analytics. The lower metric level indicates less impact on the system’s processing.

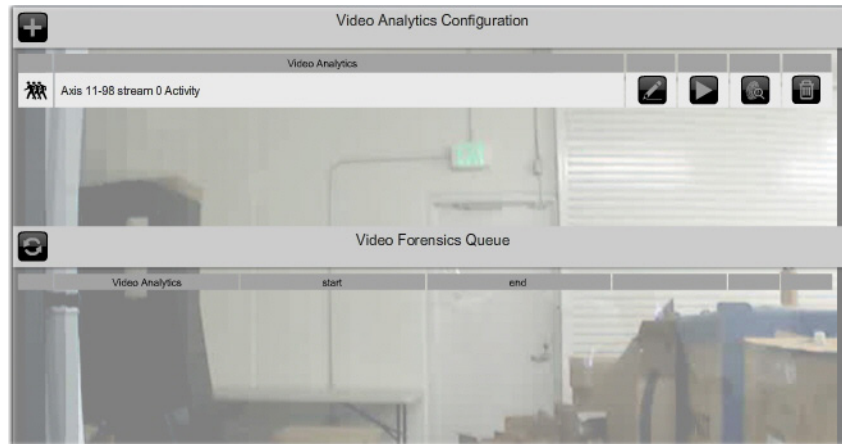
Metric Level	Video Analytic
.5	Transcode One transcode is required for each MPEG4 encoded video stream that is viewed via the browser.
1	Activity Direction Face Capture Line Crossing People Count People Count Direction Perimeter
2	Dwell Object Moved Object Taken
3	Forensic video analytics

The total number of *Metric 1* video analytics that can be supported is determined on a per platform (NLSS device) basis. See the NLSS web site, nlss.com, for specific information.

When an analytic detects an event for which it is looking, an event is generated in the timeline. Camera events are discussed in [Camera Events](#).

1. Open the **Cameras** menu and select a camera or streaming video. The camera’s video stream is displayed in the video player in your browser.
2. In the *Camera Toolbar* under the video player, click the **Analytics** button. The *Video Analytics Configuration* overlay is displayed with the *Video Analytics Configuration* list and *Video Forensics Queue*.
 - The Video Analytics Configuration list contains the analytics set for this camera. From this list, you can edit, play or pause, or delete an analytic. You can also send an analytic to the Video Forensics Queue.

- The Video Forensics Queue lists the analytics that have been tagged for further analysis. See [Video Forensics](#).



Click the **Analytics** button in the toolbar to hide these analytics displays.







3. Click the **Add Video Analytics (+)** button at the top of the list to attach an analytic to a camera. The *Video Analytics* options pop-up menu is displayed.



4. Click the desired video analytic. The analytic is added to the Video Analytic Configuration list.

The video analytic options are discussed in the following subsections.

- [Activity](#)
- [Direction](#)
- [Dwell](#)
- [Face Capture](#)
- [Line Crossing](#)
- [Object Moved](#)
- [Object Taken](#)
- [People Count](#)
- [People Count Directional](#)
- [Perimeter](#)

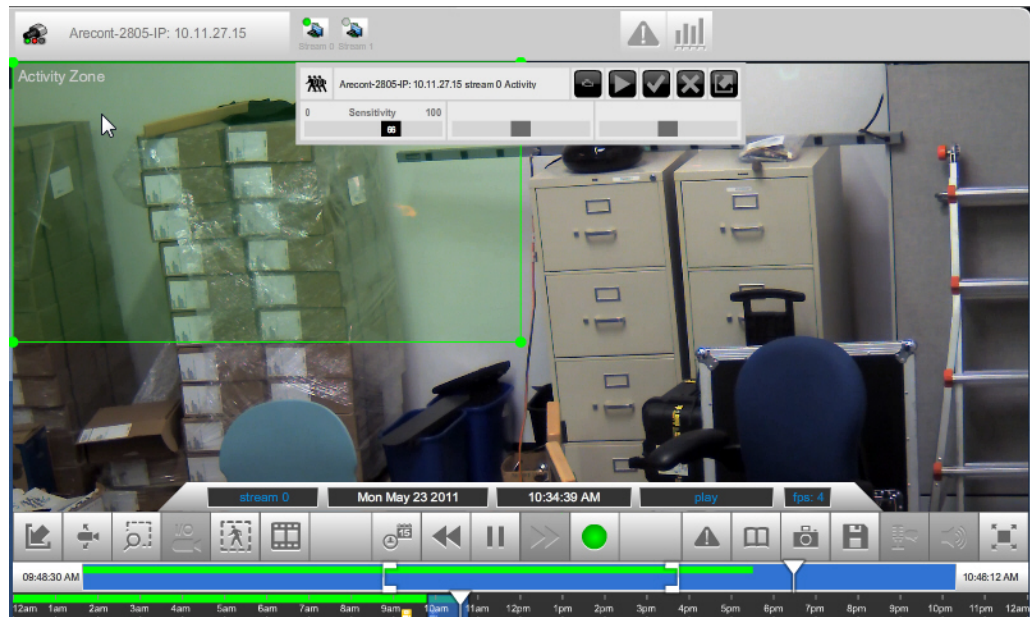
5. Click an analytic in the list to select it to configure.
 - Click the **Edit** button to configure or edit the analytic. The parameters vary between the video analytic options. Sensitivity is set for all analytics. The higher the number, the more likely the analytic is to trip and generate an event.

 - Click the **Save** button to keep the settings.

Click the **Cancel** button to leave edit mode without saving the changes.

 - Click the **Start** button to activate the analytic. Only one analytic can run for a camera at one time.

 - Click the **Stop** button to stop the analytic for running on that camera.

 - Click the **Hide** button to hide the Video Analytic Edit dialog.


4.2.3.6.1 Activity

Activity detects movement within a selected area. The area is drawn in the video player while in edit mode for this analytic:

1. Click the **Edit** button for **Activity** in the Video Analytics Configuration list.
The video player is displayed with an *Activity Zone* highlighted. By default, a rectangular area is selected.
2. Click-hold-drag the rectangle to move the rectangle to the area that you want to monitor.

- Click-hold-drag the corner points of the rectangle to resize and reshape it to select the area to be monitored.



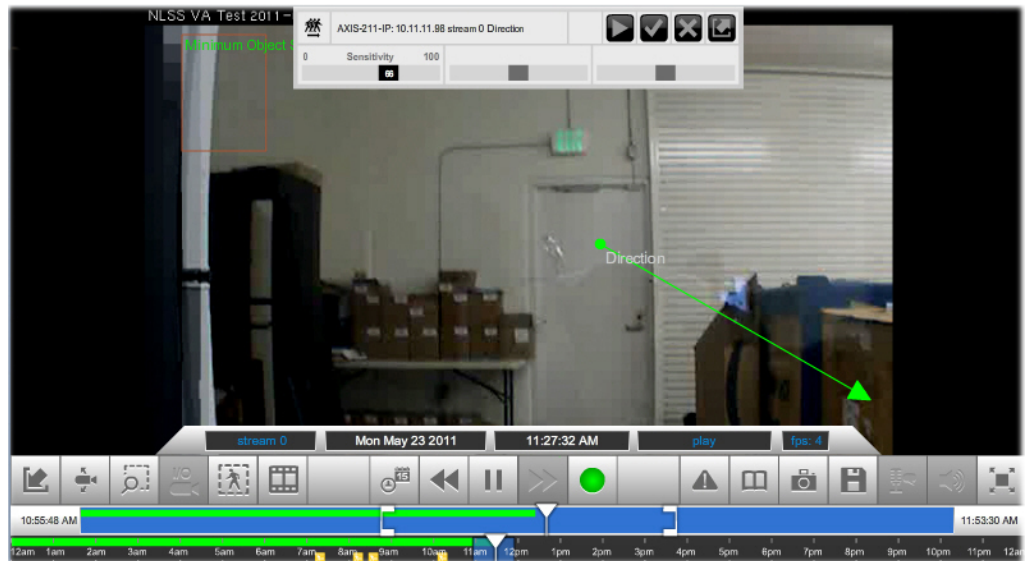
- Adjust the **Sensitivity** slider to set the sensitivity of this video analytic. Higher values make this video analytic more sensitive to small movements and small objects.
- Click the **Save** button to keep the changes.
- Click the **Start** button to activate this video analytic. If someone (or something large enough) moves through the rectangle, a video analytic event is generated.

4.2.3.6.2 Direction

Direction detects movement in a specific direction within the video stream. The direction is defined by drawing a directional line in the video player.

- Click the **Edit** button for **Direction** in the Video Analytics Configuration list.
The video player is displayed containing a line with an arrow indicating the direction in which movement will be monitored.
- Click-hold-drag the line to move it around the video stream.

3. Click-hold-drag the end point (green dot) to change the direction and distance of a movement needed to trigger the analytic.



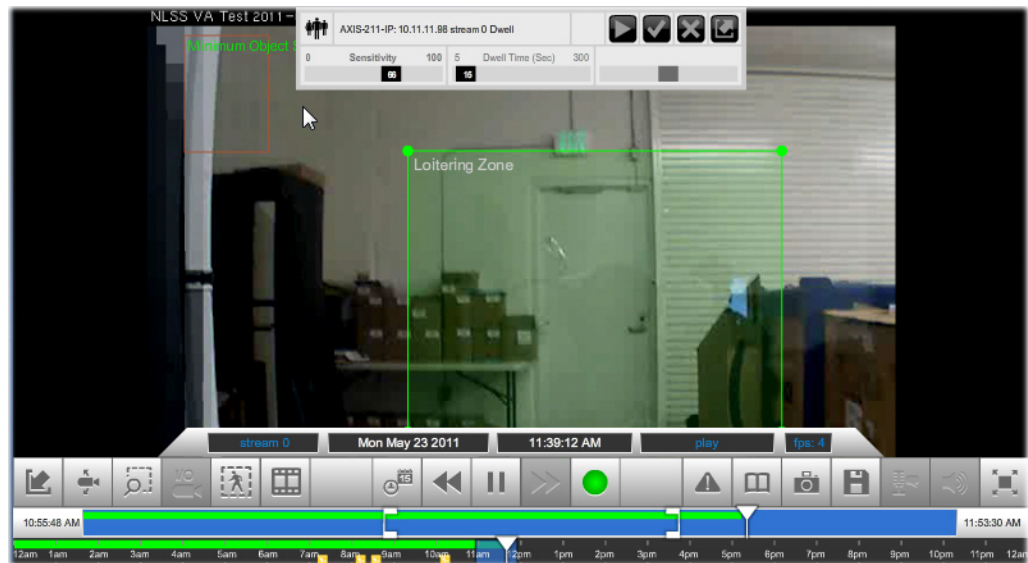
4. Adjust the **Sensitivity** slider to set the threshold of this video analytic. Higher values make this video analytic more sensitive to small movements.
5. Click the **Save** button to keep the changes.
6. Click the **Start** button to activate this video analytic. A video analytic event is generated if a movement is detected for the set direction and distance.

4.2.3.6.3 Dwell

Dwell detects when an object or a person moves into a monitored location and stays longer than a designated time.

1. Click the **Edit** button for **Dwell** in the Video Analytics Configuration list.
The video player is displayed with a *Dwell Zone* highlighted. By default, a rectangular area is selected.
2. Click-hold-drag the rectangle to move the rectangle to the area that you want to monitor.

- Click-hold-drag the corner points of the rectangle to resize and reshape it to select the area to be monitored.



- Adjust the **Sensitivity** slider to set the threshold of this video analytic. Higher values make this video analytic more sensitive to the lack of movement.
- Adjust the **Dwell Time** slider to set the length of time (in seconds), to pass before an analytic event is generated because someone stayed in the designated zone for too long.
- Click the **Save** button to keep the changes.
- Click the **Start** button to activate this video analytic. If a person or object stays in the Dwell Zone for longer than the set threshold, a video analytic event is generated.

4.2.3.6.4 Face Capture

Face Capture records all clearly visible faces as events. You can see the faces later by displaying the events referencing them.

- Click the **Edit** button for **Face Capture** in the Video Analytics Configuration list. The video player is displayed with a rectangular *Face Capture Zone* highlighted.
- Click-hold-drag the rectangle to move the Face Capture Zone to the area that you want to monitor.
- Click-hold-drag the corner points of the rectangle to resize and reshape it to select the area to be monitored.
- Use the **Sensitivity** slider to adjust the threshold of this video analytic. Higher values make this video analytic more sensitive to smaller images of faces. Larger values require that a face be a larger size (relative to the picture) before the system attempts to record that face.
- Click the **Save** button to keep the changes.
- Click the **Start** button to activate this video analytic.

A square, labeled *Minimum Object Size*, is displayed to indicate the minimum size that a face image must be to be recognized by the system. The size is based on the Sensitivity setting, and cannot be adjusted by clicking and dragging the corners of the square. This square is an indicator, and does not need to be moved.

- To increase the minimum object size, increase the **Sensitivity** setting.
- To reduce the minimum object size, reduce the **Sensitivity** setting.

If someone moves into the Face Capture Zone, and the image of their face meets the minimum object size, then a video analytic event is generated.

CONFIGURATION NOTES

- A *larger* Face Capture Zone results in a *longer* detection time. Reduce the size of the Face Capture Zone to reduce the detection time.
- A *smaller* Minimum Object Size results in a *longer* detection time. Increase the Sensitivity setting to reduce the detection time.

FAQ ON THE FACE CAPTURE VIDEO ANALYTIC

- What if you define a randomly shaped Face Capture Zone?
 - For Face Capture Zones other than rectangles, the video analytic engine automatically selects the minimum rectangle that covers the defined shape.
- Why does the minimum face size differ between cameras even when you use the same threshold number?
 - The minimum detectable face size is affected by the number of pixels within the Face Capture Zone, the aspect ratio of the zone, and the camera's resolution.
 - The video analytics engine automatically adjusts the minimum face size for optimal detection. Basically, smaller activity zone (or bigger minimum face) results in better frame rate and also lower CPU usage, and vice versa.
- How does the face detection engine learn about background objects?
 - The video analytics engine has a smart filter for filtering mathematically face-like background objects.
 - The engine recognizes a face as a background object after it stays motionless for a certain amount of time in the scene and stops sending out events.
 - The smart filter is updated after the object is removed from the position for a certain time.

4.2.3.6.5 Line Crossing

Line Crossing monitors movement that crosses a line you draw in the video player.

1. Click the **Edit** button for **Line Crossing** in the Video Analytics Configuration list. The video player is displayed with a red line labeled *Line Crossing* displayed.
2. Click-hold-drag the line to move it to the location that you want to monitor, such as a door or hallway.

3. Click-hold-drag each end point to resize and position the line to cover the area to be monitored. Position the tripwire so the people and things you wish to measure must cross it.



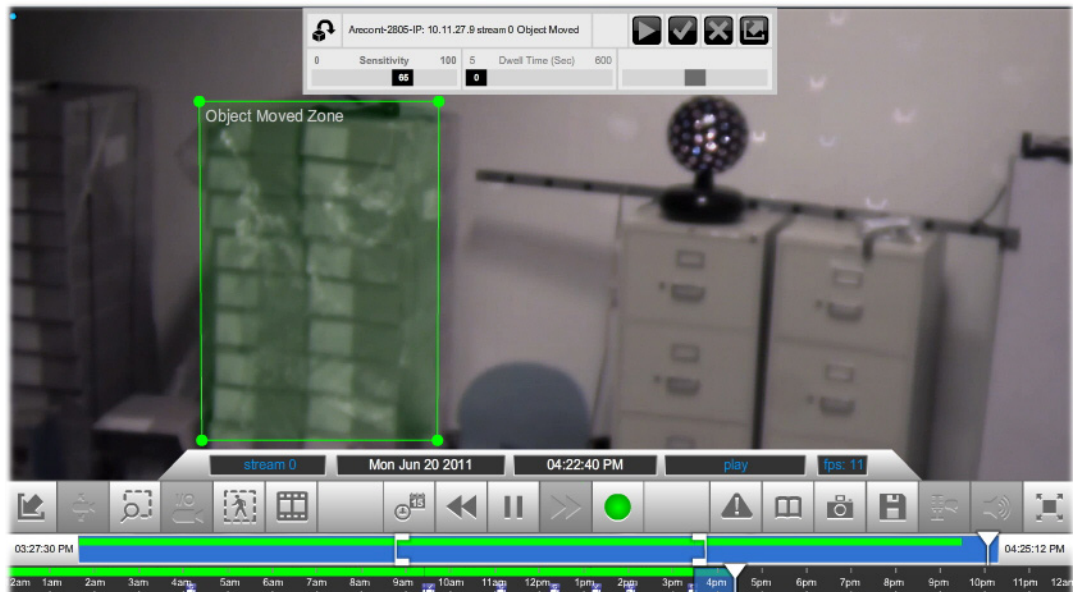
4. Use the **Sensitivity** slider to adjust the threshold of this video analytic. Higher values increase sensitivity to small movements.
5. Click the **Save** button to keep the changes.
6. Click the **Start** button to activate this video analytic. If a person or object moves across the line crossing in either direction, an event is generated.

4.2.3.6.6 Object Moved

Object Taken monitors for objects that are placed in or removed from an area.

1. Click the **Edit** button for **Object Moved** in the Video Analytics Configuration list. The video player is displayed with a *Object Left Zone* highlighted. By default, a rectangular area is selected.
2. Click-hold-drag the rectangle to move the rectangle to the area that you want to monitor. The smaller the box, the more precise the monitoring.

- Click-hold-drag the corner points of the rectangle to resize and reshape it to select the area to be monitored.



- Adjust the **Sensitivity** slider to set the threshold of this video analytic. Higher values make this video analytic more sensitive to an object being left.
- Set the **Dwell Time** for the length of time needed to trigger an event.
 - If an object is left in the *Object Moved Zone* for longer than the Dwell Time, an event is triggered.
 - If the analytic detects that an object has been removed from the *Object Moved Zone* for longer than the Dwell Time, then an event is triggered.
- Click the **Save** button to keep the changes.
- Click the **Start** button to activate this video analytic. If an object stays in the Object Left Zone for longer than the set threshold, a video analytic event is generated.

4.2.3.6.7 Object Taken

Object Taken monitors for objects removed from a selected area.

- Click the **Edit** button for **Object Taken** in the Video Analytics Configuration list. The video player is displayed with a *Object Taken Zone* highlighted. By default, a rectangular area is selected.
- Click-hold-drag the rectangle to move the rectangle to the area that you want to monitor.

- Click-hold-drag the corner points of the rectangle to resize and reshape it to select the area to be monitored.



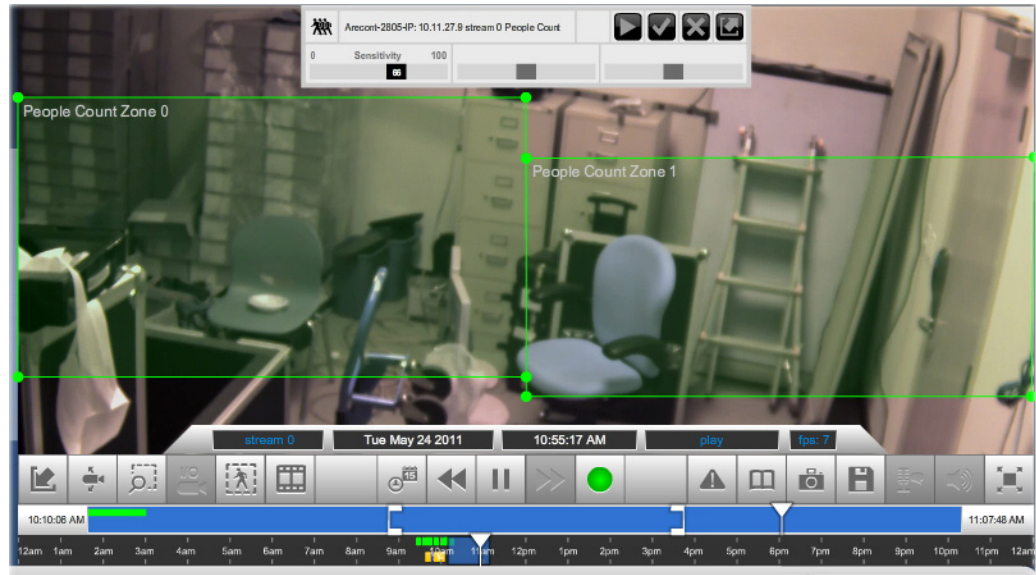
- Adjust the **Sensitivity** slider to set the threshold of this video analytic. Higher values make this video analytic more sensitive to an object being removed.
- Click the **Save** button to keep the changes.
- Click the **Start** button to activate this video analytic. If an object is removed from the Object Taken Zone, a video analytic event is generated

4.2.3.6.8 People Count

People Count monitors the number of humans moving from one zone to another in the video stream. The count is done in either direction.

- Click the **Edit** button for **People Count** in the Video Analytics Configuration list.
The video player is displayed with two highlighted areas: *People Count Zone 0* and *People Count Zone 1*.
- Click-hold-drag each rectangle to move it where you want monitor in the video stream.

3. Click-hold-drag the corner points of each rectangle to resize and reshape it, so as to encompass the area to be monitored.



4. Adjust the **Sensitivity** slider to set the threshold of this video analytic. Higher values make this video analytic more sensitive to movement between the zones.
5. Click the **Save** button to keep the changes.
6. Click the **Start** button to activate this video analytic. If someone moves from one zone to the other, in either direction, a video analytic event is generated.

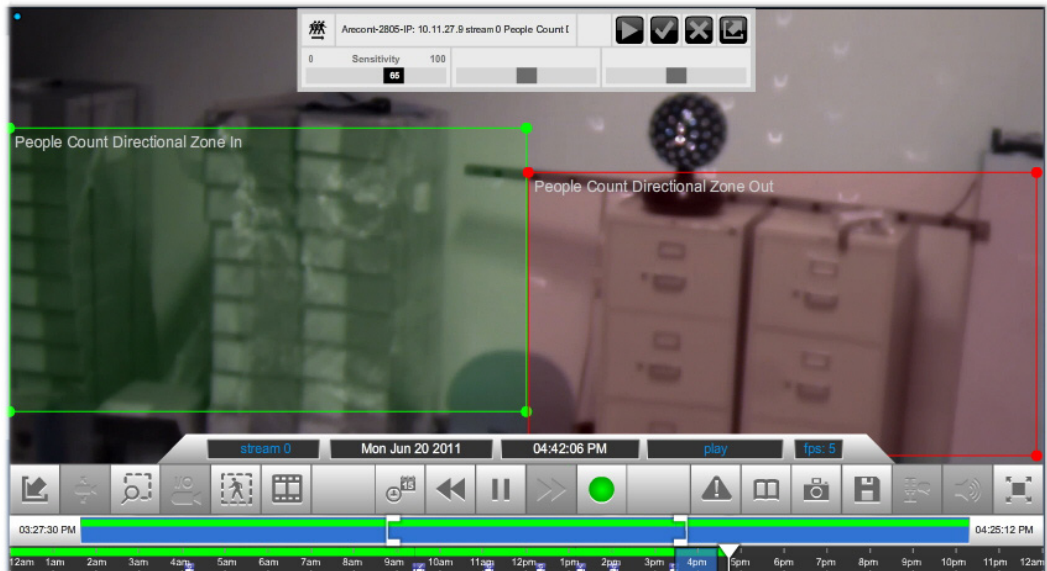
4.2.3.6.9 People Count Directional

The People Count Directional video analytic is the directional version of the **People Count** video analytic. It monitors people moving from one zone to another, but only in one direction. Just as with the non-directional version of People Count, you define both areas with rectangles in the video player.

1. Click the **Edit** button for **People Count Directional** in the Video Analytics Configuration list.
The video player is displayed with two highlighted areas: *People Count Zone 0* and *People Count Zone 1*.
2. Click-hold-drag each rectangle to move it where you want monitor in the video stream.

Note: To register as a People Count Directional event, people must move from the *Direction In* (green) rectangle to the *Direction Out* (red) rectangle, but not the other way.

- Click-hold-drag the corner points of each rectangle to resize and reshape, so as to encompass the area to be monitored.



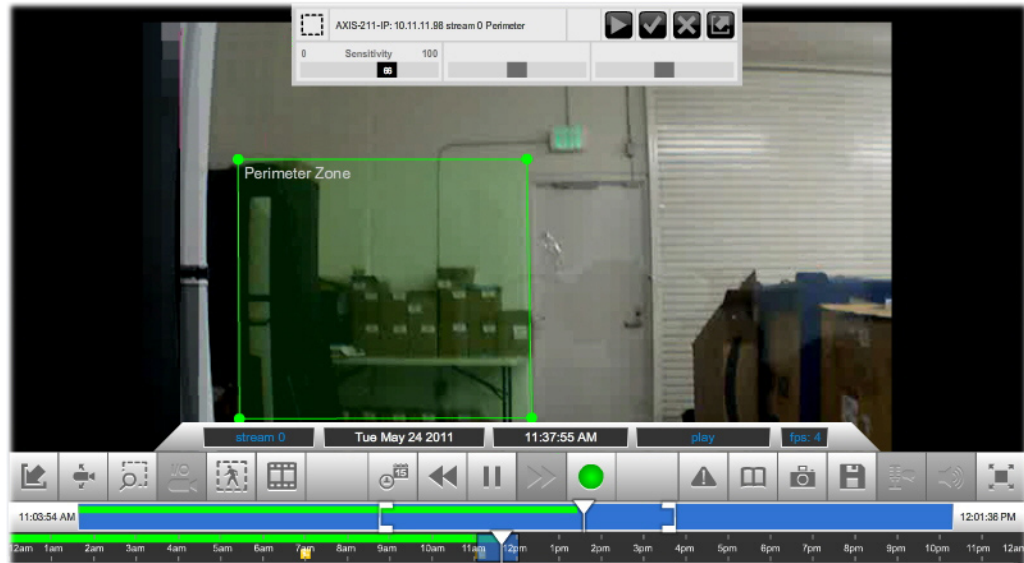
- Adjust the **Sensitivity** slider to set the threshold of this video analytic. Higher values make this video analytic more sensitive to the movement between the zones.
- Click the **Save** button to keep the changes.
- Click the **Start** button to activate this video analytic. If someone moves from one zone to the other in the designated direction, a video analytic event is generated.

4.2.3.6.10 Perimeter

The Perimeter video analytic functions similar to the Line Crossing analytic, but encompasses a four sides boundary. Any moving person or object that enters the Perimeter Zone from any direction is counted as an event.

- Click the **Edit** button for **Perimeter** in the Video Analytics Configuration list.
The video player is displayed with a highlighted area labeled *Perimeter Zone*.
- Click-hold-drag each rectangle to move it where you want monitor in the video stream.

- Click-hold-drag the corner points of the rectangle to resize and reshape it, so as to encompass the area to be monitored.



- Adjust the **Sensitivity** slider to set the threshold of this video analytic. Higher values increase the sensitivity.
- Click the **Save** button to keep the changes.
- Click the **Start** button to activate this video analytic. If a person or object crosses a perimeter zone boundary, a video analytic event is generated.

4.2.3.6.11 Troubleshooting Video Analytics

Video analytics are among the more challenging and subjective features to configure in the system.

This section lists some of the most common problems and solutions for setting up video analytics. These items are listed in a rough order for troubleshooting.

- Problem:** noisy scene, such as swaying trees, seeing errant bounding boxes in unexpected locations.

Solution: decrease the Sensitivity setting.
- Problem:** missing bounding boxes. Moving objects in scene to not have boxes around them and/or smaller objects are not identified.

Solution: increase the Sensitivity setting.

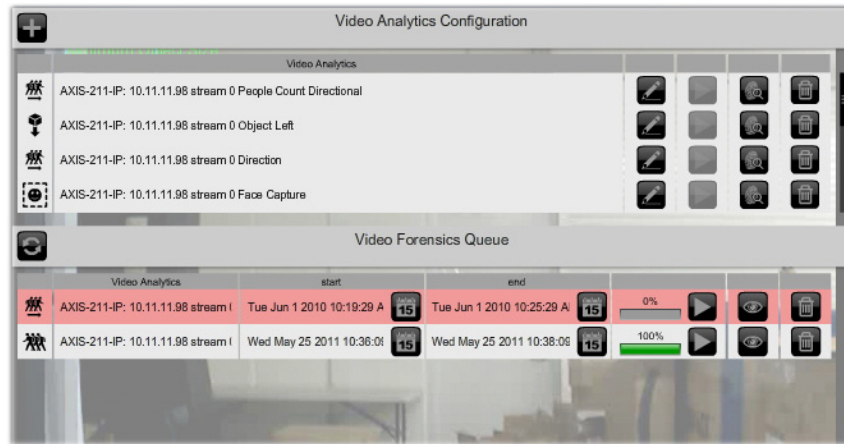
- **Problem:** People Count too high.
Solutions:
 - Make the camera angle as close to straight down as possible.
 - Reduce or eliminate changes to the lighting in the scene.
 - Make boxes smaller or farther apart.
 - Increase the Sensitivity setting.
- **Problem:** People Count too low.
Solutions:
 - Make the camera angle as close to straight down as possible.
 - Reduce or eliminate changes to the lighting in the scene.
 - Make boxes larger or closer together.
 - Increase the Sensitivity setting.

4.2.3.6.12 Video Forensics

Video Forensics allow analytics to be run on recorded video. Video Forensics are added to the *Video Forensics Queue* from the *Video Analytics Configuration* overlay.

1. Select the desired camera.
2. Click the **Analytics** button in the toolbar.
3. Click the **Add Video Analytics (+)** button at the top of the list to attach an analytic to a camera. The *Video Analytics* options pop-up menu is displayed.
4. Configure the analytic according to the instructions earlier in this section.
5. Click the **Forensics** button in the *Video Analytics Configuration* overlay. The analytic is added to the *Video Forensics Queue*.
6. Click the **start** and **end Calendar** buttons in the queue to set the time of the recorded video on which to run the forensic.
A dialog is displayed for each field. Click the arrow buttons to set the date and time. The selected date and time are displayed in the **start** and **end** fields.
7. Click the **Play** button.
 - A green bar indicates progress of the analytic. Click the **Refresh** button in the upper left corner of the queue to update the progress bar for a running forensic.
 - The line item in the queue turns pink if the analytic cannot run. For example, if a date or time was entered that has no recorded video.
 - An event is generated when the analytic detects an event for which it is looking.

- The result remains in the Video Forensics Queue until it is manually deleted. Click in the **Delete** button (trash can) to remove the result from the queue.

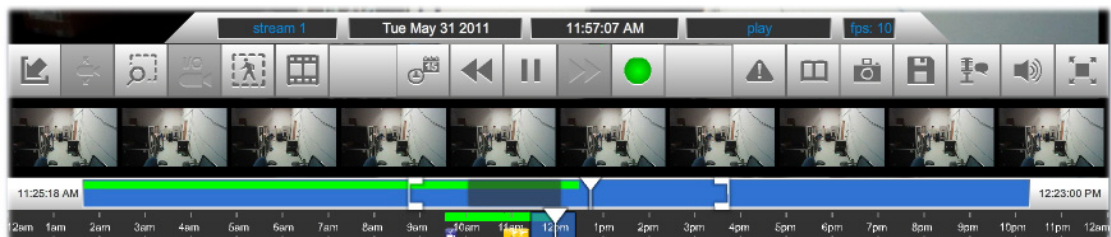


4.2.3.7 FILMSTRIP

A series of thumbnails of recorded events can be displayed from the timeline. Clips from the filmstrip can be played back in the video player.

1. Select the desired camera.
2. Click the **Filmstrip** button in the video player.

The filmstrip dialog is displayed. A semi-transparent bar highlights the recorded period on the timeline.



3. Click a clip to play it back. The Live/Recorded button turns red.
 - Click another clip to play it back, if desired.
4. Click the **Filmstrip** button to hide the dialog.
5. Click **Live/Recorded Toggle** button to return to live video.

4.2.3.8 DATE & TIME SELECTION

The Date & Time selection button is active only if the selected camera is configured to record, and the recordings are saved as far back in time as you are trying to access.

1. Click the **Date & Time** button.
The *Time & Date* dialog is displayed. The dates marked with *green* are the days on which recordings were made.
2. Click the desired date in the calendar.
3. Use the up and down arrows to select the time of the recorded video.
The **Time Sliders** in the toolbar update to reflect the new date and time, as does the playback in the video player.

Note: The timeline is updated only if the camera has been set to record, and recordings on the target date and time have been saved.

4. Use the playback controls to view the video.
5. Click the **Live/Recorded Toggle** to return to live video. The button turns green when live video is displayed.

4.2.3.9 REWIND AND FAST FORWARD

The Rewind and Fast Forward buttons are active only if the selected camera has been configured to record. You can rewind only as far back as recorded video has been saved.

1. Click the **Play/Pause** button in the toolbar to access recordings made from this camera.
2. In the toolbar, use the **Date & Time Selection** buttons and/ or the **Time Sliders** to select the day and time to rewind to.
3. Use the **Rewind** and **Fast Forward** buttons to fine tune the exact time of playback.

Note: Click the buttons repeatedly to cycle between 0.5x, 2x, 5x, and 10x speed.

4. Click the **Play/Pause** button at any time to start playback.

4.2.3.10 PLAY/PAUSE

The Play/Pause button is active only if the selected camera has been configured to record and a recording is currently playing in the video player. You cannot pause a live camera.

1. Display the desired camera in the video player, and use the **Live/Recorded Toggle** in the toolbar to play recordings made from this camera instead of the live view.
2. In the toolbar, select the time to start playback using the **Date & Time Selection** buttons and/ or the **Time Sliders**, as well as the **Rewind and Fast Forward** buttons.
3. Toggle the **Play/Pause** button to start and stop playback.

4.2.3.11 LIVE/RECORDED TOGGLE

The Live/Recorded toggle button is active only if the selected camera has been configured to record.

The Live/Recorded toggle turns green whenever the selected camera is playing a live stream in the video player. The button turns red when playing a recorded stream.

1. Display the desired camera in the video player.
2. In the Camera Toolbar, select the time to start playback by using the **Date & Time Selection** button and the **Time Sliders**, as well as **Rewind and Fast Forward**, or **Filmstrip** buttons.
3. To return to the live video stream, click the **Live/Recorded** toggle button.

4.2.3.12 CAMERA EVENTS TOGGLE

Event markers can be displayed or hidden in the timeline.

- Click the **Camera Events Toggle** to hide or display events markers.

4.2.3.13 EVENT BOOKMARK

A bookmark is a manually defined event.

1. To manually add an event to the timeline of the current camera, click the **Bookmark** button in the Camera Toolbar. A Bookmark event is added to the event lists for this camera, as well as the entire system.
2. Optionally in the **Camera Events** screen, open Event Notes for the Bookmark event that you just set, and enter notes about the event.

4.2.3.14 SNAPSHOT

A snapshot of a video clip can be grabbed via the toolbar. The video can be live or recorded.

1. Display the desired camera in the video player.
 - If you want an image of a recorded clip, navigate to the location in the timeline.
2. Click the **Snapshot** button in the toolbar.

A separate browser window is opened with the image. The image is in JPEG format. A *Magnifying Glass* tool is displayed with the image to allow you to zoom in and out.
3. Use the browser to save the picture in a location you desire.

4.2.3.15 SAVE A CLIP

A recording can be exported if the selected camera is configured to record and the target recording period has been saved.

1. Display the desired camera in the video player.
2. In the toolbar, select the date and time of the video to be exported:
 - To export a clip from a day other than today:
 - » Use the **Date & Time Selection** button to choose the date.
 - » Then use the **Time Sliders** to select the time range for export.
 - To export a clip recorded today, use the **1-Hour Slider**.
3. Click the **Save a Clip** button. A dialog appears confirming the date and time range to export.
4. In the Export dialog, click **Yes** to start the export, or **No** to cancel the export.
5. When the exported file has finished processing and is ready to save, another dialog appears for you to specify the location and file name of the exported file.

4.2.3.16 LOCAL MICROPHONE CONTROL

The NLSS Gateway supports full duplex audio. The toolbar contains a slider that controls the volume of your local microphone to the camera speaker.

1. Display the desired camera in the video player.
2. Click the **Microphone Control** button in the toolbar.
3. Drag the slider up and down to increase or decrease the local microphone's volume.

4.2.3.17 VOLUME / MUTE

The NLSS Gateway supports full duplex audio. The toolbar contains a slider that controls the volume of the camera microphone that is heard in the local speaker.

1. Display the desired camera in the video player.
2. Click the **Volume Control** button in the toolbar.
3. Drag the slider up and down to increase or decrease the camera's microphone volume.

4.2.3.18 FULL SCREEN TOGGLE

You can hide the menus and tab to enlarge the video player fill the browser screen.

- Click the **Full Screen** button to toggle between full screen and the menu view.

4.2.3.19 TIME SLIDERS

In the NLSS Web Interface, two time sliders are located at the bottom of the toolbar under the embedded video player: a [24-Hour Slider](#) and a [1-Hour Slider](#).

4.2.3.19.1 24-Hour Slider

The lower time slider shows the 24-hour period of the current day, or an earlier date if you are playing back a recording from a previous day.

The 24-hour slider includes:

- A **Detail Zone** is a blue box that can be moved with the mouse to select a specific hour. The time period you select determines the location of the [1-Hour Slider](#) in the top portion of the timeline. The brackets are not displayed unless the system contains recorded video for that camera.
- A **Time Bar** is a cursor that you can slide to an earlier hour on the 24-hour slider, causing the camera to play back a recording from that time.
- Small vertical markings at the times that events were recorded with this camera. The color of the markings indicates the type of event.

4.2.3.19.2 1-Hour Slider

The upper time slider shows the 1-hour period selected with the Detail Zone in the lower slider. The 1-Hour Slider is a more precise version of the timeline in the 24-hour slider.

- The exact start and end times of the 1-hour slider are displayed at either end of the slider.
- Drag the **Time Bar** to an earlier time to play back a recording from that time. This feature is only available if the camera is configured to record.
- Adjust the **Start** and **End** brackets (left and right) to set a time interval for saving a clip as a separate video file, in a standard format. For details, see [Save a Clip](#).

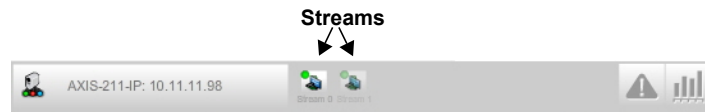
4.2.4 Additional Camera Controls

Additional controls for cameras appear above the embedded video player for the selected camera.

4.2.4.1 SELECT STREAM

Some cameras simultaneously output more than one stream. Each has a different codec and/or resolution. If a camera supports multiple streams, and the NLSS Web Interface is configured to handle more than one stream from that camera, then you can select which stream to view in the video player.

1. Select the desired camera from the **Cameras** menu.
Above the video player, buttons are displayed for the available camera streams. The streams are numerically labeled, such as *Stream 0*, *Stream 1*, etc.
2. Click the button of the desired stream to play it in the video player. A green dot is displayed on the button of the selected stream.



4.2.4.2 CAMERA EVENTS

Five types of events are associated with a selected camera:

- **Video Analytics** that are set up on this camera.
- **Event Bookmark** that are manually set up for this camera.
- The *operational status* reported by this camera, such as loss of signal.
- **Camera Motion**
- **Input Port**

You can display an *Event Log* related to this camera. See **Camera Event Log**. Also, buttons of events related to this camera appear within the **Time Sliders** under the video player, offering a quick method to **Playback Events**.

4.2.4.2.1 Camera Motion

Some cameras are designed to generate an event when motion is detected. The NLSS Gateway can accept this event from many cameras, and lists that event with other events. This event is configured within the camera, not in through the NLSS Web Interface.

4.2.4.2.2 Input Port

Some cameras contain an input port that generates an event when triggered. The NLSS Gateway can accept this event from many cameras, and lists that event with other events. This event is configured within the camera, not in through the NLSS Web Interface.

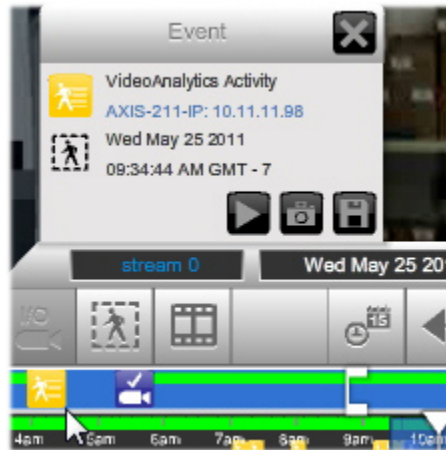
4.2.4.2.3 Viewing Events from the Timeline

Events are marked in the timeline for each camera.

To take a quick look at an event:

1. Place your cursor over the event marker in the timeline.

An *Event* dialog is displayed in the video player. This dialog can be dragged to other locations in the player screen. The dialog appears in the same location when accessed for subsequent events.



Note: If you click the event, the timeline cursor is placed at that location, and recorded video is played, as indicated by the red Play button in the timeline. Click the [Live/Recorded Toggle](#) button again to return to live video, as indicated when it turns green.

2. In the dialog:
 - Click the **Play** button to replay the event in the video player.
 - Click the **Snapshot** button to take a screen shot of the event. Pause the playback in the timeline to get the exact moment to be captured.
 - Click the **Save** button to save the event and prevent it from being groomed off (deleted) by the system. See [Configure Groomer Settings](#) for more information on grooming stored video.

The Event dialog can stay open while live video continues to play.

3. Click the **Close** button (X) to exit the dialog.

4.2.4.2.4 Camera Event Log

Events for a camera are collected in the Event Log.

1. Select a camera in the **Camera** menu.
2. Click the **Events** button above the video player.



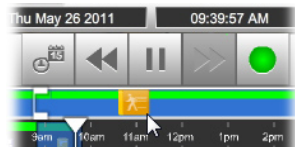
The *Events Log* for the selected camera replaces the Operations menu and the video player in the screen. Only the events for that camera are displayed. See [Event Log](#) for more information.

3. Open the appropriate tab for the event category, either **All Events**, **Shunted Events**, **Locked Events** or **Emergencies**.
4. Click the **Camera Event Type** button to configure the filter.
5. In the dialog box, uncheck the event types that you do not want in the list.
6. Click the **Close (X)** button to exit the dialog.
7. Click the desired event to display the details.

4.2.4.2.5 Playback Events

If the selected camera is set to record, then you can play back from the time of a camera event.

1. Select a camera in the **Cameras** menu.
2. In the 1-hour timeline of the Camera Toolbar, double-click the desired event marker. The video that triggered the event is played in the video player.



Note: If no event icons are displayed in the timeline, click the **Camera Events Toggle** in the toolbar to ensure that the icons are displayed.

4.2.4.3 CAMERA REPORTS

A graphical report can be generated for events related to a selected camera.

1. Select a camera from the **Cameras** menu.
2. Click the **Reports** button above the video player.
A *Reports* screen for the selected camera replaces the video player. The screen is blank until a report is generated.
3. Customize the report as desired. See [7.1 Generating Reports](#) for instructions on configuring reports.
 - Select a **Daily**, **Weekly**, or **Monthly** time period.
 - Use the *Date* dialog to select the day for Daily reports, or the last day in Weekly or Monthly reports.
 - Select **Column**, **Line** or **Pie** to set graph type.
4. Click the **Start** button to generate the report.

Note: To change the report, select the new parameter or type and click the **Start** button.

Chapter 5: Displaying Video

In the NLSS Web Interface, you can display video streams from IP cameras. You can even display multiple camera streams simultaneously using Views, and string together Views into Sequences.

The ability of the NLSS system to display video in a web browser is intended to aid investigations with video surveillance, but is not intended to provide constant long-term surveillance. Due to the complexities and shortcomings of various web browsers, NLSS cannot guarantee the performance, stability, or functionality of video displayed in a web browser. To display video continuously over long periods, we recommend adding one or more *NLSS HD IP Media Decoders* to your system.

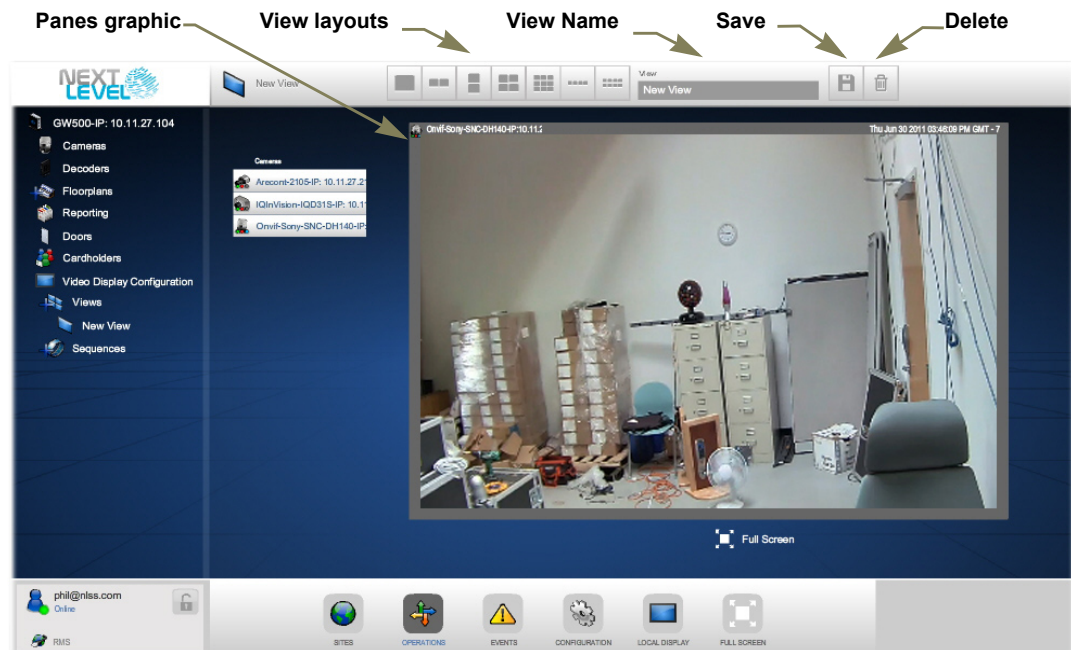
To support the continuous long-term display of video, the NLSS Web Interface features the ability to [Push Views and Sequences to Decoders](#) installed in your system, and thereby display video on HD monitors attached to those decoders.

For more information, see:

- [Create and Display Views](#)
- [Create and Display Sequences](#)
- [Push Views and Sequences to Decoders](#)

5.1 CREATE AND DISPLAY VIEWS

If you select a **View** in the **Operations > Video Display Configuration** menu, a screen is displayed with a list of cameras on the left and an embedded video player in the middle.



When you create a View Layout, a pane graphic appears in the video player to illustrate the layout. The initial layout uses a 1x1 pane (a single stream), but other View Layouts are available as well, such as 2x1 horizontal panes, 4x4 panes, and 3x3 panes. Initially, the NLSS logo plays in each pane.

Select any available video stream—from live cameras, RTSP, and HTTP—to place in the panes of this View Layout. A View provides simultaneous monitoring of up to nine cameras and other streams.

5.1.1 Views: Parameters

The Views screen contains the following parameters.

- **View Name:** give this View any name you wish.
- **View Layouts:** select a layout from the list of available layouts—single pane, 2x1 horizontal, 1x2 vertical, 2x2, 3x3, 1x4 vertical, and 2x4 vertical. The *Panes* display updates to show your selection.
- **Camera List:** all the cameras that have been discovered in your system are listed. You can assign any in-service camera to any pane in the layout.
- **Panes Graphic:** this graphic shows the video Panes in the View Layout you selected above. Using this graphic, you can assign specific camera streams to the Panes.
- **Save/Delete:** click the **Save** button to save the values of the parameters above, or the **Delete** button to abort.

5.1.2 Views: Actions

Select **Operations > Video Display Configuration** and click on the **Views** option. A list of existing Views is displayed. For instructions, see the sections below and the figure under [Create and Display Views](#).)

5.1.2.1 CREATE VIEWS

Here's how you create a new View:

1. In the Main Menu, navigate to the **Operations > Video Display Configuration**.
2. In the **Video Display Configuration** menu, click the **(+)** button next to **Views** to display a *New View* screen.
3. Click a **View Layout** to set the number of video panes in the new View. Your selection is reflected in a graphic presenting the panes in the selected layout.
4. In the *Panes* graphic, click a **pane** to select it.
5. In the Camera List to the left of the *Panes* graphic, select a camera to assign it to the pane.



Note: If a Pane already contains a camera, then assigning a new camera replaces the old camera assigned to that Pane.

6. Repeat the previous step for the rest of the panes in the layout.
7. In the **View Name** field, enter a name for the new View.
8. Click the **Save** button to add the new View to the list of existing Views.

5.1.2.2 EDIT VIEWS

An existing View can be edited.

1. In the Main Menu, select **Operations > Video Display Configuration > Views**.
2. Select view to display from the list of existing views in the Views menu.
3. In the *View* screen, update the View as needed.
The possible changes include:
 - Change the **View Name**.
 - Assign different cameras to one or more panes in the layout.
 - Select a different **View Layout**.
4. Click **Save** to keep the changes.

5.1.2.3 DELETE VIEWS

An existing View can be removed.

1. In the Main Menu, select **Operations > Video Display Configuration > Views**.
2. Select the view from the list of existing views in the Views menu.
3. In the *View* screen, click the **Delete** button.
 - Click **Yes** to confirm the deletion when prompted.

5.1.2.4 DISPLAY VIEWS

Two methods are available to display an existing View on the same monitor being used to access the NLSS Web Interface:

5.1.2.4.1 Method 1

Existing Views can be accessed from the Operations menu. This method does not allow you to view video in full size, because some screen space is used by configuration control.

1. From the Main Menu, select **Operations > Video Display Configuration > Views** to display a list of existing Views.
2. In the **Views** menu, click the name a View to display it.

5.1.2.4.2 Method 2

The **Local Display** menu is optimized for viewing video in the full window of your browser, without controls for configuration.

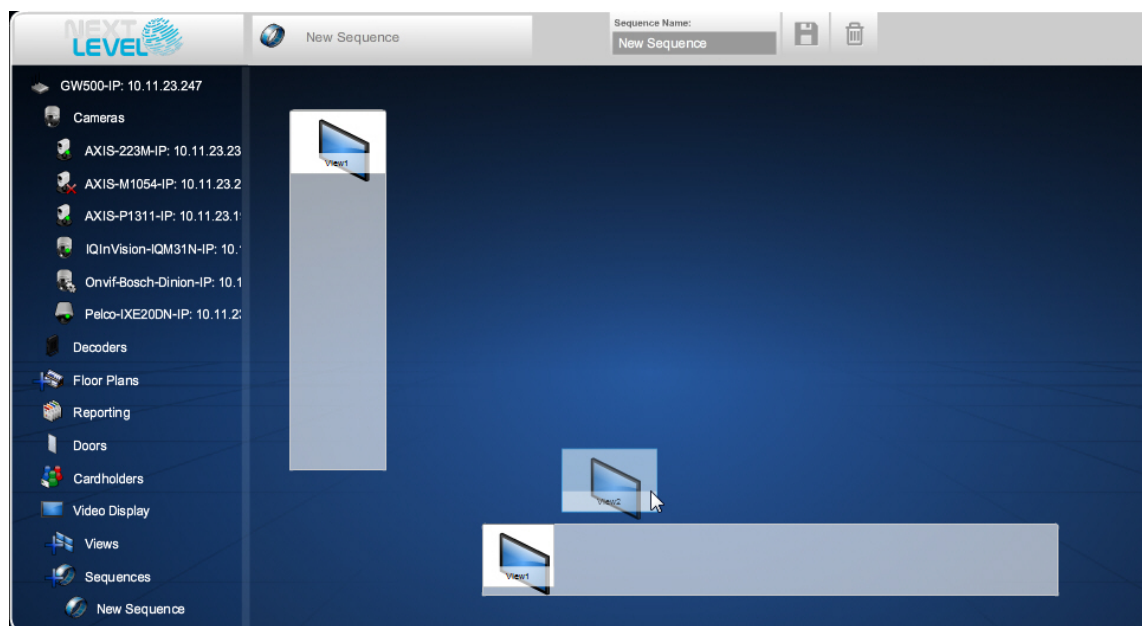
1. From the Main Menu, select **Local Display > Views** to list existing Views.
2. Select a View from the list to display it locally. After a few seconds, the icons for the Main Menu and View menu are hidden.
 - Click the **Toolbar** button to display the Main Menu.

5.1.2.5 ABOUT CAMERA PRESETS, PATROLS, AND VIDEO ANALYTICS

Presets, patrols, and video analytics that were assigned to individual cameras are preserved in Views and Sequences. For details, see [Chapter 4: Controlling Cameras](#).

5.2 CREATE AND DISPLAY SEQUENCES

If you select Sequences in the Operations > Video Display Configuration menu, a screen is displayed with a list of cameras on the left; an embedded video player in the middle, and an initially blank horizontal list under the video player.



5.2.1 Sequences: Parameters

The *Sequences* screen contains the following parameters:

- **Sequence Name:** Give the Sequence any name you wish.
- **Views:** all the Views in this vertical list (to the left of the video player) is available for use in Sequences. For usage, see the *Current Views in Sequence* parameter below.

Note: A View must already exist to be used in a Sequence.

- **Current Views in Sequence:** this is a horizontal list of the Views in the current Sequence. You can add, remove, and rearrange these Views, as follows:
 - To add an existing View to this Sequence, drag the desired View from the vertical list of Views on the left, to the horizontal *Current Views in Sequence* list under the video player.
 - To remove a View from the Sequence, drag that View out of the *Current Views in Sequence* list.
 - To change the order of Views in the *Current Views in Sequence* list, drag-and-drop the Views into the desired order.
 - To change the time that a View is displayed before switching to the next View in the Sequence, click on the View and enter the desired display time (in seconds) in the **Duration** field. Then click the **green check** to record the new duration, or the **red X** to retain the previous duration.
- **Save / Trash:** select the **Save** icon to save the values, or the **Trash** icon to abort.

5.2.2 Sequences: Actions

Sequences allow monitoring of two or more Views in a User configured order. Sequences can be created, edited, and displayed.

The video player and blank area under it initially are empty. You can define a Sequence by dragging Views into the blank area under the video player. Once two or more Views are added to the Sequence, use drag-and-drop to change their order.

5.2.2.1 CREATE NEW SEQUENCES

1. Select **Operations > Video Display Configuration** from the Main Menu.
2. In the Video Display Configuration menu, click the **+ (Add)** button next to **Sequences**. The *Add/Edit Sequence* screen is displayed.
3. In the Add/Edit Sequence screen, enter the parameters for the new Sequence, as described in [Sequences: Parameters](#).
4. Click **Save** to keep the settings.
 - Click the **Trash** button to clear the fields and not keep the settings.

5.2.2.2 DELETE SEQUENCES

1. Select **Operations > Video Display Configuration > Sequences** from the Main Menu.
2. In the **Sequences** menu, click a Sequence to display its *Add/Edit Sequence* screen.

3. In the *Add/Edit Sequence* screen, click the **Delete** (trash can) button to delete this Sequence.

5.2.2.3 EDIT A SEQUENCE

1. Select **Operations > Video Display Configuration > Sequences** from the Main Menu.
2. In the **Sequences** menu, click the Sequence to display its *Add/Edit Sequence* screen.
3. In the *Add/Edit Sequence* screen, edit the parameters of the Sequence, as described in [Sequences: Parameters](#).
4. Click the **Save** button to keep the changes.
 - Click the **Delete** button to cancel the changes.

5.2.2.4 DISPLAY SEQUENCES

Two methods are available to display a configured Sequence on the same local monitor that is displaying the NLSS Web Interface:

5.2.2.4.1 Method 1

Existing Sequences can be accessed from the Operations menu. This method does not allow you to view video in full size, because some screen space is used by configuration control.

1. Select **Operations > Video Display Configuration > Sequences** from the Main Menu.
2. Click the name of the desired Sequence to display it.

5.2.2.4.2 Method 2

The **Local Display** menu is optimized for viewing video in the full window of your browser, without controls for configuration.

1. Select **Local Display > Sequences** from the Main Menu. A list of existing sequences is displayed.
2. Click the desired Sequence to display it locally.

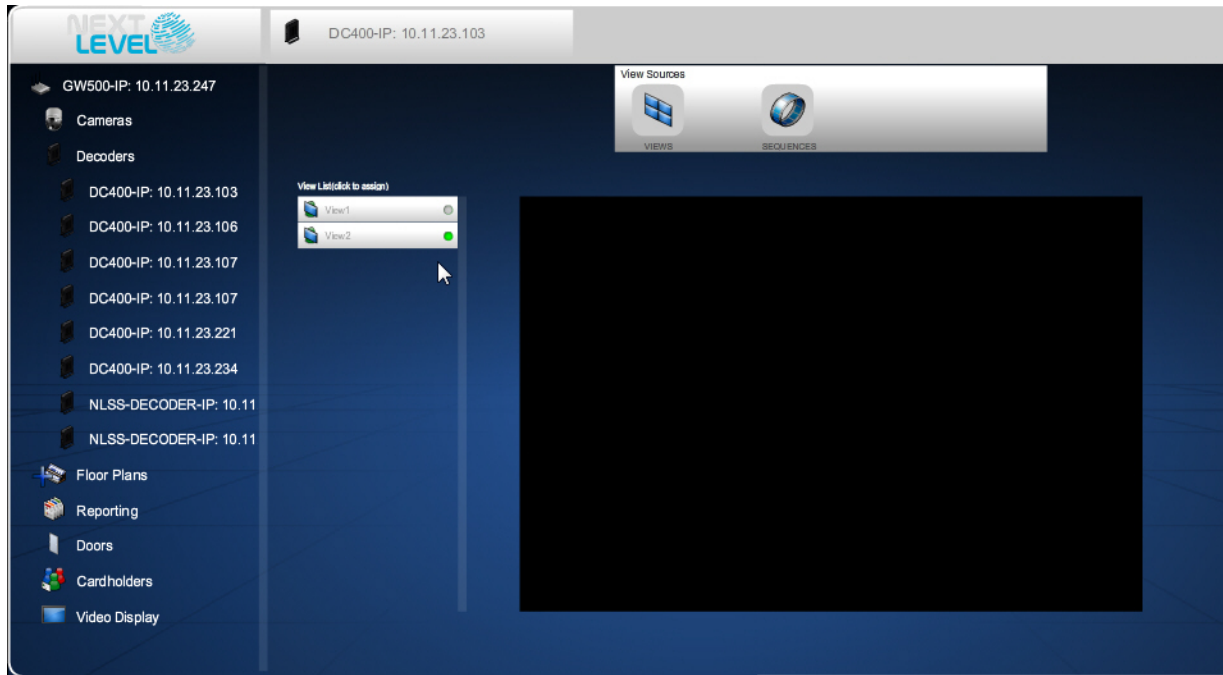
After a few seconds, the icons for the Main Menu and View menu are hidden.

- Click the **Toolbar** button to display the Main Menu.

5.3 PUSH VIEWS AND SEQUENCES TO DECODERS

When the NLSS Web Interface is logged into an NLSS Gateway, all the NLSS HD Media Decoders managed by that Gateway can be listed.

1. Select **Operations > Decoders** from the Main Menu.
2. Select a decoder under this menu to display the *Decoder Configuration* screen.



The Decoder Configuration screen contains three major elements.

- **View Sources:** select between Views and Sequences.
- **View / Sequence List:** Lists existing Views or Sequences, depending on the View Sources selection.
- **Embedded video player:** Displays the video streams in the current selection.

5.3.0.1 DISPLAY VIEWS VIA DECODERS

An existing View can be displayed on HD monitors driven by one or more NLSS HD Media Decoders installed in your system.

1. Select **Operations > Decoders** menu from the Main Menu.
2. In the Decoders menu, select the desired NLSS HD Media Decoder to display its configuration screen.
3. In the *Decoder Configuration* screen, select **Views** under View Sources. All existing Views are displayed in the View List.
4. In the View List, click one or more Views to push to the selected decoder.
 - Click a specific View again to stop pushing to the selected decoder.

5.3.0.2 DISPLAY SEQUENCES VIA DECODERS

You can optionally display an existing Sequence on HD monitors driven by one or more NLSS HD Media Decoders installed in your system.

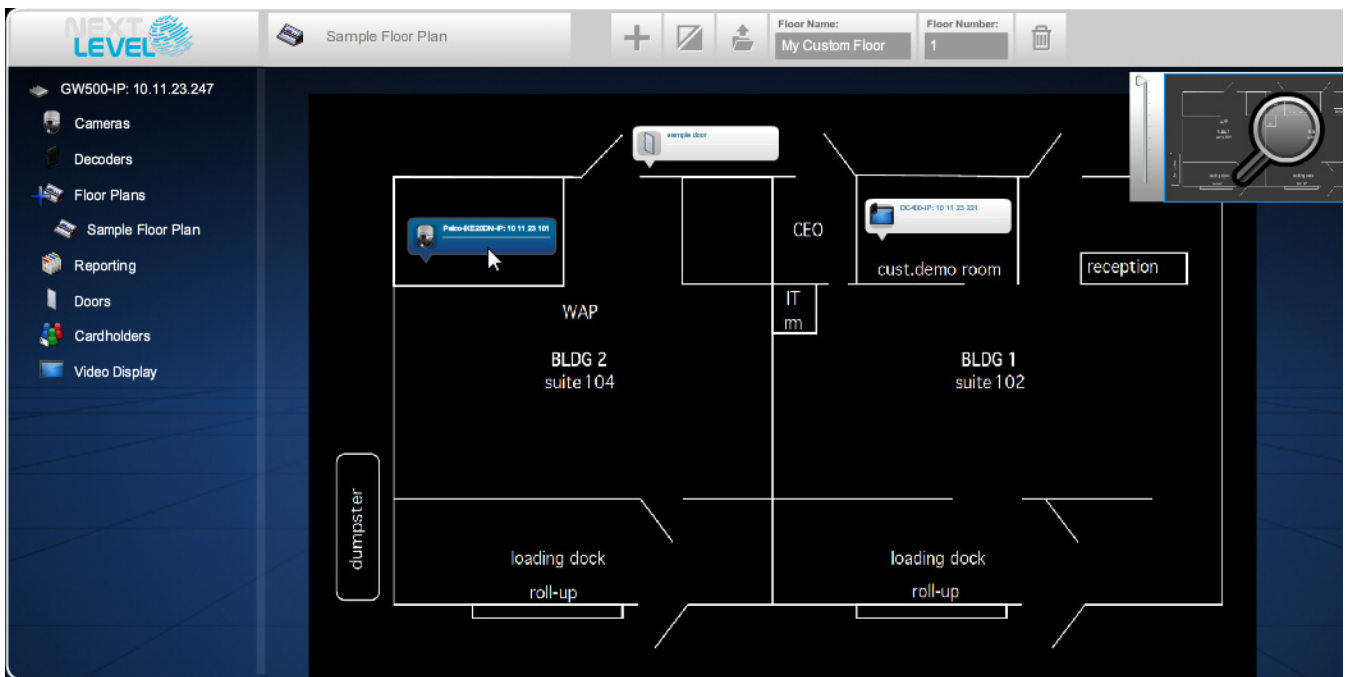
1. Select **Operations > Decoders** from the Main Menu.
2. In the Decoders menu, select the desired NLSS HD Media Decoder to display its configuration screen.
3. In the *Decoder Configuration* screen, select **Sequences** under View Sources. All existing Sequences are displayed in the Sequence List.
4. In the Sequence List, click one or more Sequences to push to then to the selected decoder.
 - Click a specific Sequence stop pushing it to the selected decoder.

Chapter 6: Using Floor Plans

A Floor Plan is a map of a building or location, with icons placed on top. The icons represent the NLSS HD Media Decoders, cameras, and doors in your NLSS Unified Security Platform. The icons are manually placed on the map to match the physical locations of the devices.

6.1 CREATE FLOOR PLANS

To create a new floor plan, a map is uploaded, such as a JPEG version of a simplified architectural diagram. The device icons are then placed on the map. The system automatically saves the changes as they are made.



6.1.1 Create New Floor Plans

1. Select **Operations** from the Main Menu.
2. In the Operations menu, click the **plus (+)** next to the **Floor Plans** option.
 - A new floor plan is created in the pane to the right, and the *Floor Plan* screen is displayed.
3. Configure the new floor plan as described in [Configure Floor Plans](#).

6.1.2 Configure Floor Plans

New floor plans are configured, and existing floor plans are edited, in the Floor plans screen.

1. Select a floor plan under the **Floor Plan** menu, if a floor plan is not open.
2. Enter a name in the **Floor Name** field.
3. Enter the number of the floor in the **Floor Number** field, such as 1 for the first floor, 2 for the second floor, etc.
4. Click the **Upload Map** button to display a file browser.
5. Locate and upload a JPEG of the map.

Note: When preparing this map in separate software, keep the file size small for optimal performance.

6. Click the **Add** button to display Decoder, Camera and Door buttons.
 - **Decoder:** click this button to display a list of NLSS HD Media Decoders in the system. Then click the desired decoder in the list to place it on the map.
 - **Camera:** click this button to display a list of IP cameras in the system. Then click the desired camera in the list to place it on the map.

Note: If you change the name of this camera in the **Configuration > Video > Cameras** menu, then you must delete the camera from the floor plan, and then re-add the camera to the same floor plan.

- **Door:** click this button to display a list of doors in the system. Then click the desired door in the list to place it on the map.
7. After icons for all the devices on the floor have been added to the floor plan, arrange their icons on the map as follows:
 - a. Toggle the **Arrange** button to enter the *Arrange Mode*. Use the mouse to drag device icons to their proper locations on the map.

Note: You can remove a device from the floor plan by dragging its icon to the trash bin, while in the Arrange Mode.

- b. When finished, toggle the **Arrange** button again to exit Arrange Mode.

6.2 USE FLOOR PLANS

Using the *Floor Plan* screen, a user can:

- [Navigate Floor Plans](#)
- [Select Devices in Floor Plans](#)
- [Monitor Events on the Floor](#)

6.2.1 Navigate Floor Plans

Use the Magnifying Glass tool to zoom in on a floor plan.

1. Move the zoom slider up and down to zoom in and zoom out in the map.
2. Drag the **Magnifying Glass** over the small display of the map display to take a closer look at a particular area.

6.2.2 Select and Edit Floor Plans

1. Select **Operations > Floor Plans** from the Main Menu. A list of floor plans is displayed in the menu.
2. Click the desired floor plan. The *Floor Plan* screen is displayed with details on the selected floor plan.
3. To edit the selected floor plan, change anything about it, as described in [Configure Floor Plans](#). The system automatically saves your changes.

6.2.3 Select Devices in Floor Plans

Click the icon of a device in a floor plan to access the operational controls for that device.

6.2.3.1 SELECT A DECODER

In a floor plan, click the icon of an installed NLSS HD Media Decoder to display the active View or Sequence playing on this decoder.

The system also lists other Views and Sequences that have been pushed to this decoder. If no Views or Sequences have been pushed this particular decoder, then the screen displays a blank view. For details on Views and Sequences pushed to decoders, see [Displaying Video](#).

6.2.3.2 SELECT A CAMERA

In a floor plan, click the icon of an installed IP camera or other video stream to display the current stream in the embedded video player.

For details on controlling cameras, see [Chapter 4: Controlling Cameras](#).

6.2.3.3 SELECT A DOOR

In a floor plan, click a door icon to display the *Door Operations* screen for that door.

For details on Door Operations, see [Chapter 8: Operations with Doors](#).

6.2.4 Monitor Events on the Floor

While viewing a specific floor plan under the Operations > Floor Plans menu, events that take place within that floor plan automatically pop up in real-time.

- Click an event to view details on that event, and potentially access associated cameras, doors or decoders.

6.2.5 Deleting a Floor Plan

A floor plan can be deleted.

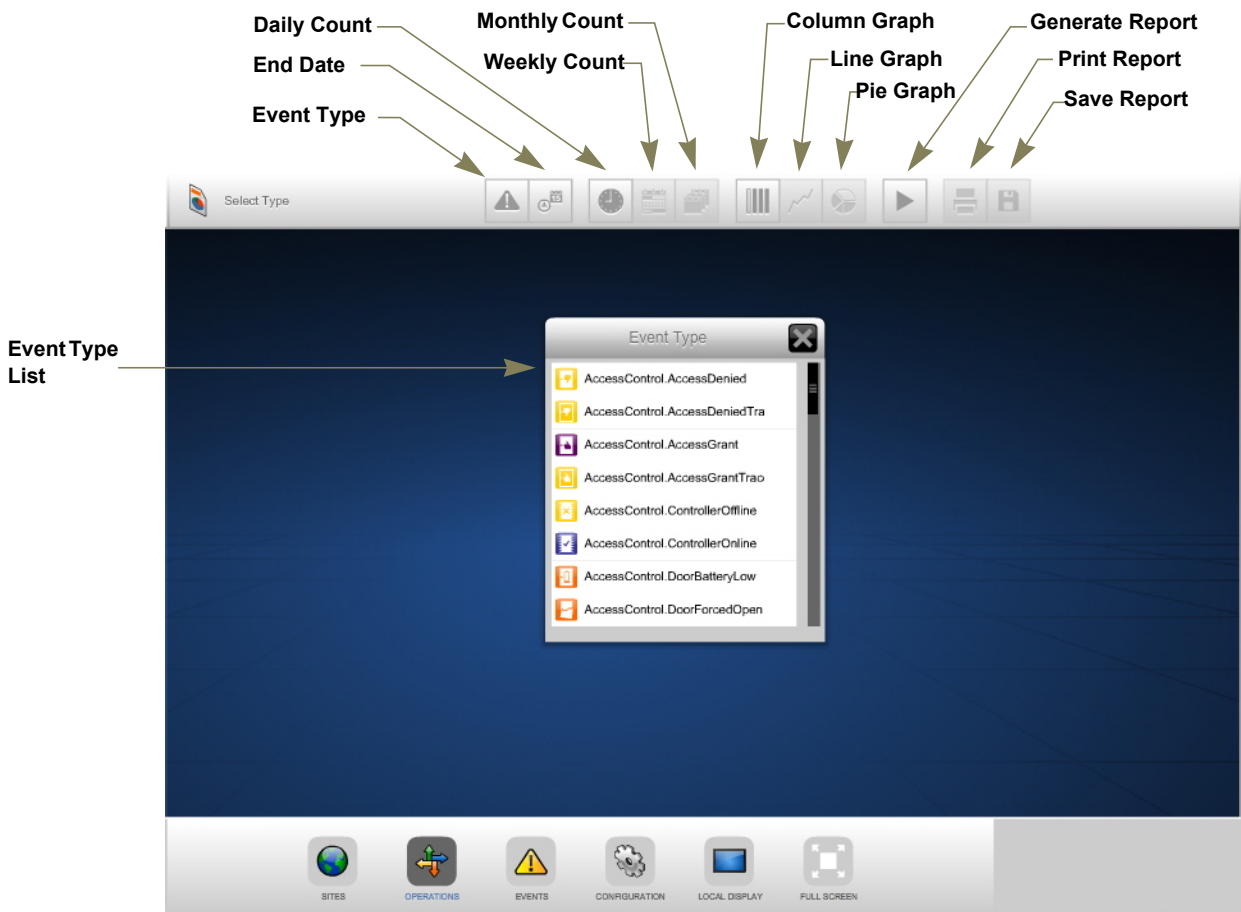
1. Select **Operations > Floor Plans** from the Main Menu. A list of floor plans is displayed in the menu.
2. Click the desired floor plan. The *Floor Plan* screen is displayed with details on the selected floor plan.
3. Click the **Delete** button (trash can).
4. Click **Yes** when prompted to confirm the deletion.
 - Click **No** to cancel the deletion and keep the floor plan.

Chapter 7: Operations with Reports

Reports collect specific information about events being tracked by the NLSS Unified Security Suite. The information collected depends on the type of report, the date/time range selected, and other filters (such as reports on individual cameras and doors).

7.1 GENERATING REPORTS

Systemic Reports address all instances of an event type throughout the entire system. **Device-Specific Reports** do the same for an individual device in the system.



7.1.1 Systemic Reports

In the Operations > Reporting menu, reports are generated for events tracked across the entire system.

1. Select **Operations > Reporting** from the Main Menu.

The *Event Type* list is displayed.

Note: The **Event Type** button can be clicked at any time to open the list to select a different report topic.

2. Select an Event Type from the list. The system generates the report the parameters for the report are configured.

- For example, if the *Door - Door Forced Open* report is selected, a report summarizes all the doors throughout the system that have been forced open within the specified time interval.

3. Click the **End Date** button.

Use the arrows to select the last day that the records are searched, according to the time period selected in the next step. The report includes all of the events prior to the end of the day, or to the time of the search if today is selected as the end date.

4. Select a time period for the report.

- **Daily:** Graphs the matching events, in hourly increments, for the 24 hours of the date selected. If today is selected, the report includes all matching events from midnight up to the time of the report.
- **Weekly:** Graphs the matching events, in one day increments, for that date and the seven days prior to the end date.
- **Monthly:** Graphs the matching events, in monthly increments, for the year prior to the end date.

5. Select a graph type for the report: **Column**, **Line**, or **Pie**.

6. Click the **Generate Report** button to create the report.

- Click **Print** to print the report.
- Click **Save** to keep a .csv version of the report.

7.1.2 Device-Specific Reports

The Operations > Reporting menu generates reports for your entire system, not individual devices.

To generate reports of events related to individual doors, cameras or cardholders, select that device and run a report.

- **For cameras:** see instructions in [Camera Reports](#).
- **For Doors:** see instructions in [Generate Reports for Individual Doors](#).
- **For Cardholders:** see instructions in [Generate Reports for this Cardholder](#)

7.2 CATEGORIES OF SYSTEMIC REPORTS

Several categories of systemic events reports are available in the Operations > Reports menu.

7.2.1 Access Control Reports

Access Control reports provide the status of key access control hardware in your system.

7.2.2 Camera Reports

Camera reports provide the count for events related to cameras in your system.

For example, the *Camera - Motion Event* report counts the motion events recorded by the cameras in the system.

7.2.3 Cardholder Reports

Cardholder reports list which Cardholders opened, or attempted to open, doors in the system.

7.2.4 Door Reports

Door reports provides the count for events related to the doors in your system.

For example, the *Door - Door Forced Open* report counts the number of times a door in the system was forced open.

7.2.5 User Reports

User reports lists when specific Users have logged in or out of the system.

7.2.6 Video Analytics Reports

Video Analytics reports list how many times the cameras in the system have detected a video analytic event.

For example, the *Video Analytics - People Count* report lists how many people have been detected by the cameras in your system.

Chapter 8: Operations with Doors

Configured doors are listed under the Operations > Doors menu. Operators can take the following actions with these doors:

- [Momentarily Unlock a Door](#)
- [Associate Cameras and Doors](#)
- [Open Camera Audio for an Associated Door](#)
- [List Events for Individual Doors](#)
- [Generate Reports for Individual Doors](#)

8.1 MOMENTARILY UNLOCK A DOOR

If a locked door needs to be unlocked outside its scheduled time, Operators can manually send a momentary unlock command to the door.

1. Select **Operations > Doors** from the Main Menu.
2. Select a door from the list under the **Doors** menu.
The *Door Operations* screen appears in the right pane.
3. In the Door Operations screen, click the **Open** button to unlock the door for its configured *strike time*.

The person requesting entry must physically open the door during the strike time, or the door re-locks.

8.2 ASSOCIATE CAMERAS AND DOORS

A camera can be associated with a specific door. The camera's stream then can be viewed directly from the Doors menu.

The association of cameras and doors also can be broken.

The most common reason to associate a door with a nearby camera is to provide a visual record of activity (authorized or not) through that door.

8.2.1 Associate Cameras with Doors

Initially, doors in the system do not have cameras associated with them.

1. Select **Operations > Doors** from the Main Menu.
A list of doors is displayed in the menu.
2. Select the desired door from the list under the Doors menu.
The *Door Operations* screen is displayed.
3. Click the **Add Camera** button to display a list of available cameras in the *Door Operations* screen.
4. Click on a camera to select it.

8.2.2 Disassociate Cameras from Doors

The association between a camera and a door can be removed.

1. Select **Operations > Doors** from the Main Menu.
A list of doors is displayed in the menu.
2. Select the desired door from the list under the Doors menu.
The *Door Operations* screen is displayed.
3. Click the **Delete Camera** button to disassociate the camera from the selected door.

8.2.3 Display Camera Streams Associated with Doors

After a camera is associated with a door, its stream can be viewed via the Doors menu.

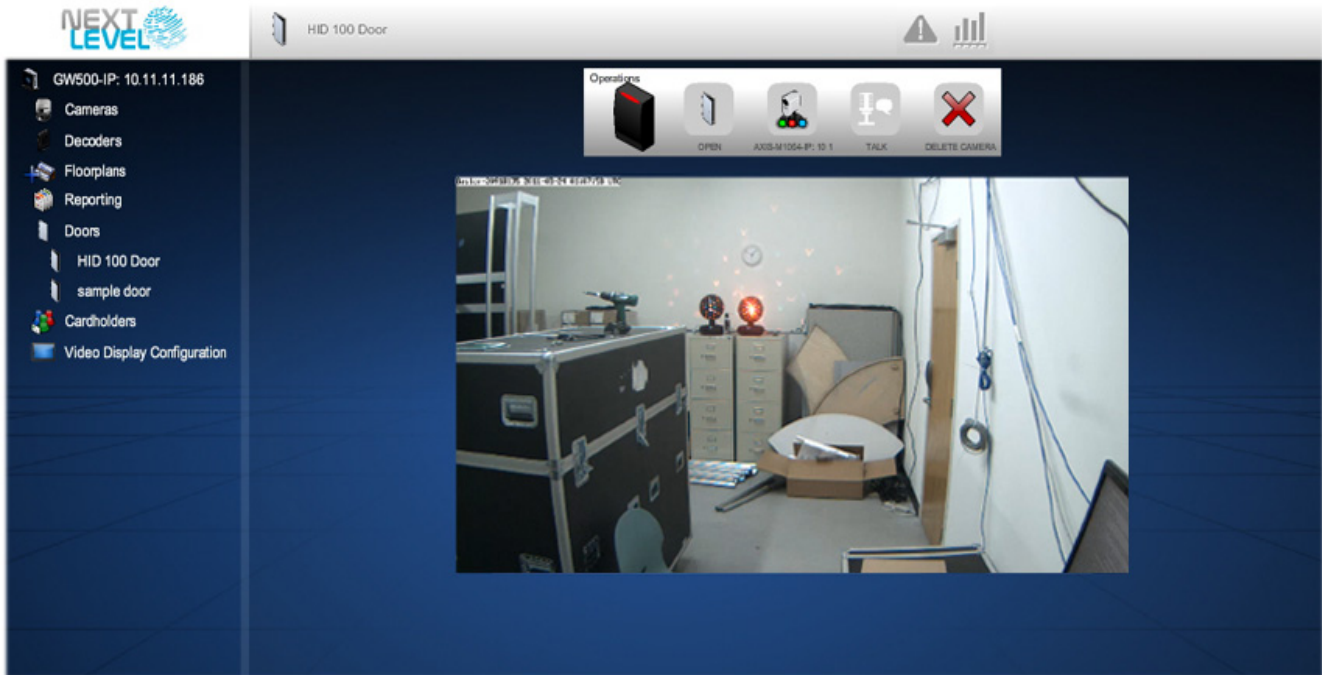
1. Select **Operations > Doors** from the Main Menu.
A list of doors is displayed in the menu.
2. Select a door from the list.
The *Door Operations* pane is displayed with a video feed from the camera.
3. To view the video player for the camera, click the button for the camera associated with this door.
This icon is located next to the Open button.
4. The video player displays the live video stream from the selected camera.

8.3 OPEN CAMERA AUDIO FOR AN ASSOCIATED DOOR

An operator can communicate via the camera speaker and microphone if a camera supports audio. A two way audio control—**Talk** button—is displayed in the Door Operations menu.

Note: An internal or external microphone and a speaker must be enabled for the computer on which the browser is running. See the instructions for the operating system or the audio program through which the microphone is connected to the computer.

1. Select **Operations > Doors** from the Main Menu.
A list of doors is displayed in the menu.
2. Select a door from the list.
The *Door Operations* pane is displayed with a video feed from the associated camera.
3. Click the **Talk** button to speak.



8.4 LIST EVENTS FOR INDIVIDUAL DOORS

An event is logged a when a Cardholder attempts to open a door in the system: generally *Access Granted* or *Access Denied*. A log of events for an individual door can be generated over a particular time period.

1. Select **Operations > Doors** from the Main Menu.
A list of doors is displayed in the menu.
2. Select the desired door from the list.
The *Door Operations* screen is displayed.
3. Click the **Events** button on the top menu bar to display Event Log for the selected door.
Only the events for that door are listed.
4. Use the **Start** and **End** fields to select the date and time range for populating the table of events.
 - a. Set the start date and time by clicking on the up and down arrows for the year, month, date, hour, minute and a.m. or p.m.
 - b. Repeat the procedure to set the end time of the range.
 - c. Click the **Search** (check mark) button to display the events in that range.
5. Sort the resulting Event Log by column. Click on a row in the log to see its Event Tag details on that event.

For further information on Event Logs, which behave similarly for systemic events as well as individual door events, see [Monitoring and Handling Events](#).

8.5 GENERATE REPORTS FOR INDIVIDUAL DOORS

Various reports related to all the doors in the system can be generated from the **Operations > Reports** menu.

A report for an individual door is done from the *Door Operations* screen.

You can generate a report on an individual door, as follows:

1. Select **Operations > Doors** from the Main Menu.
A list of doors is displayed in the menu.
2. Select the desired door from the list.
The *Door Operations* screen is displayed.
3. Click the **Reports** button. A *Reports* screen for the selected door replaces the video player. The screen is blank until a report is generated.
4. Customize the report as desired. See [7.1 Generating Reports](#) for instructions on configuring reports.
 - Select a **Daily**, **Weekly**, or **Monthly** time period.
 - Use the *Date* dialog to select the day for Daily reports, or the last day in Weekly or Monthly reports.
 - Select **Column**, **Line** or **Pie** to set graph type.
5. Click the **Start** button to generate the report.
6. To change the report, select the new parameter and click the **Start** button.

Chapter 9: Operations with Cardholders

When the **Operations > Cardholders** menu is selected, a list of configured Cardholders is displayed. Select a Cardholder from the list to display the *Cardholder Operations* screen for that individual.

The Cardholder screen is displayed with a list of Access Cards that have been assigned to him or her. This display is called the *Cards* view.

If one of the access cards is selected, the Persons view is displayed from which an access card can be *Enabled* or *Disabled*.

Note: Only *one* access card can be active per cardholder.

9.1 ACTIONS WITH CARDHOLDERS

Records for a selected Cardholder are displayed in the right pane.

- [Information on the Cardholder](#)
- [Photo of this Cardholder](#)
- [Activate / Deactivate Cards](#)
- [List Events for this Cardholder](#)
- [Generate Reports for this Cardholder](#)



9.1.1 Information on the Cardholder

The configured name, Employee number, Title, Location, and Supervisor of the selected Cardholder appears in the *Cards* view.

9.1.2 Photo of this Cardholder

If a photo was uploaded for the Cardholder (see [Cardholders: Credentials Tab](#)), the photo is displayed in the Cardholders screen.

9.1.3 Activate / Deactivate Cards

After clicking on a button to select a specific access card, click button in the lower right corner to **Activate** or **Deactivate** that card.

- If the selected card is currently active, clicking its Card List in the Cardholder screen displays the **Deactivate Card (X)** option. Select this option to disable the card.
- If the selected card is currently inactive, clicking its Card List in the Cardholder screen displays the **Activate Card** option. Click this option to enable the card.

Note: Only one (1) access card can be active per Cardholder.

9.1.4 List Events for this Cardholder

When a Cardholder attempts to access a door controlled by the NLSS Unified Security Platform, an event is logged, generally *Access Granted* or *Access Denied*. For a specific Cardholder, a log of all such events can be generated for a given time period.

1. Select **Operations > Cardholders** from the Main Menu.
A list of Cardholders is displayed in the menu.
2. Select a Cardholder from the list.
The *Cardholder Operations* screen is displayed.
3. Click the **Events** button to display the Event Log for this Cardholder.
4. Use the **Start** and **End** fields to select the date and time range for populating the table of events.
 - a. Set the start date and time by clicking on the up and down arrows for the year, month, date, hour, minute, and a.m. or p.m.
 - b. Repeat the procedure to set the end time of the range.
 - c. Click the **Search** (check mark) button to display the events in that range.
5. Sort the resulting Event Log by column. Click on a row in the log to see its Event Tag details on that event.

See [Chapter 10: Monitoring and Handling Events](#) for more information.

9.1.5 Generate Reports for this Cardholder

Various reports related to all Cardholders in the system can be generated from the **Operations > Reports** menu, and directly from the Cardholders screen.

A report for an individual Cardholder is done from the *Cardholder Operations* screen.

1. Select **Operations > Cardholders** from the Main Menu.
A list of Cardholders is displayed in the menu.
2. Select the desired Cardholder from the list, and the specific individual access card on which to the report run.
The *Cardholder Operations* screen is displayed.
3. Click the **Reports** button. A *Reports* screen for the selected Cardholder is displayed. The screen is blank until a report is generated.
4. Customize the report as desired. See [7.1 Generating Reports](#) for instructions on configuring reports.
 - Select a **Daily, Weekly, or Monthly** time period.
 - Use the *Date* dialog to select the day for Daily reports, or the last day in Weekly or Monthly reports.
 - Select **Column, Line** or **Pie** to set graph type.
5. Click the **Start** (check mark) button to generate the report.
6. To change the report, select the new parameter and click the **Start** button.

Chapter 10: Monitoring and Handling Events

Through the Events menu, incidents can be track and handled, and occurrences detected by an NLSS Gateway.

10.1 MONITORING EVENTS

From the Main Menu, the Events menu displays events in real-time, as well as providing a log of recent events. The events list can be filtered and customized by date and time, device type and severity.

In the NLSS Web Interface, when Events is selected in the Main Menu at the bottom of screen, the system lists events in either a [Realtime View](#) or an [Event Log](#).

- Click the **Events** button in the Main Menu.



By default, the [Realtime View](#) is displayed the first time the button is clicked in the current session. Viewing events in an Event Log view is available by selecting the **Event Log** button in the upper menu bar of the *Realtime View*.

Both views provide details about events, and the option to take action on the event. Those actions include acknowledging the event, masking run away events, locking the event, and adding notes on actions taken.

Note: The Events button in the video player only accesses the Events Log for the selected camera or video stream.

Important: If the Events button is pulsating, an Emergency event has been generated. See [Emergency Events](#) for instructions.

10.1.1 Realtime View

The *Realtime View* provides an Event Stream that displays events as they happen.



- If Events opens in the *Events Log*, click the **Realtime View** link at the top of the main Events menu screen.
 - The event markers in the stream are the most recent events. The events listed to the left are the event markers that have scrolled off of the event stream.
 - Click an event marker to display **Event Details**. You can take action and view the particulars of an event in the **Event Details** pane.
 - Move the slider up on the right of the pane to increase the speed of the event stream. Move the slider down to decrease the speed.
 - The buttons above the Realtime View list the event categories, and provide the option to filter out a category from this view.
By default, all event types are included in the event stream.
 - Click the button to filter out that event category from the Realtime View.
For example, click the Informational button to prevent Informational events from being included in the event stream.
The dark gray button becomes faded when that event type is being filtered out of the event stream.
The solid colors do not fade for the event level buttons, such as the red Emergency button. Only the gray highlight around the button becomes faded.
 - Click the button again to include the event category in the Realtime View.
- Note:** The past events of the filtered category still are displayed in the list on the left. These filters do not impact the Event Log.
- Click an event marker in the event stream or in the list on the left to display the **Event Details** dialog for more information.

10.1.2 Event Log

The *Event Log* lists events over a specified time period. The Event Log also provides more granular filtering than the RealTime View. You can access **Event Details** from the Event Log List to take action and view the particulars of an event.

10.1.2.1 EVENT LOG LIST

The Event Log List provides high level information on events.





- Click the **Event Log** link at the top of RealTime View. Each row in the Event Log lists a single event tracked by the system.

Note: If the list is empty when first accessed, and events are recorded in the Realtime View, check the START and END times. *Do not* use the browser's refresh button, as that returns you to the login screen.



10.1.2.1.1 Event Log Queues

The Event Log contains four queues, accessible through the tabs.

-  **Event:** lists all events.
-  **Shunted:** lists events that are generated with no notices issued for those events. This flag is setting is enabled in the **Event Details** dialog. See **Shunt Toggle**.
-  **Lock State:** lists events that are flagged as locked, meaning the event cannot be groomed. This flag is setting is enabled in the **Event Details** dialog. See **Lock State Toggle**.
-  **Emergency:** lists events with an emergency status. See **Emergency Events**.

10.1.2.1.2 Date & Time Range

The Event Log list can be filtered to display only events within a specified time period.

Use the **START** and **END** fields to select the date and time range for populating the Event Log.

1. Set the start date and time by clicking on the up and down arrows for the year, month, date, hour, minute, and a.m. or p.m.
2. Repeat the procedure to set the end time of the range.
3. Click the **Search** button to display the events in that range.

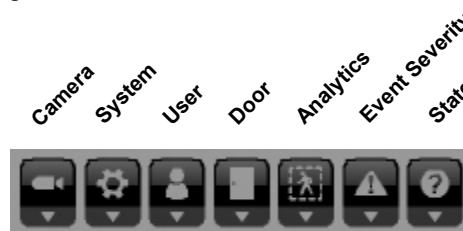
The events that occurred within that range are displayed.

10.1.2.1.3 Event Filters

The Event Log List can be filtered to display only specific event types. Filtering can be done on a high level to filter out entire categories, such as cameras, or to filter out specific events, such as camera informational events.

All categories and event types are allowed by default. An event category is filtered out of the list when it is deselected.

Use the buttons to the right of the START and END fields to set the filters.



An entire event category can be filtered out of the list by clicking the corresponding button. The button is grayed out when selected to filter out that category.

The filter can be set to a more granular level by selecting individual event types from a drop-down list.

1. Click the down arrow under the category button. A dialog box lists the event types of the event category. The dialog box cannot be displayed if the button is deselected.
2. Check the items to be allowed. Only events matching the checked items now are displayed in the list. The other items are filtered out.
 - Click the **All** button to select all event types in the dialog and allow them in the Event Log list.
 - Click the **None** button to deselect all event types and filter them out of the Event Log list.
3. Click the **Close (X)** button to exit the dialog.
4. Click the **Search** button to display the events matching the filter.

Note: Filtering an event type out of the Event Log does not prevent the Gateway from collecting that data and storing the event. The filter is applied across all event queues. When the filter is reset to allow that event type, all matching events that were previously filtered out now are displayed.

10.1.2.1.4 Event List

The Event Log provides high level information on each event.

- **Event Date** and **Event Time**: the date and time the event took place.
- **Event Source**: the device, User, Cardholder, or other system resource that triggered this event.
- **Event Type**: a subset of the Event Category.


For example, when a Cardholder opens a monitored door, the system records the event type as *access granted* under the *Cardholder* category.

If a User uses the NLSS Web Interface to open the same door for someone, the system records the event type as *User Door Opened* under the *User* category.

The event type's severity level is indicated by the color of the icon. The event type severity levels are set under Global settings in the Configuration menu. See [Configure Event Severity](#).

- **Event Category**: the categories of events include Access Control, Camera, Cardholder, Door, User, and Video Analytics. These icons are the same as used for the filter buttons. See [Event Filters](#).
- **Current State**: indicates whether the event is:

 Open

 Needs Acknowledgment: if an event requires acknowledgement, it first appears in the Open state, but the icon is red, not orange.

 Acknowledged

 Closed

If an event requires acknowledgement, it first appears in the Open state, but the icon will be red, not orange.

- **Lock Status**: indicates whether this event has been locked to prevent grooming. Grooming occurs when the database deletes the oldest events to make room for newer events.
 - An *open* lock indicates that the event is not locked and can be groomed.
 - A *closed* lock indicates the item is locked and cannot be groomed. The event can be locked in the [Event Details](#) dialog. See [Lock State Toggle](#).

10.1.2.1.5 List Actions

The Event Log List also contains a series of buttons to run additional actions on the list.





Pause/Play: toggles between displaying a live list and pausing the list so new events are not displayed. Click **Pause** to temporarily stop the display of new events. Click **Play** to resume the live list display.



Search: triggers any update of the Event Log list. If a value is entered in the adjoining field, Search only checks the Event Source field for the value, and displays only the events that match that criteria.



List and Grid Views: selects the display layout of the list.

-  **Save:** exports the current Event Log list to a .csv file.
-  **Print:** takes a screen shot of the Event Log List and sends to a printer. Landscape mode is recommended for printing.

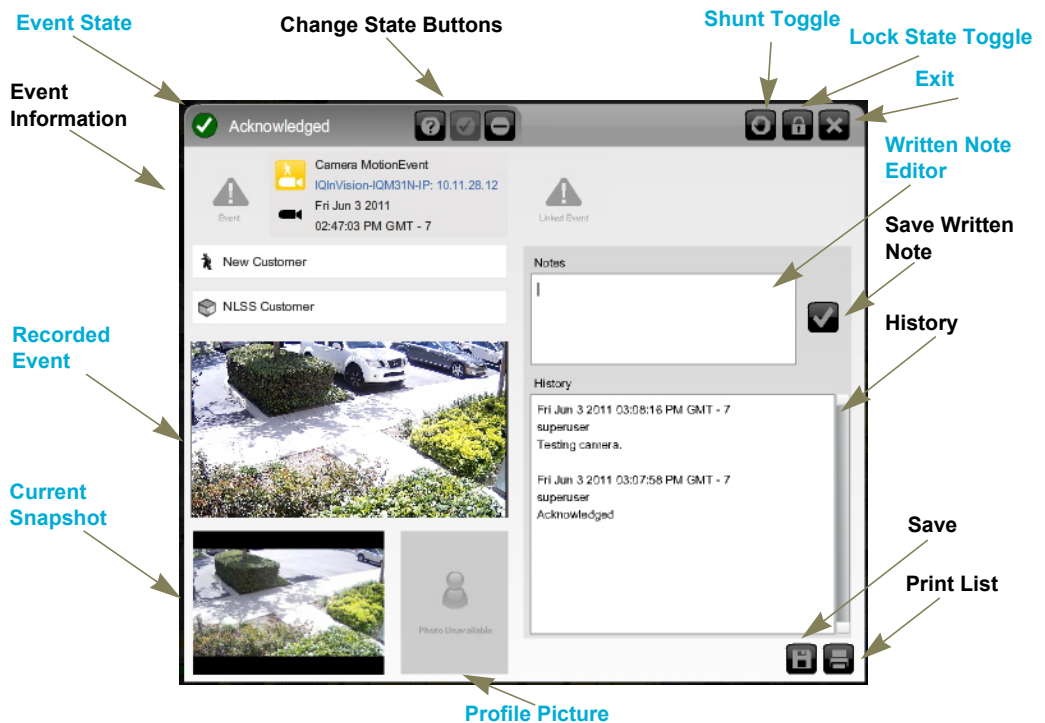
10.2 EVENT DETAILS

When an event is selected in the Realtime View, the Event Log, or from the Camera Event dialog, the *Event Details* dialog is displayed. This dialog lists the details of the event, as displayed in the Event Log and other events windows. The Event Details dialog displays the event if recording is enabled for a camera, and a User can take actions on the event.

10.2.1 Event Details Actions

The *Event Details* dialog allows a User to acknowledge an event, play it back, add notes, and save and print a record of the event.

- Click an event to open the *Event Log Details* dialog.



10.2.1.1 EVENT STATE

The current state is indicated by the icon and text in the upper left corner of the dialog. When an event is triggered, the state is listed as *Open*.

- After the Event Detail dialog is opened, the **Acknowledge** button (check mark) can be clicked to indicate that someone has looked at the event.



Events may be configured by the Superuser to require acknowledgement. See [Event Type Details](#).

- If no further action is needed on the event, click the **Close** (–) button. This marks the event as resolved.



- This button does not close the dialog. Use the **Exit Dialog** button to leave the dialog.

10.2.1.2 SHUNT TOGGLE

If an event type is generating frequent notices that do not need to be reviewed, the event notice can be *shunted*. The event is not recorded to the database. When the event is no longer shunted, the database resumes recording that event.

- Click the **Shunt** toggle to shunt the event type.

To view shunted events, select the **Shunt** tab in the Event Log list.

Note: The shunt setting is specific only to the event type and the source. Events are still displayed for that event type on other devices, unless they are also shunted.

10.2.1.3 LOCK STATE TOGGLE

Events can be saved in the database, to prevent grooming. Grooming occurs when the database deletes the oldest events to make room for newer events.

- Click **Lock** to change the lock state to *Locked*. The Lock button is grayed out when the event is locked. The Lock icon in the Event Log list becomes a closed lock.

10.2.1.4 WRITTEN NOTE EDITOR

A note can be added to the record of any event. Notes provide a chronological history for later reference.

1. Display the Event Log Detail dialog for the desired event.
2. Enter comments in the **Notes** editor.
3. Click the **Save** button (check mark) next to the editor to keep the text.

The note is displayed in the History box below the editor.

Notes also are added automatically to the History box every time a state is changed.

10.2.1.5 RECORDED EVENT

If recording was enabled for the camera that sent the event, a playback of the triggering event loops in the dialog.

10.2.1.6 CURRENT SNAPSHOT

The dialog also displays a snapshot of the camera's video stream at the moment the dialog was opened.

10.2.1.7 PROFILE PICTURE

A profile picture can be displayed if the event is triggered by a User or Cardholder, and a picture is stored in the database.

10.2.1.8 EXPORTING THE EVENT

The data in an Event Detail dialog can be saved to a file or printed.



Save: exports the current Event Log list to a .csv file.



Print: takes a screen shot of the Event Detail dialog and sends it to a printer. Landscape mode is recommended for printing.

10.2.1.9 EXIT

The **Exit** button only is available in the Event Detail dialog if the dialog is launched from an Event pop-up in the Realtime Events View or the video player. In the Event Log, the Detail dialog cannot be closed.

10.2.2 Emergency Events

If the Events button is pulsating in the Main Menu, an Emergency event has been triggered. Emergency events are user configured by setting the severity of an event type. See [Configure Event Severity](#) for more information.

1. Click the **Events** button.
 - If the Realtime View is displayed, click the Event Log link at the top of the screen.

2. In the *Event Log*, click the **Emergency** tab.



3. Click the event item in the list with an *Open* status.



The Event Detail dialog is displayed.

4. Click **Acknowledge** in the top of the Detail dialog.



5. Use the Detail dialog to replay video, add notes, save the event to a .csv file, print a screen shot, shunt or lock the event. See [Event Details Actions](#) for more instructions on using these features.

6. Click the **Close** to remove the event from the Emergency queue.



PART 2: SYSTEM CONFIGURATIONS

System Configurations contains instructions for configuring the devices and data used by the NLSS Unified Security Suite. Configurations are typically done by Superusers through the NLSS Web Interface generated by a NLSS Gateway in your system. A web browser is used to log into a specific NLSS Gateway, from which you can configure and control your system.

Only users with the appropriate software *permissions* on your platform can access and edit the Configuration menu in the NLSS Web Interface. Each system comes with at least one *superuser* with unlimited permissions. This default superuser cannot be deleted, but the default password for this account should be customized. Anyone with the new password can set up other user accounts with various permissions (including other superusers also with unlimited permissions).

NLSS recommends configuring the NLSS Unified Security Suite in the following order.

1. Do global configurations, as described in [Chapter 12: Global Configurations](#).
2. Configure identity related information, as described in [Chapter 13: Configure Identity and Credentials](#).
3. Configure Access Control, as described in [Chapter 14: Configure Access Control](#).
4. Configure video sources, as described in [Chapter 15: Configure Video, Storage, & Decoders](#).

Note: This list assumes that all hardware already has been physically installed.

Chapter 11: General Configuration Functions

Many Configuration menu options contain a table listing the items discovered by the system or added by the User. Four basic functions are available for each list:

- **Search:** lists can be filtered by searching for specific characteristics. See [Searching Tables](#).
- **Print:** click the printer-shaped button in the lower left corner below the table to print the list.
- **Refresh:** click **Refresh** button next to Print button to updates the list.

The ability to add, edit and delete items is dependent on the menu. Each section indicates which functions are available.

11.1 SEARCHING TABLES

The tables at the top of each Configuration pane can be filtered by using the search function above the table. Only the items matching the search criteria are listed.

1. From the **Search** drop-down list, select the column on which you want to search.
2. Enter a value in the **Search** field.
3. Click the **Magnifying Glass** to run the search.
A list of matching items is displayed.
 - If necessary, click a column header to sort the results.
4. To display the entire list again, clear the **Cancel Search** button in the **Search** field. This button is only displayed after a search is run.

Chapter 12: Global Configurations

NLSS recommends doing global configurations in the following order:

1. [Configure RMS](#)
2. [Configure Customer](#)
3. [Configure Sites](#)
4. [Configure NLSS Gateways](#)
5. [Configure Holidays](#)
6. [Configure Schedules](#)
7. [Configure Event Types](#)
8. [Configure Event Severity](#)
9. [Configure Groomer Settings](#)
10. [Configure Actions](#)
11. [Configure Event Linkages](#)

Select **Configurations > Global** from the Main Menu to access the Global Configurations.

Note: The **Save** and **Cancel** buttons are grayed out in the configuration screens until a change is made. The Save button remains grayed out if one of a required field is blank.

12.1 CONFIGURE RMS

Remote Management Services (RMS) allows a *customer* to view and administer multiple *sites* (NLSS Gateways) from a single portal. The devices managed by a Gateway can be monitored from the RMS portal.

Skip this section if you are not running RMS.

If a site is controlled by RMS, a token is generated by the *partner* to allow the site to connect to RMS. That token must be entered manually.

1. Access **Configurations > Global > RMS** from the Main Menu.
2. Click on **RMS**.
3. In the **Remote Management Services Token** field, enter the token from the Partner.
 - If you do not have the token, contact the NLSS Partner who set up RMS.
 - The other fields are filled in automatically by the Partner after the token is saved.
4. Click **Save** to record the token.
 - Click **Cancel** to clear the token.

12.2 CONFIGURE CUSTOMER

Unless this gateway is managed by RMS (Remote Managed Services), details about the customer (site owner) are not critical to the operation of the system. Without RMS, these details are informational, and can be entered in the *Global > Customer* screen.

12.2.1 Customer Details

These parameters define the specific customer that is selected in the table in the top pane of the *Customer Details* screen:

- **Customer Name:** the name of the customer (usually the name of a business).
- **Primary Contact:** the full name of the primary contact person at this customer.
- **Mailing Address:** the mailing address of this customer.
- **Billing Address:** the billing address of this customer. If the billing and mailing addresses are the same, check the **Use Mailing Address** box.

Note: If a site is managed by RMS, enter the same customer details at each site.

12.2.2 Customer: Actions

1. Select **Configuration > Global > Customer** from the Main Menu.
2. Fill in the **Customer Details**, as desired.
3. Select **Save** to keep your changes.
 - Click **Cancel** to restore the previous settings.

12.3 CONFIGURE SITES

NLSS software associates one NLSS Gateway with one site. Site details are optional, unless the site is managed by RMS.

12.3.1 Site Details

The Site Details pane, in the *Configuration > Global > Sites* screen, defines the site managed by the NLSS Gateway to which the NLSS Web Interface is connected.

- **Site Name:** the name of this particular site.
- **Site Address:** various fields for the addresses of this site.
- **Time Zone:** time Zone in which this site is located.
- **Time Mode:** the method is used to set the time on the Gateway. Choices for this setting are either **Manually** or via **NTP Time** (Network Time Protocol Time Server).

12.3.2 Editing Site Details

1. From the Main Menu, select **Configuration > Global > Sites**.
The *Site Details* screen is displayed.
2. Fill in the **Site Details**, as needed.
3. Click **Save** to keep your changes.
 - Click **Cancel** to revert to the previous settings.

12.4 CONFIGURE NLSS GATEWAYS

NLSS Gateways can be managed and configured via the NLSS Web Interface, via the *Configuration > Global > Gateways* screen.

- Select **Configuration > Global > Gateways** from the Main Menu.

The *Gateways* screen is displayed with a table and a *Gateway Details* pane with three tabs:

- **Gateways: General Tab**
- **Gateways: Wired Network Tab**
- **Gateways: Email Tab**

12.4.1 Gateways: General Tab

1. Select a Gateway from the table in the top pane of the *Gateways* screen.
The *Gateway Details* pane is displayed.
2. Open the **General** tab.

12.4.1.1 GENERAL PARAMETERS

If any of the following values are changed, click **Save** to record the changes, or **Cancel** to return to the previous values:

- **Device Name:** a unique name for this NLSS Gateway.
- **Device Type:** (read-only) the hardware series of the selected NLSS Gateway.
- **Firmware Version:** (read-only) the firmware version running on the Gateway.
- **New Firmware Version:** (read-only) indicates the latest version available, which can be updated via [Check Update](#) or [Firmware Update](#).
- **Hardware Version:** (read-only) the hardware version of the Gateway.
- **Serial Number:** (read-only) the serial number of the Gateway, as reported by the Gateway.
- **Install Date:** the date on which this Gateway was installed.
- **Installer:** the name of the person, or system's integrator, who installed this Gateway.
- **Enable SSH:** when SSH is enabled, qualified technical support staff can access and troubleshoot the Gateway remotely using its SSH username and password. When they are finished, disable SSH to prevent further access.

Notes

- Only Superusers have permission to enable SSH.
- The username is **nlss** and the default password is **NextLS32!** for allowing external access. The password can be changed by using an SSH login from a command line and issuing the Linux **passwd** command.
- As long as SSH is disabled, no one can log into the Gateway via SSH, even if they have your SSH password.

12.4.1.2 GENERAL ACTIONS

The following actions are available in the *General* tab of the Gateway Configuration screen:

- [Configuration Backup](#)
- [Configuration Restore](#)
- [Download System Logs](#)
- [Reboot](#)
- [Shut Down](#)
- [File System Check](#)
- [Check Update](#)
- [Factory Reset](#)
- [Firmware Update](#)

12.4.1.2.1 Configuration Backup

Doing a *Configuration Backup* saves all configuration settings in the system to a backup file. **Configuration Restore** reloads the configuration file and restores the Gateway's settings after a **Check Update** and **Firmware Update**, or **Factory Reset** is performed.

1. In the **General** tab, click the **Configuration Backup** button.
2. Follow the instructions on the screen to create a protected copy of the current configuration settings for the system.

The configuration backup file is a compressed ZIP file. Depending on the browser and its settings, this file might be saved in compressed or uncompressed form.

When doing a **Configuration Restore**, the configuration file must be in a *compressed* format. Therefore, if the browser uncompressed the configuration file, then the file must be recompressed before being used to restore system configurations.

12.4.1.2.2 Configuration Restore

Selecting *Configuration Restore* lets you restore your system to the configuration settings that were last saved via the **Configuration Backup** option.

1. In the *Configuration > Global > Gateways* screen, select the target NLSS Gateway from the table, so as to display its configuration settings in the **General** and **Wired Network** tabs of the *Gateway Details* page.

The *Gateway Details* pane is displayed.

2. In the **General** tab, click the **Configuration Restore** button.
3. Follow the instructions on the screen to restore your system to the configuration settings that were last backed up via the *Configure Backup* option.

Note:

- You must first do a **Configuration Backup** to create a configuration backup file, before you are able to follow the *Configuration Restore* procedure.
- The configuration backup file must be in compressed (ZIP) format before it can be used to restore your configurations. Depending on your browser and its settings, this backup file might be saved in compressed or uncompressed form. Therefore, if your browser had uncompressed the configuration file when it was created, then you must recompress the file before using it to restore your configurations.

12.4.1.2.3 Download System Logs

If you contact NLSS or its authorized representatives for support, a technician might ask you for your Gateway's system logs to help with troubleshooting. Here's how to save these logs to a file:

1. In the *Configuration > Global > Gateways* screen, select an NLSS Gateway from the table to display its configuration settings.

The *Gateway Details* pane is displayed.

2. In the **General** tab, click the **Download System Logs** button.
3. Follow the instructions on the screen to save the log file locally.

12.4.1.2.4 Reboot

Important: The NLSS Gateway and its monitoring features are not available during a reboot.

1. In the *Configuration > Global > Gateways* screen, select an NLSS Gateway from the table, so as to display its configuration settings in the General and Wired Network tabs of the Gateway Details page.
2. In the General tab of Gateway Details, click the **Reboot** button to reboot the Gateway. A confirmation dialog is displayed.
3. Click **Yes** to confirm the process.
 - Click **No** to abort the reboot.

12.4.1.2.5 Shut Down

An NLSS Gateway can be shut down via the NLSS Web Interface.

1. In the **General** tab, click the **Shut Down** button. A dialog box is displayed asking for confirmation.
2. Click **Yes** to confirm the process.
 - Click **No** to abort the shut down.

12.4.1.2.6 File System Check

The NLSS Web Interface provides an option to run a File System Check on an NLSS Gateway's internal drive. The check seeks file system inconsistencies and repairs them. This procedure may be necessary if the Gateway is improperly shut down, such as due to a power failure.

Important: The NLSS Gateway and its monitoring features are not available while check is running. The length of time to run a File System Check depends the amount of data stored on the internal hard drive.

1. In the **General** tab, click the **File System Check** button. A dialog box is displayed asking for confirmation.
2. Click **Yes** to confirm the process.
 - Click **No** to abort the File System Check.

When the File System Check is completed, the NLSS Gateway is rebooted.

12.4.1.2.7 Check Update

Selecting *Check Updates* causes the system to check the NLSS web site for updates to the firmware used on your NLSS Gateways.

Important: Monitoring is disabled for approximately five (5) minutes or more during this upgrade.

1. In the *General* tab of the *Configuration > Global > Gateways* screen, select an NLSS Gateway from the table, so as to display its configuration settings.

2. In the General tab of Gateway Details, click the **Check Updates** button. Then follow the instructions on the screen to check for updated firmware. If a more recent version of the Gateway's firmware is found, the firmware will be updated and your Gateway should automatically reboot when done.

Note: After updating the firmware for the NLSS Gateway, you need to clear the cache in your browser to see new features in the NLSS Web Interface of that Gateway.

12.4.1.2.8 Firmware Update

If you don't have an Internet connection to support automatic firmware updates (via the Check Updates button), or if you prefer to update the firmware manually for any reason, then do the following:

1. Download the latest firmware file for your Gateway from the NLSS web site, or obtain it from your authorized NLSS representative.
2. Copy the firmware file to the hard drive of any PC on the same network as the target Gateway.
3. In the *Configuration > Global > Gateways* screen, select an NLSS Gateway from the table of Gateways, so as to display its configuration settings.
4. In the General tab of Gateway Details, click the **Firmware Update** button to display a file loader.
5. In the file loader, click the **Browse** button and locate the new firmware file that you saved on your PC's hard drive. Then select **Upload** to copy the file to the Gateway.
6. After the upload is done, reboot the Gateway if it does not automatically reboot.

Note: After updating the firmware for the NLSS Gateway, you need to clear the cache in your browser to see new features in the NLSS Web Interface of that Gateway.

12.4.1.2.9 Factory Reset

The Factory Reset function restores the NLSS Gateway to its factory state, with the exception of preserving firmware updates that have been installed since the Gateway shipped.

Specifically, a *Factory Reset* deletes all files and configurations (except firmware updates and configuration backups) recorded by the Gateway since leaving the factory.

Note: After doing a Factory Reset, the Gateway must be reinstalled on the LAN. See [Install NLSS Gateways](#).

Important: Before you use the following procedure to restore an NLSS Gateway to its factory state, [Configuration Backup](#) can be run. A Factory Reset deletes the system configurations and records saved by the Gateway.

If desired, you may backup the configuration via the [Configuration Backup](#).

1. In the *Configuration > Global > Gateways* screen, select an NLSS Gateway from the table, so as to display its configuration settings in the tabs of the Gateway Details page.
2. In the General tab of Gateway Details, click the **Factory Reset** button. Then follow the instructions on the screen to restore the Gateway to its factory state.

3. To restore configuration settings, select **Configuration Restore** in the General tab of the *Gateway Details* pane.

Follow the instructions on the screen to restore the previous configuration settings.

Note: After resetting the firmware for the NLSS Gateway, clear the cache in the browser to fully restore the NLSS Web Interface of that Gateway.

12.4.2 Gateways: Wired Network Tab

The GW-3000 Gateway has two Ethernet ports and two sets of DHCP parameters. The GW-500 has only one Ethernet port with one set of DHCP parameters.

- **Enable DHCP:** enabling DHCP is recommended for most network installations, since DHCP automatically assigns an IP address to the NLSS Gateway. Disabling DHCP requires that you manually define the network location of your NLSS Gateway by entering the correct values in the following fields. These fields are only available only if DHCP is disabled.
 - **IP Address:** if DHCP is enabled, the system automatically displays the IP address of the selected Gateway. If DHCP is disabled, enter a valid numerical IP address in this field, such as 10.11.23.170.
 - **Subnet Mask:** if DHCP is enabled, the system automatically displays the subnet mask address of the selected NLSS Gateway. If DHCP is disabled, enter a valid subnet mask here, such as 255.255.255.0
 - **Default IP Gateway:** if DHCP is enabled, the system automatically displays the IP address of the *network gateway* used to access the selected NLSS Gateway. If DHCP is disabled, enter a valid IP address.

Note: The network gateway is a standard networking device. An NLSS Gateway is the nerve center of the NLSS Unified Security Platform. They are very different devices.

- **Primary DNS:** the IP address of the primary DNS server.
- **Secondary DNS:** the IP address of the secondary DNS server.
- **MAC Address:** (read-only) The physical address of the selected NLSS Gateway on your network. It is independent of DHCP and the IP address.
- **Link Speed:** (read-only) The data transfer speed (in Megabits per second) of the network to which the NLSS Gateway is attached.

If any of the parameters are changed:

- Click **Save** to keep the changes.
 - Click **Cancel** to return to the previous settings.

12.4.3 Gateways: Email Tab

An email can be sent by the Gateway to notify a user when a certain event takes place. This feature is set up using *Event Linkages* and *Actions*. See [Configure Event Linkages](#) and *SendEmail* in [Action Type](#) for more information.

The Email tab provides the fields needed to set an email server to through which the Gateway can send a message when triggered by an event.

1. Select **Configuration > Global > Gateways** from the Main Menu.
2. Under *Gateway Details*, select the **Email** tab.
3. Select a Mail Server. Check with your system administrator as to the correct server type, either **Sendmail** or **SMTP**.
 - If an SMTP server is installed, enter the **SMTP Server** name and **Password**, if required.
4. Enter a **Test Email Recipient** to verify the email connection.
5. Click **Test** to send a test message.
6. Click **Save** to keep the setting.
 - Click **Cancel** to return to the previous settings.
7. Check with the email recipient that the test message was received.

12.5 CONFIGURE HOLIDAYS

In the *Configuration > Global > Holidays* screen, the configured Holidays are listed. Initially, the screen is empty. Holidays can be added, configured, searched and deleted.

12.5.1 Holidays Table

After the Holidays are entered, a table is displayed in the top pane. Click on a Holiday to display the Holiday Details in the bottom pane.

Click the column headers to sort the list.

See [Searching Tables](#) for search instructions.

12.5.2 Holiday Details

Three parameters apply can be configured in the *Holiday Details* pane.

- **Name:** enter the name of this holiday.
- **Start Date:** the start date of the holiday. The time the Holiday begins is 12:01 a.m. on the Start Date.
- **End Date:** the end date of the Holiday being configured. The time it ends is 11:59 p.m. on the End Date. For one day Holidays, the End Date is the same as the Start Date.

12.5.3 Holidays: Actions

Holidays can be added, edited, deleted and searched.

12.5.3.1 ADD NEW HOLIDAYS

1. Select **Configuration > Global > Holidays** from the Main Menu.
The *Holidays* screen is displayed.
2. Click **Add** in the *Holidays* screen.
The *Holiday Details* pane is displayed.
3. Enter the **Holiday Details**.
4. Click **Save** to keep the settings.
 - Click **Cancel** to return to the previous settings.

12.5.3.2 EDIT HOLIDAYS

1. Select **Configuration > Global > Holidays** from the Main Menu.
The *Holidays* table is displayed.
2. Select an existing Holiday from the table.
The *Holiday Details* pane is displayed.
3. Edit the **Holiday Details**, as needed.
4. Click **Save** to keep the settings.
 - Click **Cancel** to return to the previous settings.

12.5.3.3 DELETE HOLIDAYS

1. Select **Configuration > Global > Holidays** from the Main Menu.
The *Holidays* table is displayed.
2. Select a Holiday from the table.
3. Click the **Delete** button.
4. Click **Yes** in the confirmation box.
 - Click **Cancel** to keep the deletion.

12.6 CONFIGURE SCHEDULES

In the *Configuration > Global > Schedules* screen, the configured schedules are listed. Initially, the screen is empty. Schedules can be added, configured, searched and deleted.

After a schedule is configured, it is available for application throughout the system.

- **Configuration > Identity > Access Levels:** in the [Configure Access Levels](#) screen, access levels are associated with schedules. When you assign an access level to a Cardholder, the Cardholder can open doors only during the days and times in the associated schedule.
- **Configuration > Access Control > Doors:** in the [Configure Doors](#) screen, select an *Auto-Unlock Schedule* to assign to each door. Those doors are unlocked only during the days and times in the associated schedule. The doors are not unlocked if the schedule is set to be disabled on Holidays configured for the system.
- **Configuration > Video > Cameras:** in the [Configure Cameras and Streams](#) screen, cameras and other streams are associated with recording schedules—so the camera records only during the dates and times in the schedule.

Important: Holidays override the schedules used by everything related to Cardholders and Access Control, but not cameras. Recordings of video streams continue according to their associated schedules, even on Holidays.

12.6.1 Schedules Table

After the schedules are entered, a table is displayed in the top pane. Click on a schedule and the [Schedule Details](#) are displayed in the bottom pane.

Click on a column headers to sort the list.

See [Searching Tables](#) for search instructions.

12.6.2 Schedule Details

The Schedule Details pane lists the parameters for the selected schedule.

- **Schedule Name:** a unique name to identify the schedule.
- **Start Time:** the time of day that this schedule starts. For example, if 8 a.m. is selected, then doors using this schedule unlock at 8 a.m.
- **End Time:** the time of day that this schedule ends. For example, if 6 p.m., then doors using this schedule lock at 6 p.m.
- **Days of Week:** select the day or days of the week to apply this schedule.
- **Disable Schedule on Holidays:** if enabled, the applicable doors are not unlocked on Holidays. For example, if an external door using this schedule is normally open during business hours on Mondays, then select this parameter to ensure that the door remains locked on a configured Holiday that falls on a Monday.

12.6.3 Schedules: Actions

Schedules can be added, edited, searched and deleted.

12.6.3.1 CREATE NEW SCHEDULES

1. Select **Configuration > Global > Schedules** from the Main Menu.
The *Schedules* screen is displayed.
2. Click **Add** in the *Schedules* screen.
The *Schedule Details* pane is displayed.
3. Enter the **Schedule Details**.
4. Optionally, to **Disable Schedules on Holidays** select the **Disable** flag.
This option prevents an auto-unlock schedules on Holidays.
5. Click **Save** to keep the settings.
 - Click **Cancel** to return to the previous settings.

12.6.3.2 EDIT SCHEDULES

1. Select **Configuration > Global > Schedules** from the Main Menu.
The *Schedules* table is displayed.
2. Select a Schedule from the table.
The *Schedule Details* pane is displayed.
3. Edit the **Schedule Details**, as needed.
4. Click **Save** to keep the settings.
 - Click **Cancel** to return to the previous settings.

12.6.3.3 DELETE SCHEDULES

1. Select **Configuration > Global > Schedules** from the Main Menu.
The *Schedules* table is displayed.
2. Select a Schedule from the table.
3. Click the **Delete** button.
4. Click **Yes** in the confirmation box.
 - Click **Cancel** to keep the Schedule.

12.7 CONFIGURE EVENT TYPES

The NLSS Unified Security Suite comes with pre-defined event types that can be used throughout the system. The Event Types that come with the system are listed in the top pane of the *Event Type* screen. Event Types cannot be created or deleted, but the parameters can be modified.

Click on a column headers to sort the list.

See [Searching Tables](#) for search instructions.

12.7.1 Event Type Table

The Event Type table lists the Event Types included with the system.

- **Event Type Name:** the default label given to the Event Type. This name cannot be changed.
- **Event Severity Name:** the Severity level assigned in the Event Type Details pane.
- **Needs Acknowledgement:** if an event is checked with Needs Acknowledgement, it displays in the Event Table in the Open State, but the Icon is Red, not Orange. The Events Table can be filtered on Needs Acknowledgement. See [Chapter 10: Monitoring and Handling Events](#) for more information.

12.7.2 Event Type Details

The Event Type Details pane lists the parameters for the selected Event Type.

- **Needs Acknowledgement:** select this box to require an acknowledgement of this event type; deselect to make an acknowledgement optional.
- **Event Name:** (read-only) The name of the selected event type from the table.
- **Description:** enter a brief explanation of this event type.
- **Severity:** the drop-down list provides pre-defined severity levels to associate with the selected event type.

12.7.3 Event Types

Event types can be edited and searched, but cannot be created or deleted.

1. Select **Configuration > Global > Event Type** from the Main Menu.
The *Event Type* table is displayed.
2. Select the desired Event Type from the table.
The *Event Type Details* pane is displayed.
3. Edit the fields as desired.
See [Event Type Details](#) for more information.
4. Click **Save** to keep the setting.
 - Click **Cancel** to return to the previous settings.

12.8 CONFIGURE EVENT SEVERITY

The NLSS Unified Security Suite comes with pre-defined Event Severity levels (IDs) that apply across the entire system. The ID levels that come with the system are listed in the top pane of the *Event Severity* screen. Select a specific event severity from the table to view its parameters.

12.8.1 Event Severity Table

This table lists the default severity levels, and their descriptions. Click on an item to display the [Event Severity Details](#).

Click on a column headers to sort the list.

See [Searching Tables](#) for search instructions.

12.8.2 Event Severity Details

The Event Severity Details lists two parameters.

- **Event Severity ID:** (read-only) The ID level of the selected Event Severity.
- **Event Severity Description:** a custom description of the selected event severity. Although the description can be edited, the system is designed so that ID **1** represents the most severe events (emergencies), and ID **8** represents the least severe events (debugging).

12.8.3 Editing the Event Severity Description

1. Select **Configuration > Global > Event Severity** from the Main Menu.
The *Event Severity* table is displayed.
2. Click the entry in the table.
The *Event Severity Details* are displayed.
3. Edit the **Event Severity Description** parameter, if needed.
4. Click **Save** to keep the change.
 - Click **Cancel** to return to the previous description.

12.9 CONFIGURE GROOMER SETTINGS

Saving video clips can take up a lot of disc space. *Groomer Settings* allow the system to automatically delete older audio-video clips, if the storage device is running low on disc space. The groomer function deletes older clips first to make room for new clips, according to the configuration settings.

1. Select **Configuration > Global > Groomer Settings** from the Main Menu.
The *Groomer Setting Details* screen is displayed.
2. Edit the Groomer Setting values as desired.

- **Minimum Retention (Days):** the shortest time (in days) that saved files are preserved, before being considered for deletion by the groomer.
 - **Maximum Retention (Days):** the longest time (in days) that saved files saved are preserved, before being deleted by the groomer function.
3. Click **Save** to keep the changes.
 - Click **Cancel** to return to the previous settings.

Important: Groomer settings can be overridden on a per-camera basis in the Recording tab of the *Configuration > Video > Cameras* screen. See [Camera Details: Recording Tab](#) for more information.

12.10 CONFIGURE ACTIONS

An *Action*, or behaviors, can be associated with a device such as a door or a camera. The action is triggered when a linked event occurs. The trigger is set using [Configure Event Linkages](#).

1. Select Configuration > Global > Action from the Main Menu.
The Action screen is displayed.
2. Click on a column header to sort the list.
 - Actions can be created, edited, deleted, or searched from the *Action* screen.
 - » See [Searching Tables](#) for search instructions.
 - Click the **Print** button to print the Action list.
 - Click the **Refresh** button to update the list.

12.10.1 Action Type

An Action is defined by an *Action Type*. Apply an Action Type to a specific device category, such as a camera or door, or across all device categories.

When an Action Type is selected for a device category, a specific device must be selected to apply the Action when the linked event occurs.

Action Type	Definition
ACDoorMomentaryUnlock	Temporarily unlocks the selected door.
ACDoorRelock	Locks the selected door.
ACDoorUnlock	Unlocks the selected door.
ACOutputOff	Disables the selected I/O output.
ACOutputOn	Enables the selected I/O output.
ChannelSetActive	Activates a channel for the selected decoder. Select a decoder then select an available channel from the second drop-down that is displayed after the decoder is selected.

Action Type	Definition
EmailSend	Creates an email to send when an event occurs. A Recipient Email Address , a Subject and Body can be entered to be sent automatically by the Gateway when the linked event occurs.
PTZGoToHomePos	Returns a PTZ enabled camera to its home position. See Using Presets for more information.
PTZGoToPreset	Moves a PTZ enabled camera to a preset position. See Using Presets for more information.
PTZStartPatrol	Starts a Patrol sequence on a PTZ enabled camera. See Using Patrols for more information.
StreamRecordStart	Starts recording of a camera or video stream when triggered by an event. See Camera Details: Recording Tab for more information.
StreamRecordStop	Stops recording of a camera or video stream when triggered by an event. See Camera Details: Recording Tab for more information.
VASStart	Starts a Video Analytic for the selected camera, when triggered by an event. Select a camera and then select an analytic from a second drop-down list that is displayed after the camera is selected. See Video Analytics for instructions on configuring analytics. Note that only one analytic may be <i>active</i> for a camera.
VASStop	Stops a Video Analytic for the selected camera, when triggered by an event. Select a camera and then select an analytic from a second drop-down list that is displayed after the camera is selected. See Video Analytics for instructions on configuring analytics.
ViewSetActive	Activate a view for the selected decoder. A second drop-down list listing the available views is displayed after the decoder is selected.

12.10.2 Creating an Action

1. Select **Configuration > Global > Action** from the Main Menu.
The *Action* table is displayed.
2. Click **Add**.
The *Action Details* pane is displayed in the bottom pane.
3. Enter a descriptive **Action Name**.
The name must be unique. If the same action applies to multiple devices, include a unique identifier in the name, such as *Unlock Main Door*, *Unlock Side Door*.
4. Select an **Action Type** from the drop-down list. See [Action Type](#) for more information.
 - If the Action Type applies to a certain device category, a drop-down list shows the available devices.

- If the Action Type applies to all devices, additional fields are displayed to configure that action.
- 5. Select a device from the drop-down list to apply the action, or fill in the fields to configure the action.
- 6. Click **Save** to add the Action.
 - Click **Cancel** to clear the settings.

12.10.3 Editing Actions

Existing items in the Action table can be edited.

1. Select **Configuration > Global > Action** from the Main Menu.
The *Action* dialog is displayed.
2. Click on the desired Action.
The item is displayed in the *Action Details* pane.
3. Update the fields as needed.
4. Click **Save** to update the Action.
 - Click **Cancel** to return to the previous settings.

12.10.4 Deleting an Action

Actions can be deleted from the Action table.

1. Select **Configuration > Global > Action** from the Main Menu.
The *Action* dialog is displayed.
2. Select an item from the Action table.
3. Click **Delete**.
4. Click **Yes** in the confirmation dialog.
 - Click **Cancel** to keep the Action.

12.11 CONFIGURE EVENT LINKAGES

Event Linkages are one of the most powerful features of the system. Event Linkages allow specific events to be linked with one or more specific Actions. This feature allows the system to be highly customized for specific applications and installations. When a specific event occurs on a device, actions are triggered for that device or related devices.

Event Linkages allow you to associate one more or actions with an event. An Event Type, Source, and Schedule, as well as Severity can be associated with a defined Action. See [Configure Actions](#).

Event Types are configured with a default Severity and a default setting of *Needs Acknowledgement*. Severity and Needs Acknowledgement can be overwritten for a specific *Event->Action* linkage in the Event Linkages page.

Note: An overwrite applies only to the source of the event when it is linked to a specific action.

- Click on a column header to sort the table.
- Event Linkages can be created, edited, deleted, or searched from the *Event Linkage* screen.
 - See [Searching Tables](#) for search instructions.
- From the *Event Linkages* dialog, linkages can be created, edited, deleted, or searched.
- Click the **Print** button to print the Event Linkages list.
- Click the **Refresh** button to update the Event Linkages list.

12.11.1 Creating an Event Linkage

1. Select **Configuration > Global > Event Linkages** from the Main Menu.
The *Event Linkages* dialog is displayed.
2. Click **Add**.
The *Event Linkages Details* pane is displayed in the bottom pane.
3. Enter a descriptive **Event Linkage Name**.
4. Select an **Event Type** from the drop-down list.
The Event Source field displays the devices associated with that event type.
5. Select an **Event Schedule** to apply to the linkage.
6. Select an **Event Source** to use with the linkage.
7. Select actions to include with the Event Linkage.
 - a. Click on an item in the **Available Actions** list.
 - b. Click the right arrow button (>) to move the action to the **Selected Actions** list.
 - » Use the double right arrows button (>>) to move all actions to the **Selected Actions** list.

- » Use the left arrow button (<) to remove an item from the **Selected Actions** list.
 - » Use the double left arrow button (<<) to remove all items from the **Selected Actions** list.
8. Select a **Severity** level from the drop-down list.
 9. Select the **Needs Acknowledgment** check box if you want the system to send a message with a required response confirming a user knows that the event occurred.
 10. Click **Save** to add the item to the Event Linkages list.
 - Click **Cancel** to clear the settings.

12.11.2 Editing an Event Linkage

Existing Event Linkage items can be edited.

1. Select **Configuration > Global > Event Linkages** from the Main Menu.
The *Event Linkages* dialog is displayed.
2. Click on the desired Event Linkage.
The item is displayed in the *Event Linkage Details* pane.
3. Update the fields as needed.
4. Click **Save** to update the Event Linkages item.
 - Click **Cancel** to return to the previous settings.

12.11.3 Deleting an Event Linkage

Items can be deleted from the Event Linkage table.

1. Select **Configuration > Global > Event Linkage** from the Main Menu.
2. Select an item from the Event Linkage table.
3. Click **Delete**.
4. Click **Yes** in the confirmation box.
 - Click **Cancel** to keep the Event Linkage.

Chapter 13: Configure Identity and Credentials

You need SuperUser permissions to configure identity and credentials for new Users and Cardholders.

NLSS recommends this configuration be completed in the following order:

1. **Configure Access Levels**: required to provide access privileges to Cardholders.
2. **Configure Card Profiles**: required to set up Badge Profiles, and to define the technical aspects of the card (such as Type, Bit Format and Facility Code).
3. **Configure Badge Profiles**: required to define the types of Cardholders in your system, and to set up Cardholders. Badge profiles are also used to set default deactivation dates, orientation, and logos.
4. **Configure Cardholders**: requires that Access Levels, Card Profiles, and Badge Profiles are already configured.
5. **Configure Cardholder-User Defined Field Labels** for Cardholders. This step is optional.
6. **Configure Users** of the NLSS Unified Security Suite software.

13.1 CONFIGURE ACCESS LEVELS

An *Access Level* associates doors to schedules and the assigned rights of Cardholders to gain access. Access Levels are set up in the *Configuration > Identity > Access Levels* screen.

An Access Level is an association of a door or doors with a specific time schedule.

Note: A very good understanding of Access Levels is needed to avoid duplication and the potential system limitation of Access Levels per cardholder record.

1. Schedules and Doors must be created before Access Levels. See **Configure Schedules** and **Configure Doors**.
2. Access Levels are assigned to Cardholders in two areas of the system for the purpose of granting access.
 - The Global Badge Profile for Default Access Level.
 - The Cardholder record, Access Level tab, additional Access Levels can be added here in addition to the Default Access Level. Additional levels may override current Access Level settings. See **Cardholders: Access Levels Tab**.

- Up to 32 Access Levels are allowed per Cardholder record, and is based on the specific Access Control manufacturer. For example: Assa Abloy allows 1 level, HID Edge allows up to 8, and Mercury allows up to 32 levels.

Note: Holidays can disable Access Levels for access control devices. See [Configure Schedules](#).

13.1.1 Access Levels Table

Select **Configuration > Identity > Access Levels** from the Main Menu. The *Access Levels* table is displayed.

Click the column headers to sort the list.

See [Searching Tables](#) for search instructions.

13.1.2 Access Level Details

When you select an Access Level from the table, the *Access Level Details* pane is displayed in the bottom pane.

- Access Level Name:** a descriptive name for the access level.
- Door Name:** all the doors in the system are listed in the drop-down list. By default, none of the doors use a schedule. To select a door, click its name in the list.
- Schedule Name:** select a schedule from the drop-down list to associate it with the door in the Door Name cell to the left (in the same row).

13.1.3 Access Levels: Actions

Actions available are:

- [Create New Access Levels](#)
- [Edit Access Levels](#)
- [Delete Access Levels](#)

13.1.3.1 CREATE NEW ACCESS LEVELS

- Select **Configuration > Identity > Access Levels** from the Main Menu.
The *Access Levels* table is displayed.
- Click the **Add** button.
The *Access Levels Details* pane is displayed.
- Using the **Schedule Names** drop-down lists, assign schedules to one or more doors in the system.
Multiple doors can use the same access level.
Multiple Access Levels can be assigned to a door, as long as Schedule Name settings are different for the door at each Access Level.

4. Click **Save** to keep the settings.
 - Click **Cancel** to clear the values.

13.1.3.2 EDIT ACCESS LEVELS

1. Select **Configuration > Identity > Access Levels** from the Main Menu.
The *Access Levels* table is displayed.
2. Click on an item in the table.
The *Access Levels Details* pane is displayed.
3. Edit the **Access Level Details** for the selected item.
4. Click **Save** to keep the settings.
 - Click **Cancel** to return to the previous settings.

13.1.3.3 DELETE ACCESS LEVELS

1. Select **Configuration > Identity > Access Levels** from the Main Menu.
The *Access Levels* table is displayed.
2. Click the **Delete** button.
A confirmation dialog is displayed.
3. Click **Yes** to verify the deletion.
 - Click **Cancel** to close the dialog and keep the Access Level.

13.2 CONFIGURE CARD PROFILES

By definition, a Cardholder can use cards to access one or more doors in the NLSS system. *Card Profiles* determine the basic data structure and other key properties of the access cards being used in the system. These technical aspects of the card are Type, Bit Format and possibly Facility Code.

Important: Card Profiles must be configured before they can be used as building blocks to **Configure Badge Profiles**.

Both Card and Badge Profiles must be configured before cards can be configured for Cardholders.

13.2.1 Card Profiles Table

Select **Configuration > Identity > Card Profiles** from the Main Menu. The *Card Profiles* table is displayed.

Click the column headers to sort the list.

See **Searching Tables** for search instructions.

13.2.2 Card Profile Details

- **Card Profile Name:** a unique, user-definable field that assigns a user-friendly label to the technical characteristics of the card.

Note: There is likely to be one (1) card profile per company.

- **Facility Code:** a unique number assigned to the customer by the card manufacturer.
 - See http://www.hidglobal.com/page.php?page_id=19 for more information.

Note: Not all Bit Formats require a facility code.

- **Bit Format:** the data structure for this card is selected from the drop-down list.
 - **26-bit: H10301**
 - » The industry standard *open* format.
 - » 255 possible facility codes.
 - » Each facility code has a total of 65,535 unique card numbers.
 - **37-bit: H10302**
 - » HID Proprietary 37 Bit Format: H10302 (without Facility code)
 - » HID controls the issuing of card numbers and does not duplicate the numbers.
 - **37-bit: H10304**
 - » HID Proprietary 37 Bit Format with Facility Code: H10304
 - » HID controls the issuing of card numbers and does not duplicate the numbers.
 - » 65,535 possible facility codes.
 - » Each facility code has a total of 500,000 unique card numbers.
 - » This format is reserved for those customers with a requirement for a large population of cards.

See http://www.hidglobal.com/page.php?page_id=10 for more information.

- **Card Profile Type:** select either **Prox** and **iCLASS** from the drop-down list.

13.2.3 Card Profile: Actions

Actions available are:

- [Create New Card Profiles](#)
- [Edit Card Profiles](#)
- [Delete Card Profiles](#)

13.2.3.1 CREATE NEW CARD PROFILES

1. Select **Configuration > Identity > Card Profiles** from the Main Menu.
The *Card Profiles* table is displayed.
2. Click the **Add** button.
The *Card Profile Details* pane is displayed.

3. Select values for **Card Profile Details**.
4. Click **Save** to keep the settings.
 - Click **Cancel** to clear those values.

13.2.3.2 EDIT CARD PROFILES

1. Select **Configuration > Identity > Card Profiles** from the Main Menu.
The *Card Profiles* table is displayed.
2. Click an item in the Card Profile list to select a profile.
The *Card Profile Details* pane is displayed.
3. Edit the **Card Profile Details**, as desired.
4. Click **Save** to keep the changes.
 - Click **Cancel** to return to the previous settings.

13.2.3.3 DELETE CARD PROFILES

1. Select **Configuration > Identity > Card Profiles** from the Main Menu.
The *Card Profiles* table is displayed.
2. Click an entry in the Card Profile list to select a profile.
3. Select the **Delete** button.
A confirmation dialog is displayed.
4. Click **Yes** to verify the deletion.
 - Click **Cancel** to close the dialog and keep the profile.

13.3 CONFIGURE BADGE PROFILES

A *Badge Profile* completes the profile of all the generic information required for Cardholder badges. The only additional information required to produce actual badges is unique to the individual Cardholder. Cardholder-specific data is entered in the Cardholder configuration screens.

Important: A key building block of Badge Profiles is Card Profiles. Before configuring a Badge Profiles, at least one Card Profile must be configured, as described in [Configure Card Profiles](#).

13.3.1 Badge Profiles Table

Select **Configuration > Identity > Badge Profiles** from the Main Menu. The *Badge Profiles* table is displayed. The table is empty until Badge Profiles are added.

Click the column headers to sort the list.

See [Searching Tables](#) for search instructions.

13.3.2 Badge Profiles Details

- **Badge Profile Name:** a unique name for this Badge Profile. These profiles are created for various badge types used by a company.
 - NLSS recommends creating a unique badge profile for each category or personnel-type at a company.
For example: Employee, Contractor, Temporary, Vendor, Janitor, Manager, Security, etc. The model provides templates from which to add new employees quickly and easily.
 - When cards with different Badge Profiles are printed, they typically lead to different looking access cards.
- **Badge Orientation:** either Portrait or Landscape orientation is available for printing badges using this profile.
- **Border Color:** sets the color of the 1/8-inch border surrounding the image for this Badge Profile.
- **Co. Logo:** optional. Launches a file browser to locate and load a JPEG image, such as a company logo. Keep the file size small for optimum performance. The recommended size is 144px wide x72px high at 300 dpi.
- **Default Deactivation:** the time (in days, months, or years) after which cards based on this Badge Profile automatically deactivates.
 - **Time Format:** a drop-down list with options for **Day**, **Month** or **Year** to set the units for the Default Deactivation time.
- **Default Access Level:** a drop-down list with Access Levels to select the default setting for this Badge Profile. When creating new Credentials in the *Identity Cardholder* screen, as the specific Badge Profile Name is selected, the Access Level is automatically applied.
- **Card Profile Name:** this setting is where the specific Badge Profile and Card Profile are mapped together. The Badge Profile inherits its data formats from the Card Profile selected from this list.

13.3.3 Badge Profiles: Actions

The following actions are available in the *Configuration > Identity > Badge Profiles* screen:

- [Create New Badge Profiles](#)
- [Edit Badge Profiles](#)
- [Delete Badge Profiles](#)

13.3.3.1 CREATE NEW BADGE PROFILES

1. Select **Configuration > Identity > Badge Profiles** from the Main Menu.
The *Badge Profiles* table is displayed.
2. Click the **Add** button.
The *Badge Profile Details* pane is displayed.

3. Enter values for **Badge Profiles Details**.
4. Click **Save** to keep the settings.
 - Click **Cancel** to clear the values.

13.3.3.2 EDIT BADGE PROFILES

1. Select **Configuration > Identity > Badge Profiles** from the Main Menu.
The *Badge Profiles* table is displayed.
2. Click an entry in the Badge Profiles list.
The *Badge Profile Details* pane is displayed.
3. Edit **Badge Profiles Details**, as desired.
4. Click **Save** to keep the changes.
 - Click **Cancel** to return to the previous settings.

13.3.3.3 DELETE BADGE PROFILES

To delete an existing badge profile:

1. Select **Configuration > Identity > Badge Profiles** from the Main Menu.
The *Badge Profiles* table is displayed.
2. Click an entry in the Badge Profiles table.
3. Select the **Delete** button.
A confirmation dialog is displayed.
4. Click **Yes** to verify the deletion.
 - Click **Cancel** to close the dialog and keep the profile.

13.4 CONFIGURE CARDHOLDERS

For the purpose of this manual, *Cardholders* with the appropriate access levels can open doors secured by the NLSS Unified Security System. In contrast, *Users* control the system (as allowed by their *roles*) by logging into the NLSS Web Interface.

A person can be a Cardholder, a User, or both. The system handles Cardholders and Users separately.

In the *Configuration > Identity > Cardholder* screen, configure each Cardholder in the following order:

1. Create a new Cardholder, as described in **Cardholder Actions**. Then configure the parameters of the new Cardholder, as follows:
2. Fill in the values in the **Cardholders: General Tab**
3. Fill in the values in the **Cardholders: Credentials Tab**
4. Fill in the values in the **Cardholders: Access Levels Tab**

5. Fill in the values in the [Cardholders: Contacts Tab](#)
6. Fill in the values in the [Cardholders: Organizational Tab](#)
7. Fill in the values in the [Cardholders: User Defined Tab](#)
8. Fill in the values in the [Cardholders: Options Tab](#)

13.4.1 Card Holders Table

Select **Configuration > Identity > Cardholders** from the Main Menu. The *Cardholders* table is displayed. The table is empty until Cardholders are added.

Click the column headers to sort the list.

See [Searching Tables](#) for search instructions.

13.4.2 Cardholder Actions

The following actions are available in the *Configuration > Identity > Cardholder* screen.

- [Create New Cardholders](#)
- [Edit Cardholders](#)
- [Delete Cardholders](#)

13.4.2.1 CREATE NEW CARDHOLDERS

1. Select **Configuration > Identity > Cardholders** from the Main Menu.
The *Cardholders* table is displayed.
2. Click the **Add** button.
The Cardholders details pane is displayed with a series of tabs. See [Cardholders Tabs](#) for more information.
3. Enter the settings in the various tabs.
4. Click **Save** to keep the settings.
 - Click **Cancel** to clear the values.

13.4.2.2 EDIT CARDHOLDERS

1. Select **Configuration > Identity > Cardholders** from the Main Menu.
The *Cardholders* table is displayed.
2. Click an entry in Cardholders table.
The settings for the selected Cardholder are displayed in the Cardholder Details tabs.
3. Edit the settings in the tabs.
4. Click **Save** to keep the settings.
 - Click **Cancel** to return to the previous settings.

13.4.2.3 DELETE CARDHOLDERS

1. Click its entry in the list.
2. Select the **Delete** button.
A confirmation dialog is displayed.
3. Click **Yes** to verify the deletion.
 - Click **Cancel** to close the dialog without deleting the access level.

13.4.3 Cardholders Tabs

Cardholder parameters are configured through a series of tabs.

- After configuring the fields, click **Save** to keep the settings.
 - Click **Cancel** to return the tab to its previous settings.

13.4.3.1 CARDHOLDERS: GENERAL TAB

The General tab includes identity-related information about the Cardholder.

- **Last Entry**: lists the date and time that the Cardholder last accessed doors monitored by the system.
- **Name**: the **First Name**, **Middle Name**, **Last Name**, **Preferred Name**, **Prefix** and **Suffix** for this Cardholder. The person's Preferred Name (nickname) is printed first on the person's badge.
- **Cardholder ID (Emp#)**: a unique number, and the *Primary Key* in the system, for this Cardholder. The system does not allow duplicates.
- **Cardholder Status**: the current status of this Cardholder is selected from the drop-down list.

Tip: the **Inactive** status is useful for preparing cards prior to activation. Later, Cardholder Status can be changed to **Active** when it comes time to print and distribute the card for the new Cardholder.

Important: Cardholder Status is applied globally and affects every card this person has assigned to them. **Active** is the only field whereby the cards can be active. All other fields disable access.

- **HR Cardholder Type**: a Human Resources category for this person is selected from the drop-down list, such as *employee*, *contractor*, *intern*, *temporary*, *student*, etc.
- **Cardholder Vehicle**: includes the **Type** (make and model), **Color**, and **License Plate** number of the Cardholder's vehicle, if desired.

13.4.3.2 CARDHOLDERS: CREDENTIALS TAB

The Credentials tab of the *Configuration > Identity > Cardholders* screen contains parameters for the security credentials and other details required for printing badges assigned to this Cardholder.

13.4.3.2.1 Cardholders: Credentials Parameters

- **PIN:** a number (1 to 5 digits long) entered in keypads to access doors in the system that are controlled by readers configured to use keypads. See *Primary Credential in Reader Details* and *Configuration > Access Control > Readers > General >Reader Mode* for more information.
Reader/keypad combinations are currently supported in Sargent and Mercury configurations.
- **Import Photo:** brings up a file browser used to locate and load a JPEG photo of this Cardholder. The recommended size is 320px high x 240px wide, with a preferred resolution of 300 dpi.
- **Print Badge:** prints the selected card to a supported badge printer. You can drag the border around the photo to center it properly.

CARDS LIST

One or multiple cards can be configured for each Cardholder:

Note: However, only one card can be active at a time for a user.

- Click an existing card in the **Cards** list to add another card (credential) to the selected Cardholder.
- Click the plus (+) below the **Cards** list box to add a new card to the selected Cardholder.

CARD DETAILS

When a card is selected in the **Cards** list, the following parameters are displayed in the *Card Details* pane:

- **Badge Profile Name:** a Badge Profile is selected from the list upon which cards are based for this Cardholder. At least one Badge Profile must exist and be selected in the Cardholders screens, before any card can be created or edited for this Cardholder.
- **Card Number:** the internal proximity number of the card. This number is entered by typing the number manually, or by swiping the card through an OmniKey reader. See *Automatic Input with OmniKey Readers* for more information.
- **Embossed Number:** the number that is printed on the outside of the credential. It may or may not match the internal number.
- **Card Status:** the status of this *individual card*, not the Cardholder: **Active**, **Inactive**, **Returned**, **Lost**, and **Damaged**. When this value is set to **Active**, the card can be used to open doors according to the access level assigned to it in the **Cardholders: Access Levels Tab**. All other designations disable the card.

Note: A cardholder may be active in the system and have deactivated cards.

- **Activation Date:** sets the date on which this card become active.

- **Deactivation Date:** the Badge Profile sets the default deactivation date when this card automatically becomes inactive. The default date can be overridden here, such as for temporary employees hired for varying times.

AUTOMATIC INPUT WITH OMNIKEY READERS

Since card numbers are not always printed on physical access control cards, the Omnikey reader may be used to enter the Card Number in the **Card Details** screen.

Note: Separate OmniKey reader models are available for both Prox and iCLASS.

This procedure can only be run on PCs with a Windows operating system:

1. Install the OmniKey Reader:
 - a. Download the OmniKey Reader software from NLSS.com.
 - b. Plug the OmniKey Reader into an available USB port on the same Windows PC where the configurations are being done.
 - c. Run the OmniKey Reader software on the Windows PC to which the device is attached. Follow the instructions on the screen to complete installation.
2. Select **Configuration > Identity > Cardholders** from the Main Menu.
3. Open the **Cardholders: Credentials Tab** in the *Cardholder Details* pane.
4. In the **Credentials** tab, click the plus (+) under the **Cards List** field. The **Card Details** fields are displayed.
5. Select an existing **Badge Profile Name**.
6. Swipe the card in the installed card reader. The card number is entered automatically in the Card Numbers field.
7. Filling in the remaining fields in the **Cardholders: Credentials Tab**.
8. Click **Save** to keep the changes.
 - Click **Cancel** to restore the previous settings.

13.4.3.3 CARDHOLDERS: ACCESS LEVELS TAB

An Access Level consists of one or more specific doors associated with schedules. Access Levels are configured in the *Configuration > Identify > Access Levels* screen, and then assigned to Cardholders in the Access Levels tab of the Cardholders screen.

See **Configure Access Levels** for more information.

The Access Levels tab of the Cardholder screen contains two fields.

- The left field lists all access levels that are already configured.
- The right field lists all access levels currently assigned to the selected Cardholder.

Note: If a cardholder has multiple cards, the cards all have the same access levels, because only one card can be active per cardholder.

In the following instructions, the selected Cardholder may have inherited a default access level from the Badge Profile assigned to that Cardholder in the **Cardholders: Credentials Tab**. The default assignments can be overridden during this procedure.

1. Select **Configuration > Identify > Cardholders** from the Main Menu.
The *Cardholders* table is displayed.
2. Click an entry in Cardholders table.
The *Cardholder Details* pane is displayed.
3. Open the **Access Levels** tab.
4. Select an access level in the right column.
5. Click the right arrow button (>) to move the access level to the assigned (left) column.
 - Remove access levels from the assigned list by selecting them and clicking the left arrow button (<).
6. Click **Save** to keep the changes.
 - Click **Cancel** to restore the previous settings.

13.4.3.4 CARDHOLDERS: CONTACTS TAB

The Contacts tab of the *Configuration > Identity > Cardholders* screen provides a place to store the contact information of the Cardholder being configured.

The Contacts tab contains three parameters.

- **Email Address:** from the drop-down list in the Type column, select the type of address (**Home** or **Work**). In the Address column, enter the email address of this Cardholder. Repeat for additional email addresses.
- **Phone Numbers:** from the drop-down list in the Type column, select the type of phone (**Home**, **Work**, **Mobile**). In the Number column, enter the phone number of this Cardholder. Repeat for additional numbers.
- **SMS:** in the Number column, enter the SMS number for sending text messages to this Cardholder. Repeat for additional numbers.

To add an entry:

1. Click the plus (+) next to a column.
2. Enter the data.
 - Select a **Type** from the drop-down list for **Email Address** and **Phone Numbers**.
 - Enter the **Address** or **Number** in the text box in the column.
3. Click **Save** to keep the changes.
 - Click **Cancel** to restore the previous settings.

13.4.3.5 CARDHOLDERS: ORGANIZATIONAL TAB

The Organizational tab of the *Configuration > Identity > Cardholders* screen contains four parameters for saving organizational information related to this Cardholder. Some of these parameters are used to populate the *Operations > Cardholders* screen for the selected Cardholder.

- **Location:** the address of the site where the Cardholder is based.
- **Cardholder Department:** the department the Cardholder is part of.
- **Cardholder Supervisor:** the name of the Supervisor for this Cardholder.
- **Cardholder Title:** the job title of this Cardholder.

13.4.3.6 CARDHOLDERS: USER DEFINED TAB

Fields with user-defined (custom) names appear in the User Defined tab of the Cardholder configuration screen. The names of these fields are defined in the *Configuration > Identity > Cardholder-UserDefined* screen.

1. Create the User Defined labels for the custom fields. See [Configure Cardholder-User Defined Field Labels](#).
2. In the **User Defined** tab of the Cardholders configuration screen, enter values in the fields created in step 1. Not all the fields must have settings.
 - 5 text fields (for plain text)
 - 5 numeric fields (for numbers only)
 - 5 date fields (for dates only)
 - 5 boolean fields (for true/false values)
3. Click **Save** to keep the changes.
 - Click **Cancel** to restore the previous settings.

13.4.3.7 CARDHOLDERS: OPTIONS TAB

The Options tab of the *Configuration > Identity > Cardholders* screen includes three miscellaneous options.

- **ADA:** the ADA flag is used to allow extra time for this Cardholder to get through doors. The Cardholder may be physically challenged or have a special need, such as employees at loading docks and mail rooms.
Setting Notes:
 - The default values for extended ADA times are defined in the [Controller Details: General Tab](#) screen.
 - In the Controllers Details screen, the **DHO Time** is the time (in seconds) that a normally closed door can be held open before activating an alarm.
 - **Strike Time** is the time (in seconds) that a normally locked door stays unlocked after receiving an unlock signal.
- **Enable Trace:** if enabled, all access attempts of this Cardholder (successful or not) are to be tagged as *trace* events, even if the Event Filter is masked.
- **Notes:** Optionally add comments.

13.5 CONFIGURE CARDHOLDER-USER DEFINED FIELD LABELS

In the *Configuration > Identity > Cardholder–User Defined* screen, you can assign custom names to fields that appear in the User Defined tab of the Cardholders screen. See [Cardholders: User Defined Tab](#).

Examples of custom fields are:

- **Text:** emergency contact person
- **Number:** Social Security Number; Driver's License
- **Date:** birth date
- **Boolean:** telecommuter yes/no

13.5.1 User Defined: Parameters

The following types of fields are available in the *Cardholder - User Defined* screen:

- **Text fields:** use these fields for a combination of text and numbers.
- **Number fields:** use these fields for numbers.
- **Date fields:** use these fields for dates.
- **Boolean fields:** use these fields for true/false values.

13.5.2 User Defined: Actions

1. Select **Configuration > Identity > Cardholder–User Defined** from the Main Menu.
The *Cardholder-User Defined* screen is displayed.
2. Enter custom field names as desired.
3. Click **Save** to keep the changes.
 - Click **Cancel** to restore the previous settings.

13.6 CONFIGURE USERS

This section describes how to configure Users of the NLSS Unified Security Suite software so that they can log into the NLSS Web Interface controlling your security system.

13.6.1 Users Table

Select **Configuration > Identity > Users** from the Main Menu. The *Users* screen is displayed with a table listing the Users and a pane containing User Details.

Click the column headers to sort the list.

See [Searching Tables](#) for search instructions.

13.6.2 User Details

- **Name:** the **First Name**, **Middle Name**, **Last Name**, and **Preferred Name** of this user.
- **User ID (email):** a unique email address to identify this User. The User enters this ID into the User Name field of the login page of the NLSS Web Interface.
- **Password:** a password for this User. The User enters this password into the Password field on the login page of the NLSS Web Interface.

Important: The default password for the *Superuser* MUST be customized when your NLSS system is initially installed, or very soon thereafter, to close a hole in your security system.

- **User Type (Role):** select a role for this user:
 - **Superuser:** the Superuser role has unlimited permissions. Superusers can create, delete, and modify everything in the system.
 - **Operator:** Users assigned the Operator role have permissions to access everything under the Operations menu, the Events menu, and the Local Display menu, but cannot access the Configurations menu. Operators can operate the system but cannot configure it.

Important: The default password for the Superuser is also **Superuser**. Similarly, the default password for the Operator is **Operator**. These default passwords should be changed to prevent unauthorized access, as explained in [Edit Users](#).

13.6.3 Users: Actions

The *Configuration > Identity > Users* provides three options:

- [Create New Users](#)
- [Edit Users](#)
- [Delete Users](#)

13.6.3.1 CREATE NEW USERS

1. Select **Configuration > Identity > Users** from the Main Menu.
The *Users* table is displayed.
2. Click the **Add** button.
The *User Details* pane is displayed.
3. Select values for **User Details**.
4. Click **Save** to keep the settings.
 - Click **Cancel** to clear the values.

13.6.3.2 EDIT USERS

1. Select **Configuration > Identity > Users** from the Main Menu.
The *Users* table is displayed.
2. Select a User from the table.
The *User Details* pane is displayed.
3. Edit the **User Details** as needed.
For example, change the default passwords of the Superuser and Operator accounts, to prevent unauthorized access.
 - a. In the Users table, select the User from the list with *superuser* and nothing else in the User ID (email) column of the table. The parameters for this User appears in the *User Details* pane.
 - b. Enter a valid email address for the **User ID (email)**. This address must be unique in the system.
 - c. Enter a new **Password** for the Superuser and verify it. Keep the new password safe from theft or loss!
 - d. Select **Super** from the *User Type (Role)* drop-down list.
4. Click **Save** to keep the settings.
 - Click **Cancel** to return to the previous settings.

13.6.3.3 DELETE USERS

1. Select **Configuration > Identity > Users** from the Main Menu.
The *Users* table is displayed.
2. Select an entry from the User table.
3. Click the **Delete** button.
A confirmation dialog is displayed.
4. Click **Yes** to verify the deletion.
 - Click **Cancel** to close the dialog without deleting the user.

Note: Superuser *cannot* be deleted. Operators can be deleted.

Chapter 14: Configure Access Control

When a Cardholder presents an access card to a card reader at a door controlled by the NLSS Unified Security Platform, data flows from the reader to a reader interface; then from the reader interface to the controller to which it is attached, either internally or externally; then from the controller to the NLSS Gateway at the site. The NLSS Unified Security Suite running on that NLSS Gateway provides the interface to configure whether or not to unlock a given the door each time a card is swiped.

Because of these dependencies, most access control devices must be configured in the opposite order as the flow of information from swiped badges.

1. [Configure Controllers](#)
2. [Configure Reader Interfaces](#)
3. [Configure Readers](#)
4. [Configure Doors](#)
5. [Configure I/O Interfaces](#)
6. [Configure I/O Linkages](#)

14.1 ADDING, EDITING AND DELETING ITEMS

Items under the **Configuration > Access** menu options can be added, edited and deleted, unless otherwise noted. The steps for each of these procedures are basically the same.

14.1.1 Adding Items

An item can be added manually, if necessary.

1. Select **Configuration > Access Control > option** from the Main Menu, where *option* is the Access Control menu choice, such as Access Level, Cardholders, etc.
The table for that option is displayed listing the current items. If no items have been added, then the list is empty.
2. Click the **Add** button in the lower right corner under the table.
The *Details* for that item are displayed in the bottom pane.
3. Complete the Details fields for the item. The fields are described in the Details section for each item. Most Details panes contain multiple tabs.
4. Click **Save** to keep the settings.
 - Click **Cancel** to clear the fields, and revert to the default settings, if any.

14.1.1.1 EDIT ITEMS

Settings for an item can be edited in its *Details* pane.

1. Select **Configuration > Access Control > option** from the Main Menu, where *option* is the Access Control menu choice, such as Access Level, Cardholders, etc.
2. Select an item from the table.
The item's *Details* are displayed in the bottom pane.
3. Edit the Details fields, as needed.
4. Click **Save** to keep the changes.
 - Click **Cancel** to return to the previous settings.

14.1.1.2 DELETE READERS

1. Select **Configuration > Access Control > option** from the Main Menu, where *option* is the Access Control menu choice, such as Access Level, Cardholders, etc.
2. Select an item from the table.
The item's *Details* are displayed in the bottom pane.
3. Click the **Delete** button.
A confirmation dialog is displayed.
4. Click **Yes** to verify the deletion.
 - Click **Cancel** to close the dialog without deleting the item.

Important: To remove a device from service without removing its record, select **Out of Service** for the Administrative state in the Details pane's General tab. Save the change.

14.2 CONFIGURE CONTROLLERS

Each controller needs to be associated with an NLSS Gateway.

Note: Each controller can be associated with only one NLSS Gateway.

The NLSS system automatically discovers Mercury controllers when attached to a network shared by at least one NLSS Gateway.

HID and Assa Abloy controllers must be pointed to the NLSS Gateway. Follow the manufacturer's instructions to configure them from their own user interfaces. Those interfaces include fields to target the IP address of the NLSS Gateway to be associated with the controller.

When these pre-configured controllers are attached to a network shared by the NLSS Gateway, the controllers and Gateway discover each other.

Another difference between Mercury, HID, and Assa Abloy controllers:

- Different models of Mercury controllers vary in the number of reader interfaces and other I/O devices that a single controller can support, but most of them support at least one external reader.

- Assa Abloy controllers typically embed reader interfaces and readers in their controllers.
- HID offers some controllers that do the same, and other controllers that embed reader interfaces. The NLSS system supports all these combinations.

Controllers are configured from the *Controllers* screen in the NLSS Web Interface.

1. Select **Configuration > Access Control > Controllers** from the Main Menu.
The *Controllers* screen is displayed with a table listing the controllers in the system.
2. Click the column headers to sort the list.
Controller items can be added, edited, searched and deleted.
 - See [Adding, Editing and Deleting Items](#).
 - See [Searching Tables](#) for search instructions.

14.2.1 Associating a Mercury Controller with an NLSS Gateway

To prevent multiple NLSS Gateways from competing over a Mercury controller, one Gateway must be configured attach to that controller. These steps are also required for Mercury controllers if only one Gateway is in the system.

1. Log into the NLSS Web Interface for the NLSS Gateway to be associated with a Mercury controller.
2. Select **Configuration > Access Control > Controllers** from the Main Menu.
The *Controllers* screen is displayed with a table listing the controllers in the system.
After the NLSS Gateway discovers this Mercury controller, the Controller table lists the controller with an **Administrative State of Preprovisioned**.
3. Select the controller from the list.
4. Enter a unique name in the **Access Controller Name** field.
5. Select an NLSS Gateway from the **Gateway Name** drop-down list.
6. Check **Attach to Gateway** to complete the association of the controller with this NLSS Gateway.
7. Complete the controller's remaining parameters in the [Controller Details](#) pane, as needed. Most of the fields are populated when the controller is discovered by the Gateway.
8. Click **Save** to keep the changes.
 - Click **Cancel** to return to the previous settings.Attaching to the controller takes about five minutes.
An event message is displayed showing that the Mercury Controller is on-line and is ready to be placed *In Service*.
9. After the controller is attached to the Gateway, return to the *Controllers Details* pane and select **In Service** from the **Administrative State** drop-down list.
10. Click **Save** to keep the changes.
 - Click **Cancel** to return to the previous setting.

14.2.2 Controller Details

The *Controller Details* pane contains two tabs: **General** and **Diagnostics**.

14.2.2.1 CONTROLLER DETAILS: GENERAL TAB

When an NLSS Gateway discovers an access controller, the Gateway automatically populates most of the fields in this tab. Some of these fields can be customized, but most are read-only.

Note: Certain fields in this pane are displayed or hidden, depending on the Controller Type selected.

- **Access Controller Name:** enter a user-friendly name for this controller. The name must be unique in the system.
- **Gateway Name:** a drop-down list to select a pre-configured NLSS Gateway to associate with this access controller.
- **Access Controller Type:** (read-only when editing) When adding an access controller, this drop-down list contains the six controllers supported by the system:
 - Assa Abloy/Sargent v.S1 includes a controller, integrated reader interface, and PoE lock.
 - Assa Abloy/Sargent v.S2 includes a controller, integrated reader interface, and wireless lock.
 - HID Edge (ERP40) is for internal use. It includes the controller and integrated multi-CLASS or iCLASS technologies for access cards.
 - HID Edge+ (E400) is for internal or external use. It includes the controller and uses a separate external reader.
 - Mercury EP1501 is a one door controller which supports 16 downstream MR51e reader interfaces, for a total of 17 doors.
 - Mercury EP1502 is a two door controller that supports a total of 64 doors. It also supports up to 31 downstream boards that include any combination of MR50, MR52, MR16-In, and MR16-Out boards.

Note: Assa Abloy and HID systems *do not* physically have Reader Interfaces modules, but programming is required. See the system's documentation for instructions.

Mercury systems workflow is as follows:

- » 1st program the Controller
- » 2nd program the Reader Interface
- » 3rd program the Reader
- **Description:** optionally enter a description for this controller, such as its physical location, or any information that would be helpful to system Users.
- **Administrative State:** from this list, select **In Service** to make the controller active.
- **IP Address:** shows the numeric IP address of this controller. Do not change this value in this screen. Example: 10.11.11.210.
- **MAC Address:** (read-only) the MAC address of this controller, for example—f8:1e:df:d7:2a:5d.

- **Attach to Gateway:** this check box is only displayed for Mercury controllers. See [Associating a Mercury Controller with an NLSS Gateway](#) for instructions on attaching a Mercury Controller.
This check box is not displayed for Assa Abloy or HID controllers as the association cannot be changed between one of these controllers and a specific NLSS Gateway.
- **Username:** the username required to access the controller.
- **Password:** the password required to access the controller.
- **DHO Time Default:** enter the default time—in seconds—that a door can be held open until an alarm activates. Individual doors optionally can override this default.
- **Extended DHO Timeout:** enter the default time—in seconds—that a door can be held open by a Cardholder with ADA enabled, until an alarm activates.
 - *ADA* stands for *American Disabilities Association*. Enabling ADA is done typically for Cardholders with disabilities, or who otherwise need to hold doors open for a longer time, such as a loading dock or a mail room employee.
 - You can enable ADA in the [Cardholders: Options Tab](#).
- **Strike Time Default:** the default time—in seconds—that a locked door stays unlocked after receiving an unlock signal. Doors optionally can override this default.
- **Extended Strike Time:** the default time—in seconds—that a locked door stays unlocked by a Cardholder with ADA enabled. Both Strike Time and the DHO Time typically increase when ADA is enabled. For details on ADA, see the **Extended DHO Timeout** parameter.
- **System Contact:** optionally enter the name of your installer or system manager.
- **ASSA Call In Frequency:** the elapsed time—in minutes—that the wireless Assa Abloy locks call in to the NLSS Gateway for updates. The default setting is **1440** minutes, which is once a day.
- **Baud Rate:** from the list, select the rate of data transfer—in bits per second—between the controller and the reader interface or I/O module attached to it. The default setting is **38400**.
- **Installer:** the name of the person or company that installed this controller.
- **Install Date:** the date this controller was installed (for warranty purposes).

14.2.2.2 CONTROLLER DETAILS: DIAGNOSTICS TAB

Four read-only parameters are displayed in the Controller Diagnostics tab. Not all controllers send the same data, so the parameters vary, depending on the controller.

- **Hardware Version:** the version of the controller, such as *HW000.1A*.
- **Firmware Revision:** the version of the operating system for the controller, such as *FW.0001A*.
- **Firmware Release Date:** the date the operating system of the controller was released, such as *1/1/2011*.
- **Serial Number:** the serial number of the controller, such as *W89511QV66E*.

14.3 CONFIGURE READER INTERFACES

When a reader interface is attached to a controller that is already installed in the system, the system discovers that reader interface—as well as the readers and doors connected to it. The main exception is the Mercury MR51e, which must be added manually.

The configuration of Mercury reader interfaces can be edited, but not HID or Assa Abloy reader interfaces. The latter two interfaces are built into the controller and do not support external reader interfaces.

Reader Interfaces are configured from the *Reader Interfaces* screen in the NLSS Web Interface.

1. Select **Configuration > Access Control > Reader Interfaces** from the Main Menu.
The *Readers* screen is displayed with a table listing the Reader Interfaces in the system.
2. Click the column headers to sort the list.
Reader Interface items can be added, edited, searched and deleted.
 - See [Adding, Editing and Deleting Items](#).
 - See [Searching Tables](#) for search instructions.

14.3.1 Reader Interface Details

1. Select **Configuration > Access Control > Reader Interfaces** from the Main Menu.
The *Reader Interfaces* screen is displayed with a table listing the Reader Interfaces in the system.
2. Click on a Reader Interface to select it.
The *Reader Interface Details* pane is displayed.

Fields in the **General** tab pertain to all reader interfaces. The **Aux Input** and **Aux Output** tabs correspond to physical ports on the Reader Interface being configured.

Note: Controllers and I/O Boards also have Aux In and Aux Out ports.

14.3.1.1 READER INTERFACES DETAILS: GENERAL TAB

These parameters are applicable to Mercury reader interfaces only. Also, not all parameters are used by all Mercury controllers.

- **Reader Interface Name:** a unique, user-defined field used to provide a user-friendly label for the reader interface in the system.
- **Reader Interface Type:** a drop-down list of pre-configured values, only displayed when programming Mercury Controllers.
 - **Mercury MR50**—1 door (RS485)
 - **Mercury MR51e**—1 door (PoE)
 - **Mercury MR52**—2 door (RS485)
 - **Mercury EP1501 RI**—1 door (on-board)
 - **Mercury EP1502 RI**—2 door (on-board)

- **Access Controller Name:** a list of installed access controllers. A controller is selected to associate with this reader interface.
- **Description:** (Informational) optionally describe this reader interface.
- **RS485 Address:** a unique address used for Mercury devices that defines the connection address with the controller. Values are 0-31.

Important: The correct number must be in this field for the reader interface to be recognized. The *correct* number corresponds to the address that is manually set by switches on the controller of the reader interface being configured. After you set these switches, then the controller automatically reads the address. Note which address on the controller corresponds with which reader interface.

- **IP Address:** (for MR51e only) The IP address of this reader interface, such as *10.11.11.210*.
- **MAC Address:** (for MR51e only) The MAC address of this reader interface, such as *f8:1e:df:d7:2a:5d*.
- **Installer:** the name of the person or system integrator who installed this reader interface.
- **Install Date:** the date this reader interface was installed.

Notes:

HID Edge Controllers have two supervised inputs and two outputs:

- Input 1 is dedicated to the Door Contact.
- Input 2 is dedicated to the REX.
- Output 1 is dedicated to the Strike
- Output 2 is spare.

EP1502 Controllers have eight supervised inputs and 4 outputs:

- Inputs 1 and 3 are dedicated to the Door Contact for doors 1 & 2, respectively.
- Inputs 2 and 4 are dedicated to the REX for doors 1 & 2, respectively.
- Inputs 5, 6 and 7, 8 are the spares for doors 1 & 2, respectively.
- Outputs 1 and 2 are dedicated to the Strike for doors 1 & 2, respectively.
- Outputs 3 and 4 are the spares for doors 1 & 2, respectively.

14.3.1.2 READER INTERFACES: AUX INPUT TAB

The Auxiliary Input and Output tabs for Mercury MR16IN and MR16OUT boards are used to attach external I/O devices. For example, an auxiliary input could come from a panel tamper detector or an door strike sensor. An output could activate a light or alarm, among other devices.

Use of auxiliary inputs and outputs is optional.

The auxiliary inputs depend on the type of reader interface being configured.

- **Input Number:** a list of I/O port numbers on the reader interface. Connect an input device to a port on the interface, and enter the Input Number corresponding to the port to which it is connected.
- **Input Name:** a unique name for the input.
- **Debounce:** the minimum time—in milliseconds—that must pass before an input signal qualifies as a real event. For example, if a door contact registers a door as *open* for only one millisecond, and then registers it as *closed* again, it is probably a false alarm.
- **Supervision:** select **Supervised** or **Unsupervised**. Supervised reader interfaces can detect a change of voltage indicative of a cut line.
- **Enabled:** select **Enabled** or **Disabled**. Select Enabled to process signals from the attached device.
- **Normal State:** a list of the possible default states of the inputs handled by this reader interface. Select **Open** or **Closed** to indicate whether the input device is normally open or closed.

14.3.1.2.1 Reader Interfaces: Inputs

The inputs vary between reader interfaces. Some supported reader interfaces are listed below.

- **Mercury MR50** has a supervised door contact sensor and a supervised REX sensor (REX means Request to Exit, which can take many forms such as a passive infrared or sensor on the exit hardware), but no spare inputs for general purposes.
- **Mercury MR51e** has 4 input relays for a single door.
 - Inputs 3 and 4 are spares for general purpose input.
 - Input 1 is for the Door Contact.
 - Input 2 is for the REX sensor.
- **Mercury MR52** has 8 general purpose input relays for 2 doors.
 - Inputs 5 and 6, 7, and 8 are spares (2 per door) for general purpose input.
 - Inputs 1 and 3 are for the door contacts, on doors 1 and 2 respectively.
 - Inputs 2 and 4 are for the REX inputs, on doors 1 and 2 respectively.

14.3.1.3 READER INTERFACES: AUX OUTPUT TAB

The auxiliary outputs depend on the type of reader interface being configured. These are the onboard Aux outputs on the MR50, MR51e and MR52.

- **Output Number:** a list of I/O port numbers on the reader interface. Connect an output device to a port on the reader interface, and enter the Output Number corresponding to the port to which the connection was made.
- **Output Name:** give this output device a unique name.
- **Enabled:** select **Enabled** to process communications signals through the selected port, or disable to pass to an attached device.

- **Normal State:** the default state of the output device that is being handled by this reader interface. Select **Normally Active** or **Normally Inactive**.

14.3.1.3.1 Reader Interfaces: Outputs

Aux Outputs are relays that can be used to control external devices. A typical application activates a siren or flashing light when a door is forced open.

- **Mercury MR50** has two General Purpose output relays for the single door.
 - Output 1 is dedicated for the Strike.
 - Output 2 is spare.
- **Mercury MR51e** has one General Purpose output relay for the single door.
 - Output 1 is dedicated for the Strike.
 - Output 2 is spare.
- **Mercury MR52** has six General Purpose output relays for both doors.
 - Outputs 1 and 2 are dedicated to the Strike for doors 1 & 2 respectively.
 - Outputs 3, 4 and 5, 6 are the spares for doors 1 & 2 respectively.

14.3.2 Reader Interfaces: Actions

When an NLSS Gateway and controller are first associated—either by the Gateway discovering the controllers such as Mercury controllers, or by the controller discovering the Gateway such as HID and Assa Abloy controllers—the Gateway automatically adds the reader interfaces, readers, and doors attached to the controller. Generally reader interfaces, readers, or doors do not need to be manually added to the system.

Note: The Mercury MR51e must be manually added to the system. This interface is generally used to expand EP1501 systems.

14.3.2.1 ADD READER INTERFACES MANUALLY

For the Mercury MR51e:

1. In the *Configuration > Access Control > Reader Interfaces* screen, select **Add** under the list of reader interfaces.
2. Fill in [Reader Interfaces Details: General Tab](#).
3. If you are connecting input/output devices (other than door readers) to this reader interface, then enter values for [Reader Interfaces: Aux Input Tab](#), and then [Reader Interfaces: Aux Output Tab](#).
4. Click **Save** to keep the settings.
 - Click **Cancel** to restore the previous settings.

14.3.2.2 DELETE READER INTERFACES

If a reader interface is physically removed from the system (directly or indirectly by removing the controller on which it is dependent), then the reader interface must be deleted from the software via the NLSS Web Interface.

1. In the *Configuration > Access Control > Reader Interfaces* screen, select the Reader Interface from the list.

2. Click the **Delete** button.
A confirmation dialog is displayed.
3. Click **Yes** to verify the deletion.
 - Click **Cancel** to close the dialog without deleting the Reader Interface.

14.4 CONFIGURE READERS

Each reader in a system typically needs to be associated with a reader interface, or with a controller if the controller is using an embedded reader interface.

1. Select **Configuration > Access Control > Readers** from the Main Menu.
The *Readers* screen is displayed with a table listing the readers in the system.
2. Click the column headers to sort the list.
Reader items can be added, edited, searched and deleted.
 - See [Adding, Editing and Deleting Items](#).
 - See [Searching Tables](#) for search instructions.

14.4.1 Reader Details

1. Select **Configuration > Access Control > Readers** from the Main Menu.
The *Readers* screen is displayed with a table listing the readers in the system.
2. Click on a reader to select it.

The *Reader Details* pane is displayed.

- **Reader Name:** a unique name entered to identify this reader.
- **Reader Interface Name:** a drop-down list of discovered and configured reader interfaces.
- **Access Controller Name:** a drop-down list of installed and configured access controllers.
- **Description:** (Informational) optional description of this reader.
- **Reader Style:** (Informational) an optional drop-down list from which the style of this reader is selected.
 - **Mullion**
 - **Switchplate**
 - **Mini-Reader**
- **Reader Type:** the type of reader determines the options available for **Reader Mode**. Reader Type has three options.
 - **Prox**
 - **Prox + Keypad**
 - **iCLASS**

- **Reader Supported Format:** (Informational) a drop-down list of possible data formats. Wiegand is the only supported format for now.
 - **Reader Mode:** a drop-down list of the input types accepted by this reader. The exact options depend on the Reader Type:
 - **Card Only:** requires a card, but does not accept a PIN code.
 - **Card + PIN:** requires both a card and a PIN.
Whether the Card or the PIN needs to be entered first depends on the *Primary Credential* set in the **Cardholders: Credentials Tab** of the selected Cardholder.
 - **PIN only:** a PIN is required. The reader does not accept a card.
 - **Card / PIN:** the Reader requires either a card *or* a PIN.
 - **Facility Code:** only cards with the correct facility code can access doors at the facility, via swiping.
 - **Locked:** keeps a door locked at all times, ignoring all cards and PINs.
 - **Unlocked:** keeps the door unlocked at all times.
 - **Reader Model:** (Informational) optional. Enter the reader's model number.
 - **Reader Interface Port:** a drop-down list from which a port number is selected to identify where the reader is physically connected to its parent reader interface or controller.
- Note:** This specific selection is based on the system design.
- **Installer:** (Informational) optional text field to enter the name of person or system integrator who installed the reader.
 - **Install Date:** (Informational) optional field to enter the date this reader was installed. Click on the **Calendar** button to select a date.

14.4.2 Readers: Actions

When a Controller/Reader Interface is added to a system, the Readers table is automatically populated in the *Configuration > Access Control > Readers* screen. Readers can be added or deleted, and the **Reader Details** can be edited. See **Adding, Editing and Deleting Items**.

Note: If a reader is physically removed from the system, it must be deleted from the software via the NLSS Web Interface.

14.5 CONFIGURE DOORS

The system discovers doors automatically when the associated readers, reader interfaces, and controllers are connected to the system.

1. Select **Configuration > Access Control > Doors** from the Main Menu.
The *Doors* screen is displayed with a table listing the Doors in the system, and the **Door Details**, which can be edited.
2. Click the column headers to sort the list.
Doors can be added, edited, searched and deleted.
 - See **Adding, Editing and Deleting Items**.
 - See **Searching Tables** for search instructions.

Notes:

- Configure schedules in the **Configure Schedules** screen *before* associating schedules with doors or other items in the system that uses schedules.
- Holidays can override schedules associated with doors. See **Configure Holidays**.

14.5.1 Door Details

1. Select **Configuration > Access Control > Doors** from the Main Menu.
The *Doors* table is displayed.
2. Click on a Door to select it.

The *Door Details* are displayed in the bottom pane, with two tabs: **General** and **Strike**.

14.5.1.1 DOOR DETAILS: GENERAL TAB

- **Door Name:** a unique name entered to identify the door.
- **Door Type:** (Informational) an optional drop-down list of available types of doors, including **glass**, **solid wood**, **hollow metal**, **store front** and **fire door**.
- **Reader Name:** a drop-down list of readers available in the system. From the list, select the reader that is physically associated with this door.
- **Description:** optional text box to enter a description of this door, such as its location.
- **Auto Unlock Schedule:** a drop-down list of configured schedules. See **Configure Schedules** for more information.
- **Door Contact Mode:** a drop-down list to select whether the door is **Normally Open** or **Normally Closed**.
- **REX Type:** (Informational) a drop-down list of available devices for sending a *Request to Exit* to the system to unlock the door. (Locking people inside is typically against fire laws; REX makes it possible for people to exit regardless of their Cardholder access.) Options include **Crash Bar**, **Push Button**, and **Motion Sensor**.

- **REX Mode:** the normal (default) state of a Request to Exit device on this door, either is **Normally Open** or **Normally Closed**.
- **DHO Time Override (Sec):** select a value only to override the default DHO value set in the [Configure Controllers](#) screen.

Note: DHO is an acronym for *door held open*.

- **REX Time (Sec):** the time (in seconds) a door can be opened, after receiving a Request to Exit, without triggering a *Door Forced Open* event.
- **Installer:** (Informational) optional text field to enter the person who installed the door lock.
- **Install Date:** (Informational) optional field to enter the date this door lock was installed. Click on the **Calendar** button to select a date.

14.5.1.2 DOORS DETAILS: STRIKE TAB

Strike parameters pertain to the locking mechanism of the door:

- **Lock Type:** (Informational) a drop-down list for the type of lock used on this door, such as **Mag Lock**, **Electric Lockset**, etc.
- **Lock Voltage:** (Informational) a drop-down list of the voltages used on the lock, either **12v DC** or **24v DC**.
- **Strike Time Override:** provides the option to override the **Strike Time Default** set in the [Configure Controllers](#) screen. *Strike Time* is the time, in seconds, that a door remains unlocked after receiving an unlock signal.

14.5.2 Doors: Actions

When a Controller/Reader Interface is added to a system, the Doors table is automatically populated in the *Configuration > Access Control > Doors* screen. Doors can be added or deleted, and the [Door Details](#) can be edited.

If a door is physically removed from the system, then it must be deleted from the software via the NLSS Web Interface. A door can be removed directly or indirectly by removing a reader or other hardware on which the door is dependent.

See [Adding, Editing and Deleting Items](#) for instructions.

14.6 CONFIGURE I/O INTERFACES

I/O Interfaces boards extend the input and output capabilities of a controller. Mercury-based systems can be configured with multiple MR16 input and output interface boards. The MR16In allows 16 inputs and 2 outputs while the MR16Out has no inputs and allows 16 outputs.

Some Mercury reader interfaces have extra inputs/outputs for general purpose use. Configuration of these I/O interfaces varies, based on the capabilities of the parent controller, as well as the specific I/O device. The instructions in this section are generalized for most cases.

1. Select **Configuration > Access Control > I/O Interfaces** from the Main Menu.
The *I/O Interfaces* screen is displayed with a table listing the I/O Interfaces found in the system.
2. Click the column headers to sort the list.
I/O Interface items can be added, edited, searched and deleted.
 - See [Adding, Editing and Deleting Items](#).
 - See [Searching Tables](#) for search instructions.

14.6.1 I/O Interface Details

1. Select **Configuration > Access Control > I/O Interfaces** from the Main Menu.
The *I/O Interfaces* table is displayed.
2. Click on an I/O Interface to select it.

The *I/O Interface Details* are displayed in the bottom pane, with general parameters plus two tabs: **Aux Input** and **Aux Output**.

14.6.1.1 I/O INTERFACES: GENERAL PARAMETERS

- **IO Interface Name:** a unique name entered to identify this I/O board.
- **IO Interface Type:** a drop-down list to select the type of I/O board being configured. For example, the Mercury 1502 controller supports the Mercury MR16IN and MR16OUT boards.
- **Access Controller Name:** a drop-down list to select the controller to which the I/O board is attached. The list contains the of installed controllers.
- **RS485 Address:** the RS485 address of the controller port to which the I/O board is physically connected. The range of valid addresses depends on the controller. For the Mercury EP1502 controller, the valid range of RS485 addresses is 0-31. The correct number must be entered, based on the system design.
- **Description:** an optional text field to add a description of this I/O board.
- **Installer:** the name of the person or system integrator who installed this device.
- **Install Date:** the date on which this device was installed (for warranty purposes).

Note: Click **Save** to keep any changes to general parameters before continuing to the Aux Input or Aux Output tabs. **Cancel** resets the fields to their previous settings.

14.6.1.2 I/O INTERFACE DETAILS: AUX INPUT TAB

The Auxiliary Input tab lists the available input points. When an input device is selected, the remaining fields in the tab are used to configure that input.

The **I/O Interfaces: General Parameters** must be configured and saved before the input settings are configured.

- **Input Devices Available:** a list of physical input ports on the selected I/O device. External devices can be connected to these ports. After a port is selected, the remaining fields can be configured for that port.
- **Input Port:** a text field identifying the port selected in the list of **Input Devices Available**.
- **Input Name:** a text field to give the selected input port a name that indicates the type of device to which it is connected, such as a panic button, motion sensor, etc.
- **Debounce:** the minimum time (in milliseconds) that must pass before an input signal from the attached device qualifies as a real event. For example, if a motion sensor detects movement for only one millisecond, then the motion is ignored as a false alarm.
- **Supervision:** a drop-down list with the options: **Supervised** or **Unsupervised**. Supervised I/O boards detect when a line is cut that affects that device.
- **Enabled:** a drop-down list that indicates whether this port is **Enabled** or **Disabled**. The system ignores inputs to disabled ports. A Disabled setting allows the port to be configured before going online. Select **Enabled** to process signals to the selected port.
- **Normal State:** a drop-down list to set the default state of the device connected to the selected port of the I/O board. **Normally Open** or **Normally Closed** indicates whether the input is normally on or off.

14.6.1.3 I/O INTERFACE DETAILS: AUX OUTPUT TAB

The Auxiliary Output tab lists the available output points. When an output device is selected, the remaining fields in the tab are used to configure that output.

- **Output Devices Available:** a list of physical output ports on the selected I/O device. After a port is selected, the remaining fields can be configured for that port.
- **Output Port:** a text field identifying the port selected in the list of **Output Devices Available**.
- **Output Name:** a text field to give the selected output port a name that indicates the type of device to which it is connected.
- **Output Duration:** length of time (in seconds) an output port changes state.
- **Enabled:** a drop-down list that indicates whether this port is **Enabled** or **Disabled**. The system ignores disabled ports. A Disabled setting allows the port to be configured before going online. Select **Enabled** to allow signals to be sent from the selected port.

- **Normal State:** a drop-down list of default state of the output device connected to the selected port. **Normally Active** or **Normally Inactive** indicates whether the output is normally on or off, respectively.

14.6.2 I/O Interfaces Actions

An I/O Interface can be added or deleted manually, if necessary. The Details fields can be edited. See [Adding, Editing and Deleting Items](#) for instructions.

14.7 CONFIGURE I/O LINKAGES

After [Configure I/O Interfaces](#) are configured, then specific input ports can be linked or associated with particular output ports on the same I/O board, or any other board with I/O inputs that is in your NLSS system. (Mercury makes dedicated I/O boards, as well as controllers and reader interfaces that include surplus I/O ports. See Mercury's documentation for details.)

Links between input and output ports are made from the NLSS Web Interface.

1. Select **Configuration > Access Control > I/O Linkages** from the Main Menu.
The *I/O Linkages* screen is displayed. The *I/O Linkages* screen is displayed with a table listing the I/O Linkage found in the system.
The table is empty until an I/O Linkage is created.
2. After items are added, click the column headers to sort the list.
I/O Interface items can be added, edited, searched and deleted.
 - See [Adding, Editing and Deleting Items](#).
 - See [Searching Tables](#) for search instructions.

Outputs generally follow inputs with which they are associated. For example, a motion detector can be connected to an input port on a dedicated Mercury I/O board in your system. Then a siren can be connected to an output port on a reader interface managed by the same NLSS Gateway. When the two devices are linked, a signal from the motion sensor triggers the siren.

When an NLSS system receives a signal on a managed input port, the system sends a signal to the linked output port during the Schedule selected with the applicable I/O Linkage rule. If the system detects an input outside this Schedule, then an output signal is *not* sent. The exception is camera events, because they do not use schedules. Camera events always apply.

I/O Linkages are configured after I/O Interfaces. See [Configure I/O Interfaces](#).

14.7.1 I/O Linkages Details

The I/O Linkage details contains four parameters.

- **Linkage Rule Name:** a unique name to help identify the link.
- **Schedule Name:** from the drop-down list, a schedule can be applied to the linkage. Schedules must be configured first. See [Configure Schedules](#).
- **Input Name:** a drop-down list of all input ports configured in the system. An input port is selected to serve as the *in* side of the linkage.
- **Output Name:** a drop-down list of all outputs ports configured in the system. An output port is selected to serve as the *out* side of the linkage.

14.7.2 I/O Linkages: Actions

I/O Linkages can be added, edited, searched and deleted.

- See [Adding, Editing and Deleting Items](#).
- See [Searching Tables](#) for search instructions.

Chapter 15: Configure Video, Storage, & Decoders

You should configure video cameras and related devices in the following order:

1. [Configure Cameras and Streams](#)
2. [Configure External Storage Devices](#)
3. [Configure External Storage Devices](#)

Cameras are controlled via the *Operations > Cameras* menu. See [Chapter 4: Controlling Cameras](#) for instructions on operating cameras.

15.1 CONFIGURE CAMERAS AND STREAMS

The parameters and actions documented in this section apply to the individual camera selected in the *Configuration > Video > Cameras* screen.

Dependencies:

- Schedules must be configured before associating schedules with cameras streams or anything else in the system that uses schedules. See [Configure Schedules](#).
- Holidays do NOT override schedules associated with cameras and other video streams, although Holidays do override schedules used by access control devices.

15.1.1 Cameras Table

The Cameras table provides an overview of each camera's status in the system. Items in the table can be added, configured, searched and deleted.

1. Select **Configuration > Video > Cameras** from the main menu.

The *Cameras* table is displayed

- Click on a column to sort the list.
- See [Searching Tables](#) for search instructions.

2. Select a camera from the table.

The *Camera Details* are displayed in the bottom pane. The Camera Details pane contains three tabs: **General**, **Stream** and **Recording**.

The General tab is available for all cameras and streams the system discovered on the network. The Stream and Recording tabs are available only for cameras with which the system has successfully connected.

15.1.2 Camera Details: General Tab

Discovering a camera does not guarantee the system is able to connect with that camera. The parameters in the General tab must be set properly for the system connect to the camera.

When you select a camera from the list in the Cameras configuration screen, a series of parameters appear in the General tab of the Camera Details screen even if the camera is not currently connected to the system.

15.1.2.1 EDITABLE PARAMETERS

- **Admin State:** a drop-down list of the possible operational states for the selected camera. Select a different state from the list to change the current operational state of the camera.
 - **Pre-Provisioned:** the system discovered this camera, but has not attempted to connect to it.
 - **In Service:** the system connected to (or is attempting to connect with) this camera. If the connection is successful, then the Stream and Recording tabs become available.
 - **Out Of Service:** the system is not connected to this camera. The lack of connection could be intentional, or the result of the failure to connect. The most common cause is an incorrect username or password for logging into this camera.
- **Username:** the user name for accessing this camera. The username is set on the camera itself, and then entered in this field so the system can receive the video stream from this camera.

Note: Not all cameras require the user name to be changed.

- **Password:** the password for accessing this camera. The password is set on the camera itself, and then entered in this field so the system can receive the video stream from this camera.
- **Device Name:** the system provides a default name, which it constructs from discovering this camera. This default name includes the model and IP address of the selected camera. The default name can be kept or customized in this field.
- **Device Location:** optional text field to enter the physical location of this camera.

15.1.2.1.1 Stream-only Parameters

If a stream is selected, additional fields must be configured.

- **Custom Stream Type:** a drop-down list with two options: RTSP and HTTP.
 - **RTSP:** applies to remote streams using the Real-Time Streaming Protocol.
 - **HTTP:** applies to remote streams running over HTTP.
- **Use Multicast:** (*RTSP only*) Enable for this stream to use multicast; disable to use unicast.
- **Stream URL:** Enter the URL of the source for the stream.

Important: Without the URL, the stream cannot be connected to the system.

Parameters for HTTP streams are the same as RTSP streams, except for the removal of the **Use Multicast** parameter.

15.1.2.2 READ-ONLY PARAMETERS

The values of these parameters are provided by the cameras and cannot be edited:

- **Device Model:** the make and model of this camera.
- **Connection State:** Displays *Connected* only if the system is able to process the video stream coming from this camera.
- **PTZ:** whether or not this camera is capable of pan, tilt, and zoom functions.
- **Serial Number:** the discovered serial number of this camera.
- **IP Address:** the IP address of this camera. Click on the IP address to directly access the camera's configuration.
- **Firmware Version:** the discovered firmware version running on this camera.
- **Hardware Version:** the discovered hardware version, if any, of this camera.
- **MAC Address:** the discovered MAC address of this camera.

15.1.3 Cameras: General Actions

The *Configuration > Video > Cameras* screen provides a series of options:

- [Connect with a Camera](#)
- [Edit Camera Details](#)
- [Add Cameras](#)
- [Add RTSP and HTTP Streams](#)

15.1.3.1 CONNECT WITH A CAMERA

1. Select **Configuration > Video > Cameras** from the Main Menu.
The *Cameras* table is displayed listing discovered cameras.
2. Select a camera from the table.
The *Camera Details* pane is displayed.
3. In the **General** tab, enter the **Username** and **Password** required to log into the camera.

Note: The NLSS system cannot control the user names and passwords of cameras. Consult the camera's manufacturer to determine its default user name and password, and for instructions on changing these values.

4. Change the **Admin State** to **InService**.

5. Click **Save**.

Give the connection a minute to be made. If the connection is successful, the Stream and Recordings tabs become available. If the connection is not completed, the system resets the camera to the *Out of Service* Admin State.

- Click **Cancel** to abort the configuration and reset the fields to the previous values.

15.1.3.2 EDIT CAMERA DETAILS

The writable fields under Camera Details can be changed, as needed.

1. Select **Configuration > Video > Cameras** from the Main Menu.
The *Cameras* table is displayed listing discovered cameras.
2. Select a camera from the table.
The *Camera Details* pane is displayed.
3. Edit the fields, as needed.
See [Camera Details: General Tab](#) for more information.
4. In the General tab, enter a name for the camera in the **Device Name** field.
5. Click **Save** to keep the settings.
 - Click **Cancel** to restore the previous settings.

15.1.3.3 ADD CAMERAS

When a new camera is installed on the network, it is added to the Camera table via the NLSS Discovery Utility.

Cameras cannot be added manually using the NLSS Web Interface, unless the camera is added as an RTSP stream. See [Add RTSP and HTTP Streams](#) for more information.

1. Physically install a new camera to the same network as the NLSS Gateway.
2. Run the **NLSS Discovery Utility** again.
 - a. Insert the supplied **NLSS Discovery Utility CD** into the computer's disc drive, or download the software from the NLSS web site (www.nlss.com).
 - b. Copy the **NLSS Discovery Utility** file to your computer's hard drive.
 - c. Launch the **NLSS Discovery Tool**.
 - d. In the *NLSS Device Discovery* screen, click **Scan**.
The system discovers the new camera and adds it to the list of discovered cameras in the system.
3. Connect the camera to the system. See [Connect with a Camera](#) for instructions.

15.1.3.3.1 Add RTSP and HTTP Streams

Generic RTSP and HTTP video streams can be added to the system. These streams behave much like cameras. RTSP also can be used to add some IP cameras that are otherwise unsupported by the system. The camera is added as a generic RTSP stream.

1. Select **Configuration > Video > Cameras** from the Main Menu.
The *Cameras* table is displayed listing discovered cameras.
2. Click **Add** to add a stream.

- The *Camera Details* pane is displayed.
3. Complete the fields in the **General** tab.
See [Camera Details: General Tab](#) for a description of the fields.
 4. Click **Save** to keep the settings.
 - Click **Cancel** to restore the previous settings.

15.1.4 Camera Details: Stream Tab

The Stream tab is available only after the system has successfully connected with a camera in the system. The Camera table lists the camera as **In Service**.

1. Select **Configuration > Video > Cameras** from the Main Menu.
The *Cameras* table is displayed.
2. Select a camera from the table.
The *Camera Details* pane is displayed.
3. Open the **Stream** tab.

The Stream tab contains three sections:

- [List of Streams](#)
- [Video Stream Parameters](#)
- [Audio Stream Parameters](#)

15.1.4.1 LIST OF STREAMS

Some cameras have multiple outputs, each with a different codec and/or resolution. For example: Stream0 and Stream 1. When a specific stream is selected, the Video Stream and Audio Stream fields update to match the selection.

15.1.4.2 VIDEO STREAM PARAMETERS

The displayed fields are dependent on the type of camera and stream. The system receives this data from the camera, so the fields are informational (read-only).

- **Video Codec Type:** the type of video codec used by this stream, such as H.264.
- **Frame Rate (fps):** frames per second of this video stream, such as 30.
- **Resolution Width:** the width (in pixels) of this video stream, such as 1920 pixels.
- **Resolution Height:** the height (in pixels) of this video stream, such as 1080 pixels.
- **Bit Rate Mode:** is either **CBR** (Constant Bit Rate) or **VBR** (Variable Bit Rate).
- **Bit Rate (Kb/s):** Video transfer rate (in kbits/s) between the camera and its Gateway.
- **VBR Quality:** if the Bit Rate Mode = VBR, then VBR Quality indicates how much compression is being used. This setting can be indicated by a percentage, or by a word like *low* or *high*.

- **VBR Upper Cap:** if the Bit Rate Mode of this camera is VBR, then VBR Upper Cap indicates the maximum amount of compression that can be applied.

15.1.4.3 AUDIO STREAM PARAMETERS

If a camera is capable of audio, then these read-only parameters are displayed.

- **Audio Codec:** the type of audio codec used by this stream, such as G.711.
- **Audio Sample Rate:** the sampling rate of audio, in kbits/s.
- **Audio Bit Rate:** transfer rate (in kbits/s) of audio data between the camera and Gateway.

15.1.4.4 CAMERAS: ENABLING A STREAM

Only selected streams in the Stream tab are available for viewing and recording, as discussed in [Monitor Cameras from the Operations Menu](#).

1. Check the box next to a Stream in the **Stream** tab.
 - To disable a stream, clear the check box.
2. Repeat step 1 for additional streams, if any.
3. Click **Save** to keep the settings.
 - Click **Cancel** to restore the previous settings.

Note: This setting must be saved before a stream can be configured for recording

15.1.5 Camera Details: Recording Tab

The Recording tab is available only after the system has successfully connected with a camera in the system. The Camera table lists the camera as **In Service**.

1. Select **Configuration > Video > Cameras** from the Main Menu.
The *Cameras* table is displayed.
2. Select a camera from the table.
The *Camera Details* pane is displayed.
3. Open the **Recordings** tab.

The Recording tab enables recording for a selected camera and its streams.

- [Stream Settings](#)
- [Camera Settings](#)

15.1.5.1 STREAM SETTINGS

If the selected camera outputs more than one stream, all available streams are listed under **Stream Settings**. A Schedule can be associated with a stream for recording, as long as that stream was enabled (checked) and the setting was saved in the Stream tab.

- **Stream:** Lists available streams being output from the selected camera.
- **Recording Schedule:** a drop-down list listing the Schedules configured for the system, such as **Never**, **Always**, etc. The selected Schedule is associated the selected stream.

See [Configure Schedules](#) for more information on Schedules.

15.1.5.2 CAMERA SETTINGS

These **Camera Settings** apply to all streams output by the selected camera.

Note: These settings override the default Groomer settings. See [Configure Groomer Settings](#).

- **Recording to Volume:** a drop-down list listing accessible storage devices on which camera recordings can be stored.
- **Min Retention (Days):** the minimum number of days a recording from the selected camera is saved on disc before being considered for auto-deletion by the Groomer.
- **Max Retention (Days):** the maximum number of days a recording from the selected camera is saved on disc before being auto-deleted by the Groomer.

15.1.5.3 CAMERAS: RECORDING CONFIGURATION

A Recording Schedule and Camera Settings must be set for a camera to be recorded.

15.1.5.3.1 Configure Stream Recording Schedule

After a stream is enabled in the Stream tab, a Schedule can be associated to the stream for recording.

1. Select a Stream under **Stream Settings** in the **Record** tab.
2. Select a **Recording Schedule** from the drop-down list.
3. Repeat this process for other streams, if desired.
4. Click **Save** to keep the settings.
 - Click **Cancel** to restore the previous settings.

15.1.5.3.2 Configure Camera Settings

The Camera Settings apply to all streams that have been configured to record.

1. From the **Record to Volume** drop-down list, select a location to store the recorded video.
 - The System Select option allows the Gateway to choose the location.
 - See [Configure External Storage Devices](#) for more information on adding external drives to the system.
2. Select **Min Retention** and **Max Retention**, as described in [Camera Settings](#).
3. Click **Save** to keep the settings.
 - Click **Cancel** to restore the previous settings.

15.2 CONFIGURE EXTERNAL STORAGE DEVICES

NLSS supports external storage connected both directly and via the network. Direct connection storage devices are discovered and displayed automatically in the list in the *Configuration > Video > Storage* screen. The NLSS Gateway contains ports for USB and eSATA.

Network Attached Storage (NAS) devices must be attached to the same Ethernet as the NLSS Gateway, and be manually added to the list in the *Configuration > Video > Storage* screen.

The NLSS Gateway supports: iSCSI and NFS.

15.2.1 Storage Table

The Storage table provides an overview of the status of each drive. Items in the table can be added, configured, searched and deleted.

1. Select **Configuration > Video > Storage** from the Main Menu.

The *Storage* table is displayed.

- Click on a column to sort the list.
- See [Searching Tables](#) for search instructions.

2. Select a storage device from the table. The *Storage Details* pane is displayed.

15.2.2 Storage Details

The top three fields in the Storage Details pane are the same for each type of disc.

- **Device Name:** a text field to enter a custom name for the device.
- **Attached to Gateway:** the Gateway to which this device is attached.
- **Device Type:** Either Internal, USB, eSATA, iSCSI or NFS.

The remaining fields are dependent on the Device Type. Internal and eSATA have no additional fields.

NFS adds one field:

- **Mount Point:** the IP address of the device, appended by the relative path to the mount point on the device. The syntax depends on the exact device. Consult the device's user manual for additional instructions.

iSCSI adds five fields.

- **Target IP Address:** the IP address for the storage device.
- **Node:** the iSCSI storage node in which the video is stored.
- **User Name:** the user name required to write to the device.
- **Password:** the password set for the User name.
- **LUN:** the location on the device where video is stored.

15.2.3 Storage: Actions

You can take the following actions in the Configuration > Video > Storage screen:

- [Add USB Storage Devices](#)
- [Add eSATA Storage Devices](#)
- [Add iSCSI Storage Devices](#)
- [Add NAS Storage Devices](#)

15.2.3.1 ADD USB STORAGE DEVICES

1. Log into the Gateway via the NLSS Web Interface.
2. Attach the USB cable from the storage device to the NLSS Gateway.
The NLSS Gateway automatically discovers and configures the attached USB storage device.
3. Optionally, to change the **Device Name** in the Storage Details.
 - a. Select the device in the Storage table.
 - b. Enter the new **Device Name**.
 - c. Click **Save** to keep the change.
 - » Click **Cancel** to restore the previous setting.

15.2.3.2 ADD eSATA STORAGE DEVICES

1. Log into the Gateway via the NLSS Web Interface.
2. Attach the eSATA cable from the storage device to the NLSS Gateway.
3. Reboot the NLSS Gateway.
4. After the NLSS Gateway reboots, log into the NLSS Web Interface.
The NLSS Gateway automatically discovers and configures the attached eSATA storage device.
5. Optionally, to change the **Device Name** in the Storage Details.
 - a. Select the device in the Storage table.
 - b. Enter the new **Device Name**.
 - c. Click **Save** to keep the change.
 - » Click **Cancel** to restore the previous setting.

15.2.3.3 ADD iSCSI STORAGE DEVICES

1. Click **Add** in the Storage table.
The *Storage Details* pane is displayed.
2. Enter a **Disc Name**.
3. Select **iSCSI** from the **Device Type** drop-down list.

4. Enter the **Target IP Address**.
5. Click the plus (+) button next to the Target IP Address field.
The Gateway locates the device on the network.
6. Select a **Node** from the drop-down list.
7. Enter a **User Name** and **Password** to access the disc.
These credentials must have read-write access.
8. Select the **LUN** from the drop-down list.
9. Click **Save** to keep the change.
 - Click **Cancel** to restore the previous setting.

15.2.3.4 ADD NAS STORAGE DEVICES

1. Click **Add** in the Storage table.
The *Storage Details* pane is displayed.
2. Enter a **Disc Name**.
3. Select **NFS** from the **Device Type** drop-down list.
4. Enter a **Mount Point**.
5. Click **Save** to keep the change.
 - Click **Cancel** to restore the previous setting.

15.2.3.5 DELETE A STORAGE DEVICE

1. Click **Delete** in the Storage table.
2. Click the **Delete** button.
A confirmation dialog is displayed.
3. Click **Yes** to verify the deletion.
 - Click **Cancel** to close the dialog without deleting the Storage device from the list.

15.3 CONFIGURE NLSS HD MEDIA DECODERS

NLSS HD Media Decoders are discovered when the NLSS Discovery Utility is run when installing the Gateway. These Decoders are listed in the NLSS Web Interface.

For details on NLSS decoders, see the *NLSS DC-400 HD Media Decoder: User Guide* available at www.NLSS.com.

15.3.1 Decoder Table

The Decoder table provides an overview of the status of each drive. Items in the table can be configured, searched and deleted.

1. Select **Configuration > Video > Decoder** from the Main Menu.
The *Decoder* table is displayed.
 - Click on a column to sort the list.
 - See [Searching Tables](#) for search instructions.
2. Select a Decoder from the table. The *Decoder Details* pane is displayed.

15.3.2 Decoder Details

Some fields in the Decoder Details can be edited, while others cannot.

- [Parameters You Can Edit](#)
- [Read-Only Parameters](#)

15.3.2.1 PARAMETERS YOU CAN EDIT

The Decoder's username and password are set on the decoder itself, via its own interface.

- **Username:** Enter the user name required to log into the selected decoder.
- **Password:** Enter the password required to log into the selected decoder.
- **Device Name:** a text field to enter a unique name for the decoder
- **Device Location:** optional text field to enter the physical location of this decoder.

15.3.2.2 READ-ONLY PARAMETERS

- **Device Model:** the model of this decoder, such as GW-400.
- **IP Address:** the Decoder's assigned IP address.
- **Connection State:** the current state of the connection between the Decoder and the NLSS Gateway to which it is attached.
- **Hardware Version:** the version of the Decoder's hardware.
- **Serial Number:** the serial number of this Decoder.
- **Firmware Version:** the version of the Decoder's firmware.

15.3.3 Decoders: Actions

Decoder Details can be edited, as needed.

1. Select **Configuration > Video > Decoder** from the Main Menu.
The *Decoder* table is displayed.
2. Select a Decoder from the table.
3. Edit the **Decoder Details** as needed.
A user-friendly Device Name and Device Location can be entered to make the Decoder easier to identify in the NLSS Web Interface.

Note: The system can access a decoder only if the correct values are entered in the Username and Password fields. The correct values are those the decoder itself has been configured to accept.

4. Click **Save** to keep the changes.
 - Click **Cancel** to restore the previous settings.

Chapter 16: Remote Management Services

Remote Management Services (RMS) provides centralized management for NLSS sites (Gateways) via the *NLSS Customer Portal*.

Users can access sites via RMS to view video, manage a Gateway, and use all the functions of the system as if they were logged in directly to the Gateway.

Video from multiple sites can be displayed in a single, multipane view.

Important: The login name can be changed to *superuser@xyz.com* when the Superuser default password is changed.

When registering with RMS, if the default login name of *superuser* is reset to *superuser@xyz.com*, then the Superuser login name is reset to *superuser*.

However, if the password has been changed from the default of *superuser*, the password is not reset.

If there is a user on the Gateway with the same user ID at the Customer level, the password on the Gateway is overwritten by the Customer password.

16.1 RMS HIERARCHY

RMS is deployed in a hierarchy.

- *Site*: an NLSS Gateway, monitoring a location's cameras, cardholders, doors, etc.
- *Customer*: the end user who buys the NLSS service from a Partner for a business or institution. A Customer can manage multiple sites, and configure settings for the sites.
- *Partner*: the organization that provides the NLSS service to customers. A Partner can have multiple customers.

16.2 LOGGING IN TO THE CUSTOMER PORTAL

The log in for an RMS Customer is different than the log in for a User managing a site.

1. In a web browser, enter the URL for the NLSS Customer Portal, as provided by the Partner.
2. Enter the credentials in the login screen.
 - a. **User Name:** this name is configured by the Partner, and cannot be changed in the Customer Portal.
 - b. **Password:** a default password is provided by the Partner, but can be changed in the Customer Portal.
 - c. **Organization:** a name set by the Partner to encompass the Customer's site. The organization name cannot not be changed in the Customer Portal.
3. Click **Login**.

The Site Map is displayed with links to the RMS registered sites.

16.3 RMS MAIN MENU

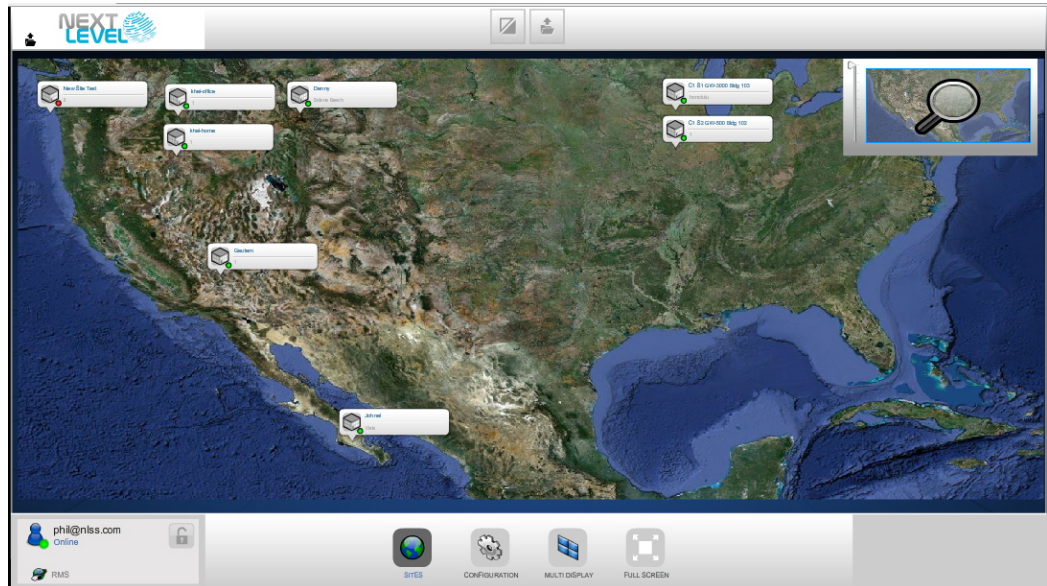
The RMS Main Menu contains three options.





- [Sites](#)
- [Multisite Display](#)
- [Sites](#)

16.4 SITES

The Site Map is the main landing page after logging in to the Customer Portal. The Site Map also is accessed anytime from the Main Menu by clicking the **Sites** button. This map provides links to the sites in your organization managed by RMS. From the Sites Map, you can monitor and configure your sites and their devices.



- Use the **Upload** button above the main pane to load a map or other graphic to be used as a background for this page.

- **Site icons** are automatically placed on the map when a site is added. The icons include the name of the site and a status dot.
 - Green dot indicates that the site is accessible.
 - Red dot indicates that the site is not available.
 These icons can be moved.
 - a. Click the **Unlock/Lock** button to unlock the icons. The button is grayed out when the icons are unlocked.

 - b. Drag the icon to the new location on the map.
 - c. Click the **Unlock/Lock** button to lock the icons.
- Slide the Magnifying Glass slider down to zoom in on the map. Drag the map around in the Magnifying Glass window to display the enlarged area that you want to view.
- Click a Site icon to go directly to that Gateway. All functions that can be done by directly accessing the Gateway can be done via RMS.

Note: When a Gateway’s configuration options are accessed under the RMS Site map, via **Configuration >Global->Gateway**, certain options are not available:

- » **Check Update**

- » **Firmware Update**
- » **Factory Reset**

These options are available by accessing the Gateway directly via the NLSS Web Interface.

16.5 MULTISITE DISPLAY

The Multisite Display provides customized views from cameras at the sites managed by RMS.

From the Multisite Display, views can be created to simultaneously monitor multiple sites and cameras.

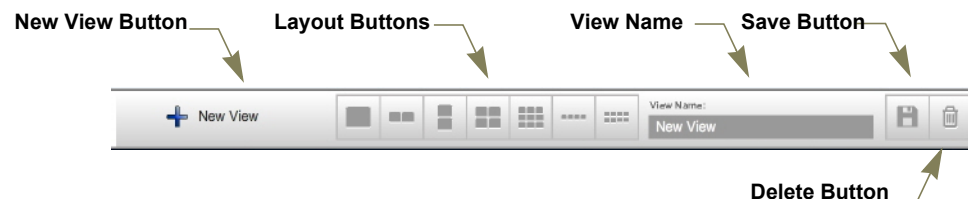
16.5.1 Displaying a View

Views can be displayed within a browser, expanded to fill the browser window, or expanded to fill the display.

1. Select a View in the **Views** list.
2. Click the **Full Screen** toggle in the Multisites Display pane to hide the lists and the menus.
 - To fill the whole screen with the View, click the **Full Screen** toggle in the Main Menu, then click the **Full Screen** toggle in the Multisite Display.

16.5.2 Creating a New View

Views can be created and saved, allowing a User to easily switch between sites and Cameras.



1. Select **Multisite Display** from the Main Menu.
2. Click the **New View** button at the top of the screen.
3. Click on the button for the screen layout desired for the View.
4. Click in a box representing a screen. A gray highlight frames the selected screen.
5. Select a site from the **Site List**. A Camera list is displayed.
6. Select a **Camera**.
7. Repeat steps 4 to 6 for each View screen.
8. Enter a **View Name**.
9. Click the **Save** button.

16.5.3 Editing a View

1. Select **Multisite Display** from the Main Menu.
2. Select a **View** from the list.
3. Modify the View, as needed.
 - Modify the layout using the layout buttons at the top of the screen.
 - Select a monitor and then select a different camera using the Site and Camera lists.
4. Click the **Save** button.
 - To discard the changes without saving them, click on another View without clicking the Save button.

16.5.4 Deleting a View

Views can be deleted.

1. Select **Multisite Display** from the Main Menu.
2. Select a View from the list.
3. Click the **Delete** button (trash can).

16.6 FULL SCREEN

The Full Screen toggle in the Main Menu hides the browser's borders to allow the RMS interface to fill the screen.

- Click on the **Full Screen** toggle in the Main Menu.
The label changes to say **Normal Screen**.
- Click the **Normal Screen** toggle or press **Esc** to restore the browser's boundaries.