NLSS Unified Security Suite 2.3

User Manual

Gateway-March 20, 2012 1:54 pm

Contents

Chapter 1: Introduction 11

KEY FEATURES 11

COMPONENTS OF THE NLSS UNIFIED SECURITY PLATFORM 12

NLSS Gateway 12

NLSS Unified Security Suite 12

Access Control Devices 12

Cameras 12

NLSS HD Media Decoder 13

External Storage 13

Generic Computers and Browsers 13

Generic HD Monitors 13

Chapter 2: Installation 14

SYSTEM REQUIREMENTS 14

Requirements for NLSS Discovery Utility 14

Requirements for Configuration and Operation 14

HARDWARE INSTALLATION 15

SOFTWARE INSTALLATION 16

Install Security Certificate 16

Install Cameras 18

Install NLSS Gateways 18

PART 1: OPERATIONS

Chapter 3: Getting Started 21

LOG IN 21

Local Login 21

Automatic Log Outs 22

Remote Login 22

THE MAIN MENU 22

Operations Menu 23

System Health 24

Operations Panels *26*

Filtering Operations Lists 27

Searching a List 27

Events Menu 28

Configuration Menu 28

Chapter 4: Controlling Cameras 29
SELECTING CAMERAS 29
Filtering the Camera List 31
MONITORING CAMERAS 32
Monitor Cameras from the Operations Menu 32
Using the Camera Toolbar 33
Video Information 33
Hide Toolbar 34
PTZ (Pan, Tilt, Zoom) 34
Digital Zoom *38*
Manual Camera Output 38
Video Analytics 38
Filmstrip 52
Date & Time Selection *53*
Rewind and Fast Forward 53
Play/Pause 53
Live/Recorded Toggle *54*
Camera Events Toggle 54
Event Bookmark 54
Snapshot 54
Save a Clip *55*
Local Microphone Control 55
Volume / Mute 55
Full Screen Toggle 55
Time Sliders *56*
Additional Camera Controls 57
Select Stream 57
Transcode/Native 57
Back 57
Camera Reports and Events 58
Camera Events 58

Chapter 5: Displaying Video 60
CREATE, EDIT, AND DISPLAY VIEWS 61
Views Menu and Layout 61
Menu Options 61
Create Views 62
Edit Views 62
Delete Views 62
CREATE, EDIT, AND DISPLAY SEQUENCES 63
Sequences Menu and Editor 63
Create New Sequences 64
Edit a Sequence 64
Delete Sequences 64
Display Sequences 65
PUSH VIEWS AND SEQUENCES TO DECODERS 65
Decoder Panel 65
Pushing a View or Sequence 66

Chapter 6: Operations with Doors 67

DOORS PANEL 67

MOMENTARILY UNLOCK A DOOR... 68

ASSOCIATE CAMERAS AND DOORS 68
Associating and Viewing Cameras with Doors......................... 68
Disassociate Cameras from Doors.. 68

OPEN CAMERA AUDIO FOR AN ASSOCIATED DOOR...................... 69

VIEW EVENT AND REPORTS FOR A DOOR 69

Chapter 7: Operations with Cardholders & Users........................ 70

CARDHOLDERS & USERS PANEL 70
Filtering Cardholders & Users List.. 71

ACTIONS WITH CARDHOLDERS 71
Cardholder Information 71
User Information.. 72
Cardholder Photo 72
Activate / Deactivate Cardholders.. 73
Cardholders & Users Reports and Events 73

Chapter 8: Using Floor Plans.. 74

Chapter 9: Using Groups.. 76

GROUPS PANEL.. 76

LIST VIEW 77
Adding and Using Maps 77

Chapter 10: Operations with Reports 80

GENERATING REPORTS 80
Reports Panel 80
Event-Specific Reports.. 81
Device-Specific Reports.. 83

CATEGORIES OF EVENT-SPECIFIC REPORTS 83
Access Control Reports 83
Camera Reports... 83
Door Reports... 84
System Reports... 84
User Reports 84
Video Analytics Reports 84

Chapter 11: Monitoring and Handling Events 85

MONITORING EVENTS 85
Event Log 86
Event Log List 86

EVENT DETAILS 89
Event Details Actions 89
Event State 89
Shunt Toggle 90
Lock State Toggle 90
Written Note Editor 90
Recorded Event 90
Current Snapshot 90
Profile Picture 90
Exporting the Event 91
Exit 91
Emergency Events 91

PART 2: SYSTEM CONFIGURATIONS

Chapter 12: General Configuration Functions 93

SEARCHING TABLES 93

ADDING, EDITING AND DELETING ITEMS 94
Adding Items 94
Edit Items 94
Delete Items 94

Chapter 13: Global Configurations 95

CONFIGURE RMS 96

CONFIGURE CUSTOMER 96
Customer Details 96
Customer Configuration 96

CONFIGURE SITES 97
Site Details 97
Editing Site Details 97

CONFIGURE NLSS GATEWAYS 97
General Tab 98
General Tab Parameters 98
General Tab Buttons and Links *99*
Wired Network Tab 103
Email Tab 104
Time Tab 104

CONFIGURE HOLIDAYS 105
Holidays Table 105
Holiday Details 105

CONFIGURE SCHEDULES 106

Schedule Details ... 106
Create New Schedules ... 107

CONFIGURE EVENT TYPES ... 107
Event Type Table ... 107
Event Type Details ... 107

CONFIGURE EVENT SEVERITY ... 108
Event Severity Table ... 108
Event Severity Details ... 108

CONFIGURE ACTIONS ... 108
Action Type ... 108
Creating an Action ... 110

CONFIGURE EVENT LINKAGES ... 110
Event Linkage Details ... 111
Creating an Event Linkage ... 112

CONFIGURE GROOMER SETTINGS ... 113

Chapter 14: Configure Identity and Credentials ... 114

CONFIGURE ACCESS LEVELS ... 115
Access Level Details ... 116
Create a New Access Level ... 116

CONFIGURE CARD PROFILES ... 116
Card Profiles Table ... 116
Card Profile Details ... 117

CONFIGURE BADGE PROFILES ... 118
Badge Profiles Table ... 118
Badge Profiles Details ... 118

CONFIGURE CARDHOLDER-USER DEFINED FIELDS ... 119
Editing a User Defined Field for Cardholders ... 119

CONFIGURE CARDHOLDERS ... 120
Cardholders Table ... 120
Cardholders Tabs ... 120
General Tab ... 120
Credentials Tab ... 121
Access Levels Tab ... 123
Contacts Tab ... 123
Organizational Tab ... 124
User Defined Tab ... 124
Options Tab ... 124

Chapter 15: Configure Access Control ... 126

CONFIGURE CONTROLLERS ... 127
Controller Details ... 128
General Tab ... 128
Controller Details: Diagnostics Tab ... 130
Associating a Mercury Controller with an NLSS Gateway ... 130

CONFIGURE READER INTERFACES ... 131
Reader Interface Details ... 131

General Tab 131
Aux Input Tab 132
Aux Output Tab 133
Reader Interfaces: Actions 134
Add Reader Interfaces Manually 134
Delete Reader Interfaces 134

CONFIGURE READERS 135
Reader Details 135
General tab 135
Aux Outputs Tab 136

CONFIGURE DOORS 137
Door Details 137
General Tab 137
Strike Tab 138

CONFIGURE I/O INTERFACES 138
I/O Interface Details 139
I/O Interfaces: General Parameters 139
I/O Interface Details: Aux Input Tab 139
I/O Interface Details: Aux Output Tab 140

CONFIGURE I/O LINKAGES 140
I/O Linkages Details 142

Chapter 16: Configure Video, Storage, & Decoders 143

CONFIGURE EXTERNAL STORAGE DEVICES 143
Storage Table 143
Storage Details 144
Adding Storage Devices 144
USB Storage Devices 144
eSATA Storage Devices 145
iSCSI Storage Devices 145
NAS Storage Devices 145

CONFIGURE CAMERAS AND STREAMS 146
Camera Details General Tab 146
Editable Parameters 146
Read-Only Parameters 147
Camera Details Stream Tab 148
List of Streams 148
Video Stream Parameters 148
Audio Stream Parameters 149
Camera Details Recording Tab 149
Stream Settings 149
Camera Settings 150
Cameras Actions 150
Connect to a Camera 151
Add RTSP and HTTP Streams 151

CONFIGURE NLSS HD MEDIA DECODERS 152
Decoder Table 152
Decoder Details 152
Editable Parameters 152
Read-Only Parameters 153

Chapter 17: Configuring Permissions 154

APPLYING PERMISSIONS EXAMPLE 155

GROUPS 157

Example 157

Groups Panel 158

Create a Group 158

Edit a Group 159

Delete a Group 159

ROLES 160

Roles Details 161

General Tab 161

Gateway Modules Tab *162*

Gateway Groups 164

Gateway Functions 165

Cloning a Role 166

Delete a Role 166

USERS 167

User Details 168

Chapter 18: Remote Management Services 169

EXAMPLE OF RMS DEPLOYMENT 169

RMS HIERARCHY 173

LOGGING IN TO THE NLSS RMS WEB INTERFACE 174

RMS MAIN MENU 174

SITES 175

OPERATIONS 176

Multiview 176

Groups 177

CONFIGURATION 178

RMS Settings 178

Initial Registration 179

RMS Dependencies 179

Transferring RMS Settings 180

Transfer Status 180

Global 181

Customer 181

Sites 181

Holidays 184

Schedules 185

Event Type 185

Event Severity 186

Identity 187

Access Levels 187

Card Profile 188

Badge Profiles 188

Cardholder - User Defined 189

Cardholders 189

Permissions 190
Groups 190
Roles 190
Users 191

FULL SCREEN 192

Chapter 19: NLSS Unified Security Suite v2.3: Mobile App ... 193

GETTING STARTED 194

NAVIGATING THE NEXT LEVEL MOBILE APP 195

SEARCHING A LIST 196

VIEWING VIDEO 197

VIEWING A DOOR 200

USING GROUPS 202

Chapter 20: Contacting Support 203

GATEWAY INFORMATION 203

SYSTEM LOG 204

CONFIGURATION BACKUP 204

CONTACT INFORMATION 204

Preface

PURPOSE, SCOPE, AND AUDIENCE OF THIS MANUAL

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

Except for access control devices, the NLSS devices in the Unified Security Suite use common connectors such as standard AC cords, and Ethernet, USB, eSATA, HDMI connections. For instructions on wiring the NLSS Gateway and third party access control devices, refer to the separate *NLSS Gateway: Quick Start 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* runs on the NLSS Gateway. This software is a unified platform for video surveillance, video analytics, and access control.

The Gateway, using the embedded NLSS Unified Security Suite, connects with third party video cameras and access control devices over an IP-based network. The NLSS Unified Security Suite collects data from separate access control devices, and video cameras. Information about users, cardholders, schedules, permissions, and related data are stored in a database on the Gateway. The *NLSS Web Interface* allows users to operate and configure their systems.

The NLSS Web Interface provides users with browser-based access to either a single site (NLSS Gateway), or to multiple sites (Gateways) managed by *RMS* (*Remote Managed Services*).

This document describes how to use the NLSS Web Interface.

1.1 KEY FEATURES

The NLSS Unified Security Suite is configured and operated using the NLSS Web Interface, which is accessed through most browsers on any computer.

- **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 finds all NLSS devices on the same Layer 2 network.
  - Discovered devices easily can be configured and updated in the system without disrupting operations.
  - Administered and operated through a browser via the user-friendly 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 at multiple locations. A Gateway can handle multiple cameras, access points, and cardholders.
  - *Video*: can auto-discover many IP cameras, including 1080p HD cameras. The NLSS Web Interface also can 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. RMS provides the ability to access, configure and operate multiple Gateways 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

An NLSS Gateway, network access, and a computer with a browser, are the minimum requirements to configure, administer, and operate the NLSS Security Platform.

1.2.1 NLSS Gateway

The NLSS Unified Security Suite software is installed on each NLSS Gateway, with *no software licenses*. Each NLSS Gateway is a network device that collects and processes video and access control information. The NLSS Unified Security 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 NLSS Unified Security Suite.

Important: NLSS recommends that the Gateway be plugged into a UPS for protection in the event of a power failure.

1.2.2 NLSS Unified Security Suite

The NLSS Unified Security Suite provides an easy and powerful means to monitor, manage and act on data from video cameras and access control devices attached to the same network as the NLSS Gateway. Use a browser to log into the NLSS Web Interface generated by the NLSS Unified Security Suite.

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 IP-based 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

When the decoder is part of an NLSS Security Platform, any Gateway in the network can manage the decoder. *Independent Mode* software also is embedded on each *NLSS HD Media Decoder* so it can operate in a stand-alone mode.

NLSS strongly recommends the use of NLSS HD Media Decoders for long-term, continuous monitoring of video. Although video can be monitored in the NLSS Web Interface, a web browser is required 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 External Storage

Third-party 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 and Browsers

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 supported: FireFox (3.0 or above), Safari (3.0 or above), Internet Explorer (8.0 or above), Chrome (16.0) or above.

- Adobe Flash Player 11.1 or above also must be installed.

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

See **Requirements for Configuration and Operation** for more information.

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.

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 Requirements for NLSS Discovery Utility

The NLSS Discovery Utility discovers NLSS Gateways and Decoders installed on the same network.

NLSS Discovery Utility runs on a Windows-based PC with:

- Access to the LAN on which the NLSS Gateway is installed
- Multicore Intel processor
- 2GB of RAM minimum. The 64-bit version of Windows 7 requires 4 GB of RAM.
- Operating systems:
  - Windows XP (32/64)
  - Windows Vista (32/64)
  - Windows 7 (32/64)
- CD/DVD reader
- Windows .NET Framework

2.1.2 Requirements for Configuration and Operation

After the NLSS Gateway is discovered, it can be configured and operated from multiple platforms and browsers.

- Minimum dual core processor
- Operating Systems:
  - Windows XP (32/64)
  - Windows Vista (32/64)
  - Windows 7 (32/64)
  - Linux

  - Mac OS X v10.6 or above

- 2GB of RAM minimum
- Access to the network on which the NLSS Gateway is installed
- Browser: FireFox (3.0 or above), Safari (3.0 or above), or Internet Explorer (8.0 or above). Flash 10.3 or above also must be installed.

Important: Disable hardware acceleration for Flash in the browser.

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.

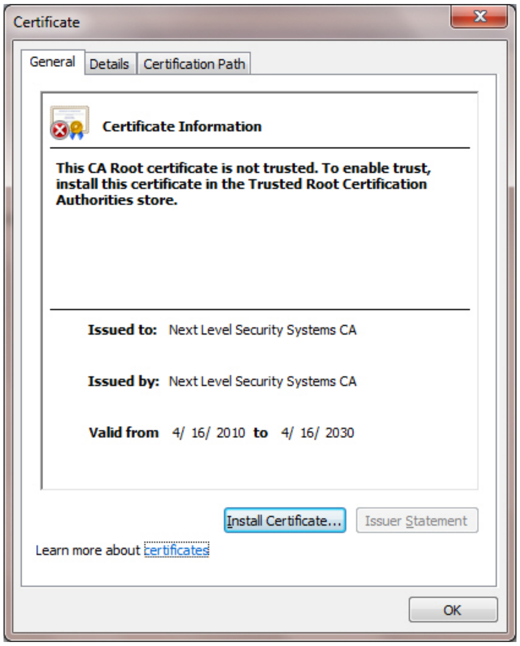
- **Install Security Certificate**
- **Install Cameras**
- **Install NLSS Gateways**

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).



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

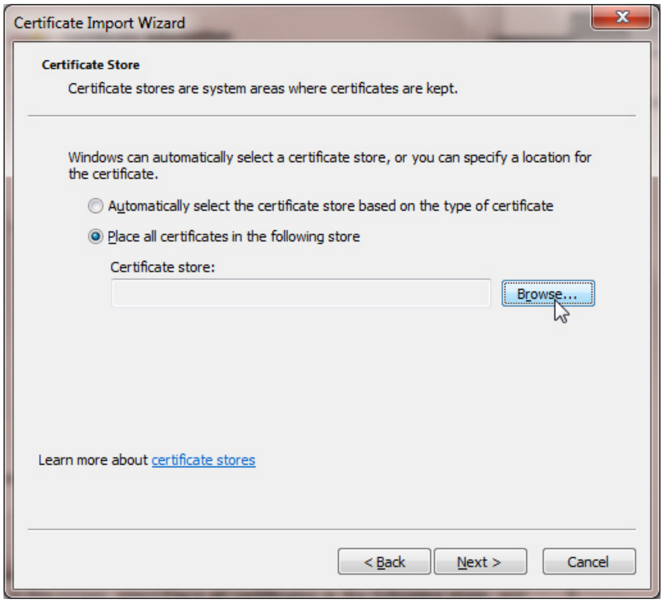
Issued to: Next Level Security Systems CA

Issued by: Next Level Security Systems CA

Valid from 4/ 16/ 2010 to 4/ 16/ 2030

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.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

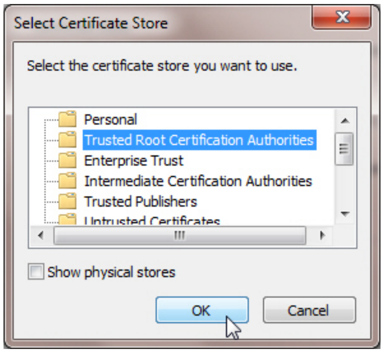
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

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



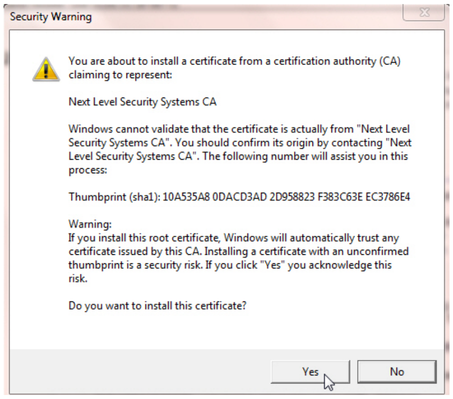
Select Certificate Store

Select the certificate store you want to use.

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.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

Next Level Security Systems CA

Windows cannot validate that the certificate is actually from "Next Level Security Systems CA". You should confirm its origin by contacting "Next Level Security Systems CA". The following number will assist you in this process:

Thumbprint (sha1): 10A535A8 0DACD3AD 2D958823 F383C63E EC3786E4

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

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 and Browsers**.

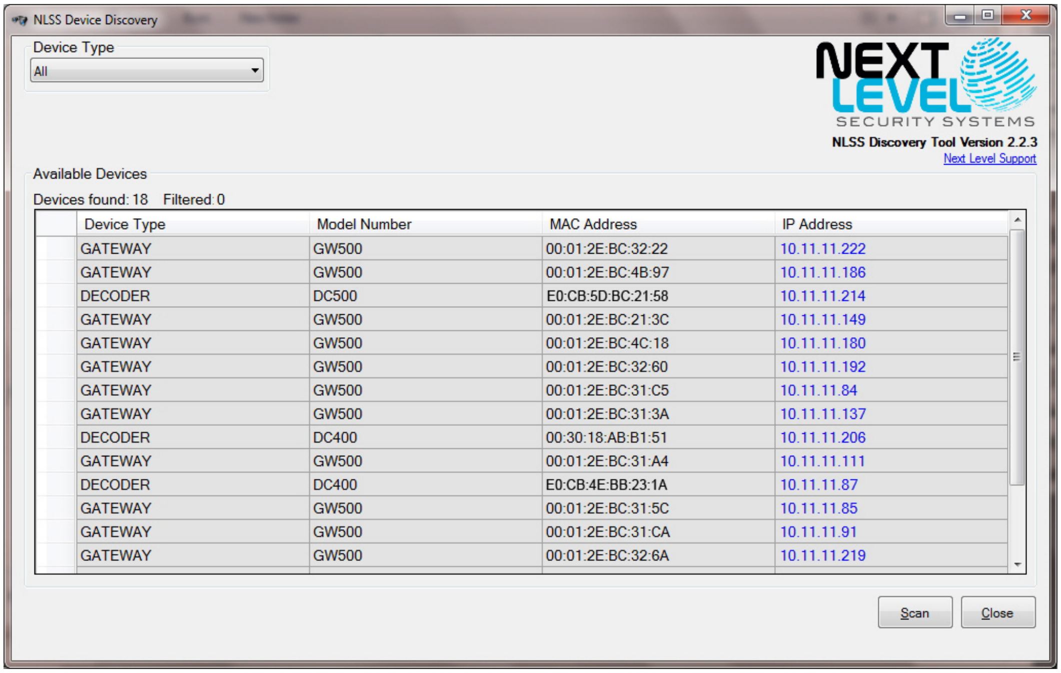
   – Ensure the computer has a high speed Internet connection to support streaming video, and is connected to the same network as the Gateway.

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.



Devices found: 18 Filtered: 0

Device Type	Model Number	MAC Address	IP Address
GATEWAY	GW500	00:01:2E:BC:32:22	10.11.11.222
GATEWAY	GW500	00:01:2E:BC:4B:97	10.11.11.186
DECODER	DC500	E0:CB:5D:BC:21:58	10.11.11.214
GATEWAY	GW500	00:01:2E:BC:21:3C	10.11.11.149
GATEWAY	GW500	00:01:2E:BC:4C:18	10.11.11.180
GATEWAY	GW500	00:01:2E:BC:32:60	10.11.11.192
GATEWAY	GW500	00:01:2E:BC:31:C5	10.11.11.84
GATEWAY	GW500	00:01:2E:BC:31:3A	10.11.11.137
DECODER	DC400	00:30:18:AB:B1:51	10.11.11.206
GATEWAY	GW500	00:01:2E:BC:31:A4	10.11.11.111
DECODER	DC400	E0:CB:4E:BB:23:1A	10.11.11.87
GATEWAY	GW500	00:01:2E:BC:31:5C	10.11.11.85
GATEWAY	GW500	00:01:2E:BC:31:CA	10.11.11.91
GATEWAY	GW500	00:01:2E:BC:32:6A	10.11.11.219

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.

Note: The features available after login are dependent on the user's role. See **Chapter 17: Configuring Permissions** for more information.

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. 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.

When the browser connects to the target Gateway, a login screen is displayed. Log in with an assigned username and password.

If logging into a new Gateway for the first time, use the following user name and password, which provide unlimited access to configuration, administration, and operation.

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

Important: After logging into the Gateway for the first time, change the default password for the *Superuser* and *Operator*.

Note: When a Gateway is registered with RMS, the superuser password is reset to *superuser.* The password can be changed at the RMS level.

Once the discovery process begins, it may take a few minutes to locate all compatible cameras and access control devices on the 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 in 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

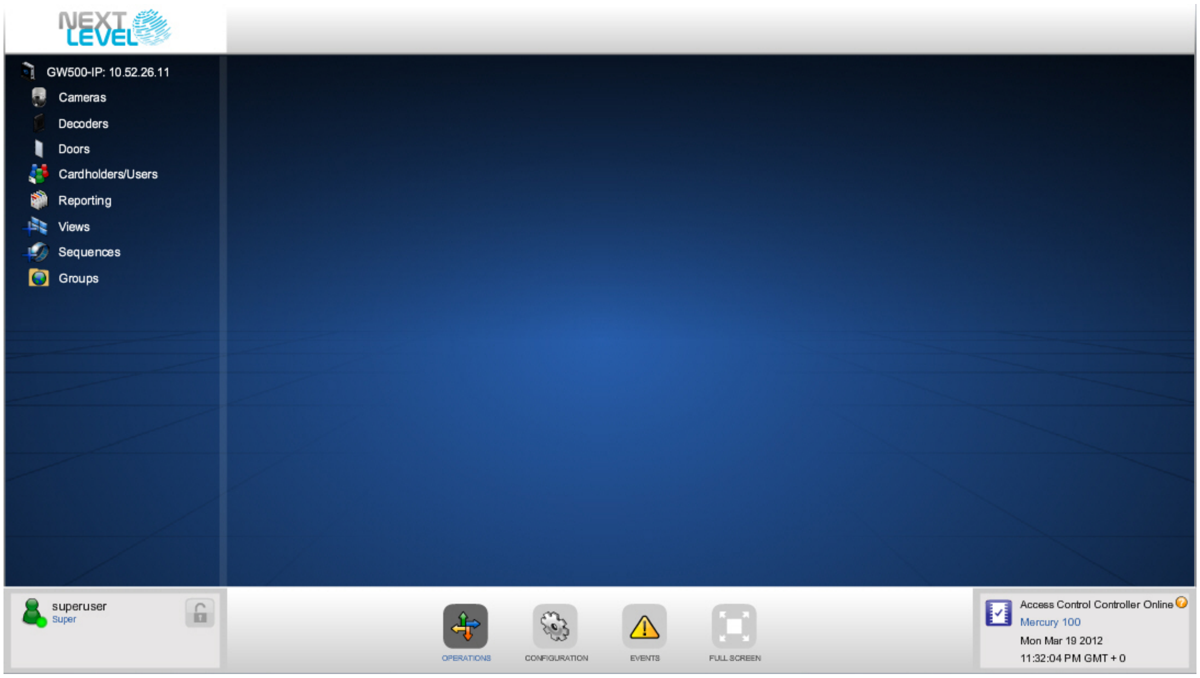
Logging into the system via the NLSS Web Interface is the same for remote users as for local users, except a VPN or another service is required to access the network on which the target NLSS Gateway is installed.

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.

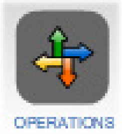
3.2 THE MAIN MENU

User permissions determine which Main Menu items can be accessed at the bottom of the screen. Users with unlimited permissions all menu options can access. See **Roles** and **Users** in **Chapter 17: Configuring Permissions** for more information.

- **Logoff**: ends your session on the NLSS Web Interface.
- **Operations Menu**
- **Events Menu**
- **Configuration Menu**
- **Full Screen**: toggles between full-screen and windowed modes.



3.2.1 *Operations* Menu

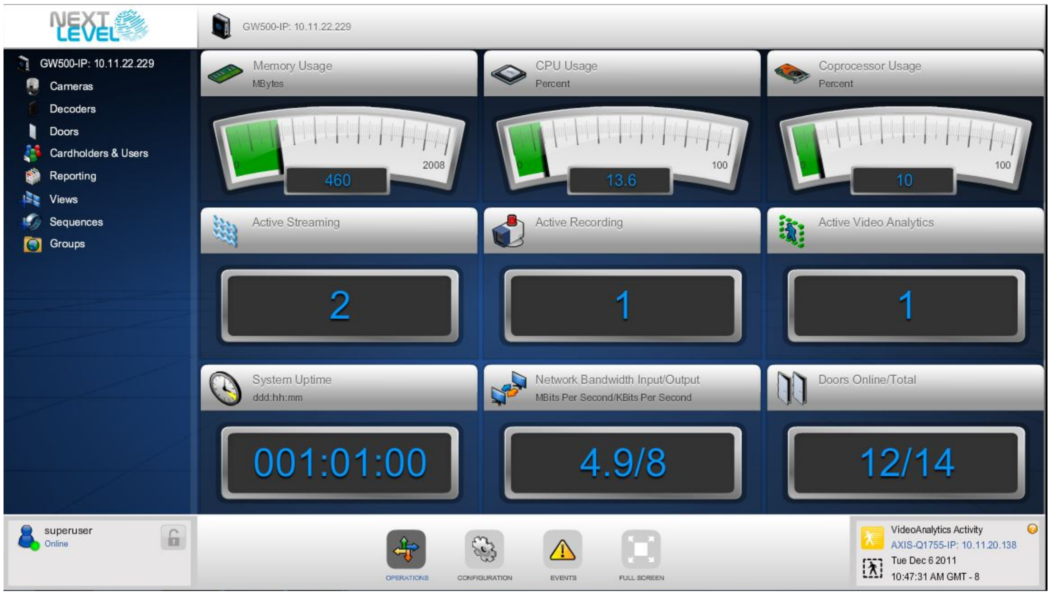


In the Operations menu on the left side of the screen contains most of the functions that Operators of the NLSS system regularly need. Operator accounts are typically configured with permission to access everything under the Operations menu. After you click the **Operations** button, a series of options 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 8: Using Floor Plans** for instructions.
- **Reporting**: run reports that summarize events, etc. See **Chapter 10: Operations with Reports** for instructions.
- **Doors:** locking and unlocking doors manually, as well as running individual door reports. See **Chapter 6: Operations with Doors** for instructions.
- **Cardholders**: tracing and deactivating individual Cardholders, as well as running individual cardholder reports. See **Chapter 7: Operations with Cardholders & Users** for instructions.
- **Views:** create custom video display layouts, using one or multiple cameras or video streams. See **Chapter 5: Displaying Video** for instructions.
- **Sequences**: create automated progression of views to display when launched. See **Chapter 5: Displaying Video** for instructions.

3.2.1.1 System Health

.System Health provides a quick overview of the load and activity on an NLSS Gateway. Monitoring System Health is important when running video analytics. Since Analytics can consume system resources, over usage can impact system performance. See **Video Analytics** for more information.



1. Open the NLSS Gateway Web Interface.

2. From the Main Menu, select **Operations > *gateway***, where *gateway* is the name of the NLSS Gateway managed in this portal. For example, *GW500-IP: 123.45.55.1*.

   The System Health pane is displayed.

This panel can be accessed at any time by clicking on the Gateway's name.

A series of real time indicators summarizes the Gateway's health. The gauges provide a graphical indictor of the system health:.

Color	Cause
Green	Operating within normal parameters.
Yellow	System is exceeding 70% of the RAM or processor capacity.
Orange	System is exceeding 80% of the RAM or processor capacity.
Red	System is exceeding 85% of the RAM or processor capacity.

- **Memory Usage**: the amount of RAM, in MBytes, currently in use. The gauge also indicates the total MBytes of RAM.

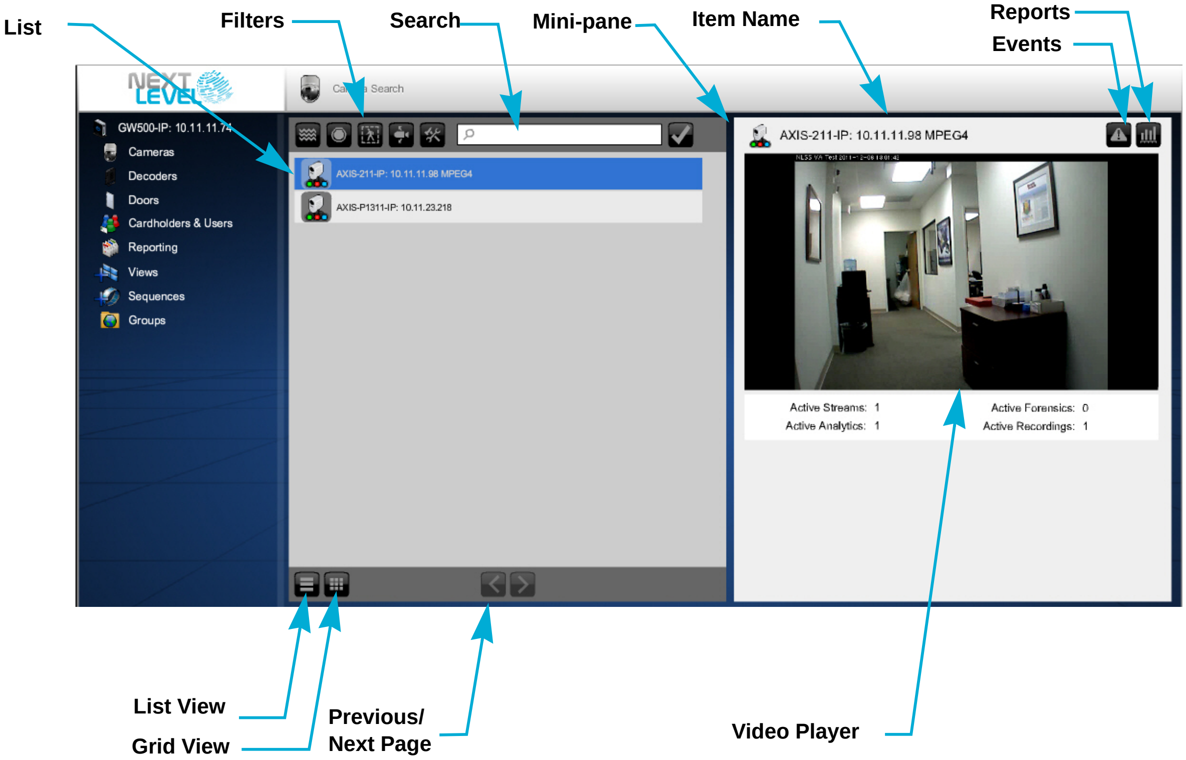
- **CPU Usage**: the percentage of CPU currently in use. When the percentage reaches 80%, the gauge turns red to indicate a high usage that could impact performance.

- **Coprocessor Usage**: the percentage of the coprocessor currently in use. When the percentage reaches 80%, the gauge turns red to indicate a high usage that could impact performance.

- **Active Streaming**: the number of video streams monitored by this Gateway.
- **Active Recording**: the number of video streams of cameras that are currently set to recording mode.
- **Active Video Analytics**: the number of video analytics currently running on cameras or video streams.
- **System Uptime**: the length of time since the Gateway last was restarted, measured in *dddd:hh:mm*.
- **Network Input/Output**: the rate that the Gateway is receiving and sending out data.
- **Doors Online/Total**: the number of doors currently available, as compared to the total number of doors placed in service on the Gateway.

3.2.1.2 Operations Panels

When the Operations > Cameras/Doors/Decoders/Cardholders & Users options are selected, List and Preview panels are displayed.



The list contains these standard features for each option:

- **Filter**: click a button to display a pop-up dialog box containing filtering choices for the list. See **Filtering Operations Lists** for instructions.

- **Search**: enter text and click the check mark to find matching items. Clear the Search field and click the check mark again to display all items.

- **List View**: displays the items in a simple list.

- **Grid View**: displays the items in a grid, with thumbnails.

Note: The view options are only available for Cameras and Cardholders.

- **Previous/Next Page**: provides navigation through multiple pages of items. These buttons are grayed out if only one page of items is available.

Click on a list item to display that item in the mini pane.

- **Item name**: identifies the selected item.

- **Events**: accesses the Events Log for this item. See **Chapter 11: Monitoring and Handling Events** for more information.

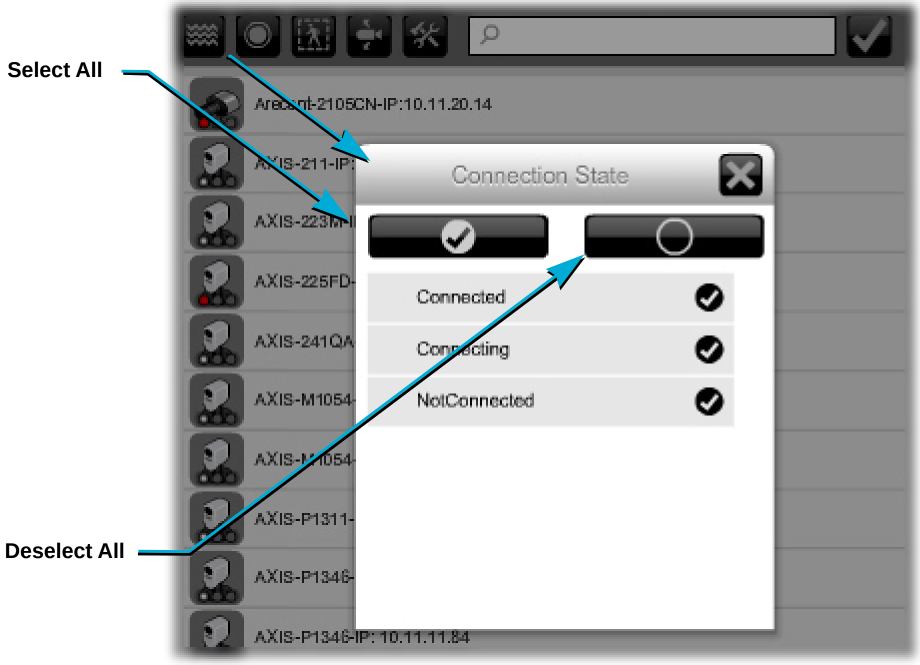
- **Reports**: accesses the reports for this item. See **Chapter 10: Operations with Reports** for more information.

- **Item**: interface to the selected item. A mini video player is displayed for Cameras, Decoders, and Doors (if applicable). Click in the mini video player pane to launch the full video player for Cameras and Doors, and the View or Sequence for a Decoder.

3.2.1.3 Filtering Operations Lists

An Operations list can be filtered.

1. Click a filter button to open a dialog.



2. Check the items you want included in the list.
   - Deselect an option to hide the matching items in the list.
   - Click **Select All** (check mark) to choose all options in the dialog.
   - Click **Deselect All** (circle) to hide items matching all options in this dialog box.
3. Click **Close** (**X**) to exit the dialog.

To display all items again, open the filter dialog box and click **Select All**.

3.2.1.4 Searching a List

A filtered or non-filtered list can be searched.

Note: A search only runs on the items currently in the list. Items hidden because of filtering are not included in the results.

1. Enter any text, such as part of a name, in the **Search** field.
2. Click **Update** (check mark).
3. To display all items again:
   a. Clear the **Search** field.
   b. Click **Update**.

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 11: 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 13: Global Configurations** for instructions.
- **Identity**: provides screens for configuring cardholders and access levels. See **Chapter 14: 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 15: Configure Access Control** for instructions.
- **Video**: provides screens for configuring installed cameras, NLSS HD Media Decoders, and external storage devices. See **Chapter 16: Configure Video, Storage, & Decoders** for instructions.
- **Permissions**: create *Groups*, *Roles*, and *Users*.

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

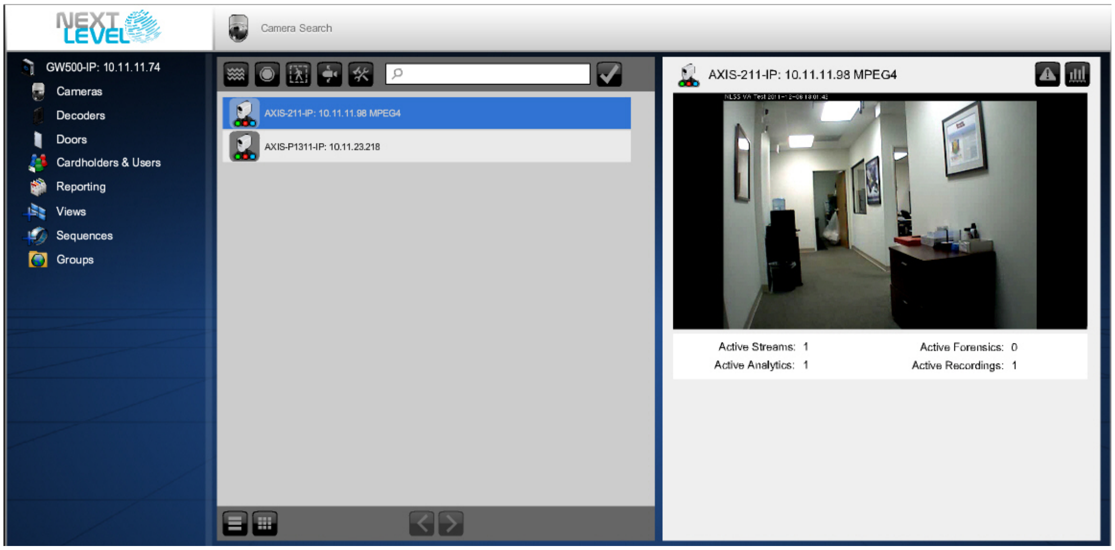
Access to cameras operations and configurations, in general, is controlled by permissions. Access to specific, pre-configured cameras can be controlled by groups. See **Chapter 17: Configuring Permissions** for more information.

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 connect to the camera, which requires configuring the camera to use its user name and password. See **Configure Cameras and Streams** for configuration instructions.

1. Select **Operations > Cameras** from the Main Menu of the NLSS Web Interface.

   A list of discovered cameras, RTSP and HTTP video streams is displayed.



AXIS-211-IP: 10.11.11.98 MPEG4

AXIS-P1311-IP: 10.11.23.218

AXIS-211-IP: 10.11.11.98 MPEG4

Active Streams: 1
Active Analytics: 1
Active Forensics: 0
Active Recordings: 1

Note: The grid view displays a thumbnail of the camera's stream.

2. Click the corresponding link to select a camera or video stream.

   A preview of the video is displayed in the far right panel.

   See **Operations Panels** for more information on these panels.

   The video preview pane contains a series of fields and options.

   – The name of the camera or stream.

   – Links to Events and Reports for that camera or stream.

   – Active statistics:

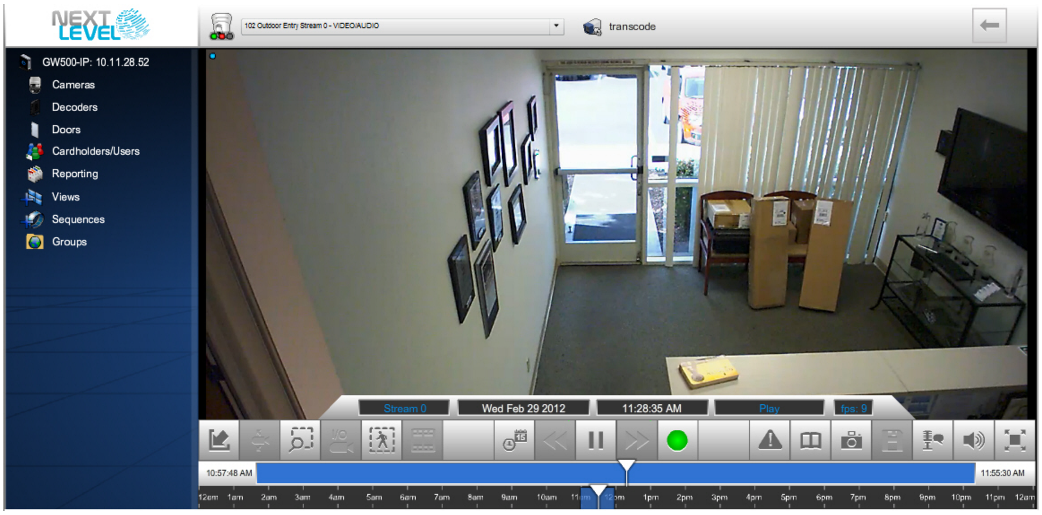
     » **Active Streams**: the number of streams available from this feed. Some cameras provide multiple streams, which can be set to different resolutions, codecs, or both. For example, a higher resolution stream may be used for a live feed, while a lower resolution stream is sent to recording to save disc space.

     » **Active Analytics**: the number of *Video Analytics* running on this camera or stream. The best practice for best performance is to run no more than one analytic at a time on a camera or stream. See **Video Analytics** for more information.

     » **Active Forensics**: the number of Forensics currently running on video recorded from this camera or stream. Best practice is to run no more than one Forensic at a time. See **Video Forensics** for more information.

     » **Active Recordings**: the number of recordings being run for this camera or stream. See **Using the Camera Toolbar** for instructions using recordings.

3. Click in the preview pane to open the video player with its controls. A stream selection drop-down menu is available above the player. See **Using the Camera Toolbar** for more information on using the video 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 many camera features, as listed in this chapter. However, some cameras do support the same features. For example, not all cameras have audio or Pan-Tilt-Zoom (PTZ) capabilities. 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 displayed next to each camera's name indicates the operational state of the camera.

Camera icons vary according to the camera model.

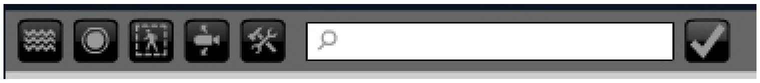
The Streaming symbol indicates an RTSP or HTTP video stream.

- 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.

  A blue dot on a screen in an RMS system indicates a peer-to-peer connection between the camera and Gateway. The video signal bypasses the RMS server.
- 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.

4.1.1 Filtering the Camera List

The Camera List can be filtered to only display cameras meeting specified search criteria. See **Filtering Operations Lists** for more information.



Filtering options:

Connection State: Connected, Connecting, Not Connected

Active Recording: All, Active, Inactive

Active Analytics: All, Active, Inactive

PTZ: All, Yes, No

Admin State: In Service, Out of Service, Preprovisioned

Use these buttons to filter the list. One or more options can be used to filter the list.

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, add one or more *NLSS HD Media Decoders* in your system.

- **Monitor Cameras from the Operations Menu**
- **Using 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**
  - Select from the camera list and open the video player, as described in **Selecting Cameras**.
  - If the camera outputs more than one stream, and these streams are enabled, select a stream from the drop-down list above the video player. Streams are enabled when the camera is configured.
  - Use the toolbar under the video player to control the selected camera. See **Using the Camera Toolbar**.
- **Operations > Views/Sequences**
  - Select View or Sequence to launch a user-configured display of one or multiple cameras or video streams. See **Chapter 5: Displaying Video** for instructions on configuring and using Views and Sequences.

Optionally, you can push streams to remote monitors via the NLSS HD Media Decoders in your system. See **Push Views and Sequences to Decoders** for details.

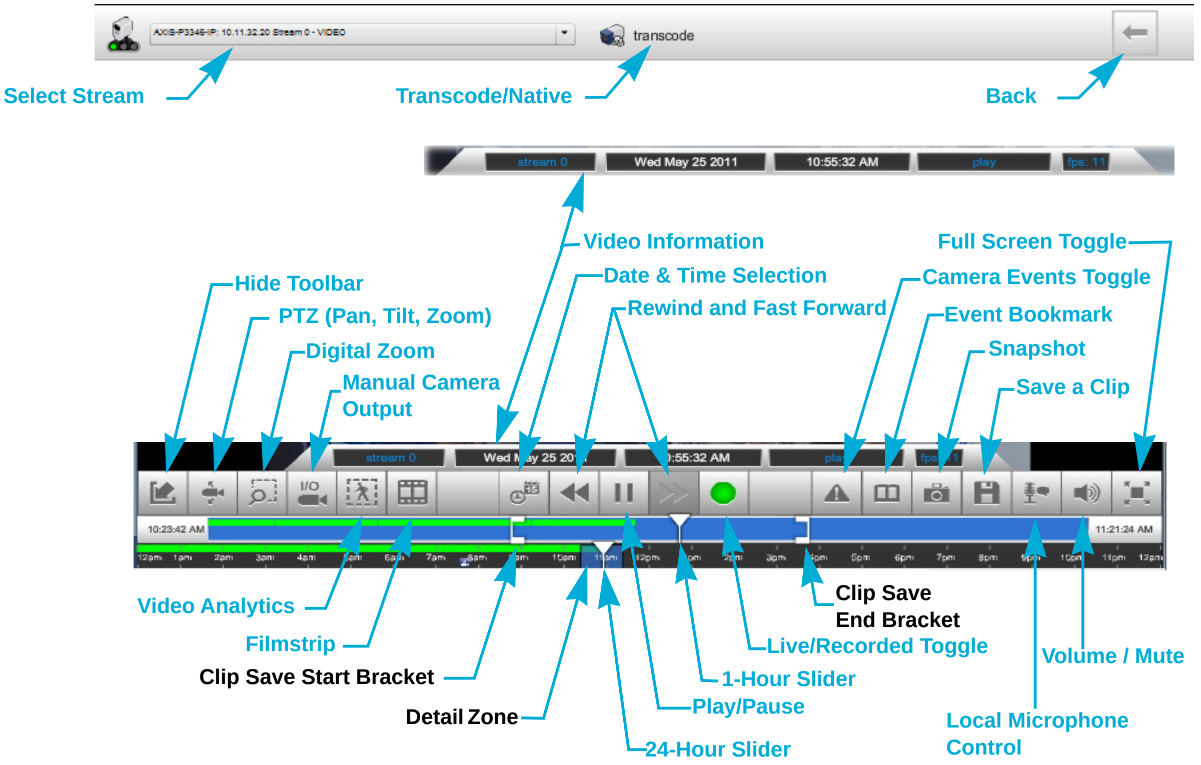
4.2.2 Using the Camera Toolbar

The *Camera Toolbar* controls the video player, and the camera or video stream displayed in the video player. The video player is opened by clicking on the preview pane when a camera or video stream is selected.

The toolbar appears under the embedded video player for both live and recorded video.

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

Specific tool bar operations on the can be controlled by permissions. See **Chapter 17: Configuring Permissions** for more information.



4.2.2.1 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 currently displayed, as selected from the drop-down list above the video player. See **Select Stream**.

Note: Some cameras output multiple streams simultaneously. Each streams can be set to a different codec or resolution, via the camera.

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

4.2.2.2 *Hide* Toolbar

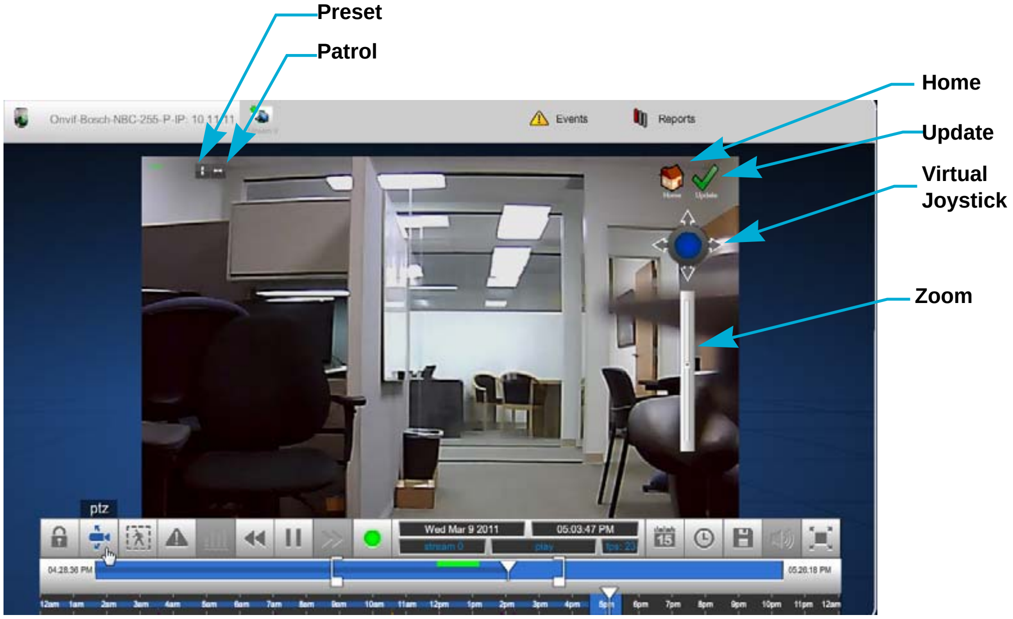
The Camera Toolbar can be temporarily hidden.

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

4.2.2.3 *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.

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



   - **Pan and Tilt**: click and drag 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 and drag the vertical zoom slider to zoom the camera.
   - **Preset**: saves the current position of the selected camera. See **Using Presets** for more information.
   - **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.

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

4.2.2.3.1 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. Select **Operations > Cameras**.
2. Select a PTZ-enabled camera.
3. Click the preview pane. The video from that camera is displayed in the video player.
4. Click **PTZ** in the toolbar.

   After PTZ is accessed, presets for that camera can be configured:

   – **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 **Update** ✓ to set this position as the Home preset.

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

CREATE CUSTOM PRESETS

In addition to a Home preset, custom presets can be added.

1. Move and zoom the camera to the desired position for the first preset.
2. Click **Preset** in the upper left to display the **Add** button (blue plus sign (**+**) in the middle of the screen).
3. Click **Add** (**+**) to display the *Add PTZ Preset* dialog.
4. In the dialog, enter a unique **Preset Name** and **Preset ID** number.
5. Click **Update** (✓) 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 **Preset** again to hide the **Add** button.

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

USE CUSTOM PRESETS

1. Click **Preset** to display the PTZ Preset List.
2. 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 **Preset** to display the PTZ Preset List.
3. In the PTZ Preset List, click **Update** (✓) 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 Update.

Delete Presets

1. Click **Preset** to display the PTZ Preset List.
2. Click the **Trash Can** next to the Update button for the Preset that you want to delete.

4.2.2.3.2 Using Patrols

When you activate a Patrol, the 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. Select **Operations > Cameras**.
2. Select a PTZ-enabled camera.
3. Click the preview pane. The video from that camera is displayed in the video player.
4. Click **PTZ** in the toolbar to access the Patrol functionality.

   From the PTZ screen, Patrols for the camera can be configured:

   – **Create Patrols**

   – **Use Existing Patrols**

   – **Delete Patrols**

Create Patrols

1. Click **Patrol** in the upper left to display the **Add** button (blue plus sign (**+**) in the middle of the screen).
2. Click **Add** to display the *Add PTZ Patrol* dialog.
3. In the dialog, enter a **Patrol Name** and **Patrol ID**.
4. Click **Update** (✓) to save the new Patrol.

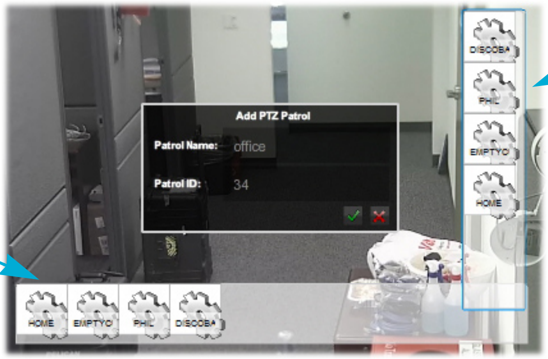
   – Click **Cancel** (red **X**) to ignore the setting and close the dialog.

Configure and Edit Patrols

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

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

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


Presets

Presets for Patrol

Add PTZ Patrol

Patrol Name: office

Patrol ID: 34

- 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 from a 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 **Update** (✓) to save the new Patrol.
      » Click **Cancel** (**X)** to ignore the setting and close the dialog.

Use Existing Patrols

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

Delete Patrols

1. Click **Patrol** to display a list of existing patrols.
2. Click the **Trash Can** next to a Patrol to delete it.

4.2.2.4 Digital Zoom

1. Click **Digital Zoom**. The *Magnifying Glass* tool is opened.
2. Move the zoom slider up and down to zoom in and zoom out in the video player.
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 **Digital Zoom** 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's display.

4.2.2.5 Manual Camera Output

Click this button in the toolbar to enable the camera's output port for five seconds. The output triggers a contact switch which can be used to trigger an alarm or warning light, or lock or unlock a door.

4.2.2.6 Video Analytics

A *video analytic* recognizes certain movements and 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 run only one analytic 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. A 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

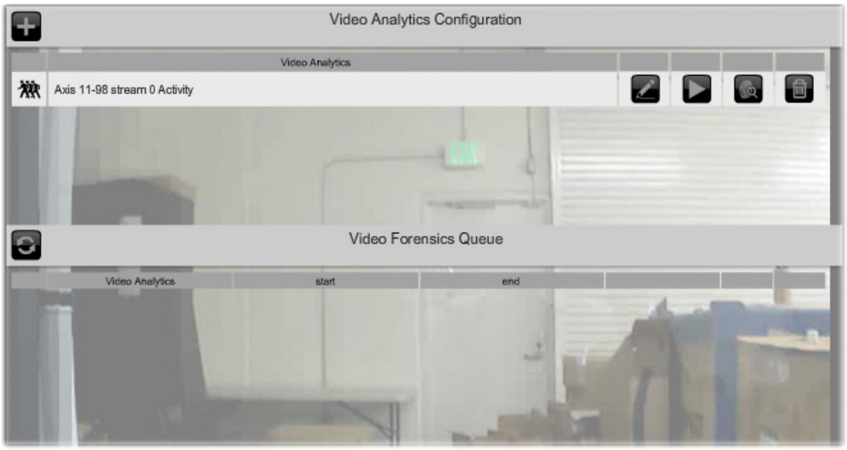
Metric Level	Video Analytic
2	Dwell Object Moved Object Taken
3	Forensic Video Analytics

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.

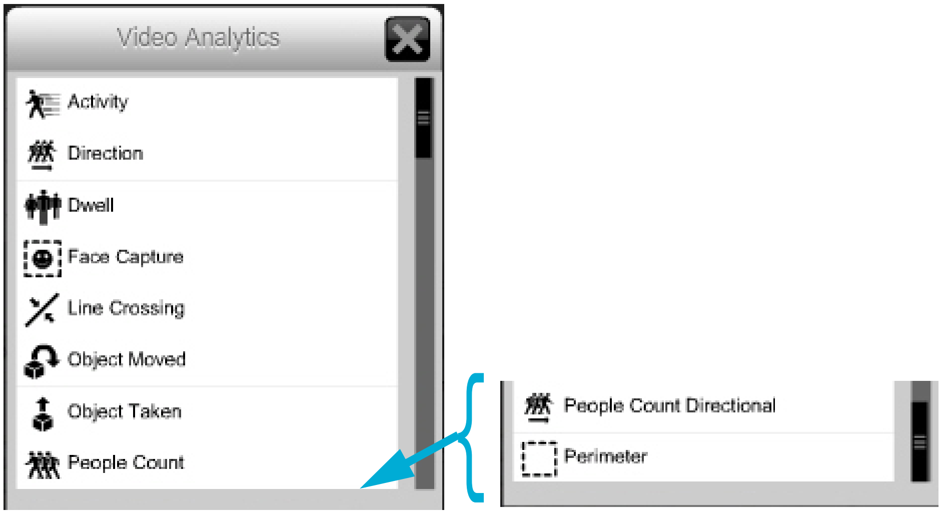
Important: The optimal setting for Video Analytic success is 12.5 frames per second. If the camera is set to a lower frame rate, the Video Analytic accuracy is compromised. If too many Video Analytics are configured, the system automatically decreases Video Analytic frame processing in order to maintain total system reliability. The Video Analytic accuracy then decreases.

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 **Analytics** in the toolbar again to hide these overlays.



3. Click **Add Video Analytics** (**+**) 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 **Edit** 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 **Save** to keep the settings.

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

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

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

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

4.2.2.6.1 Activity

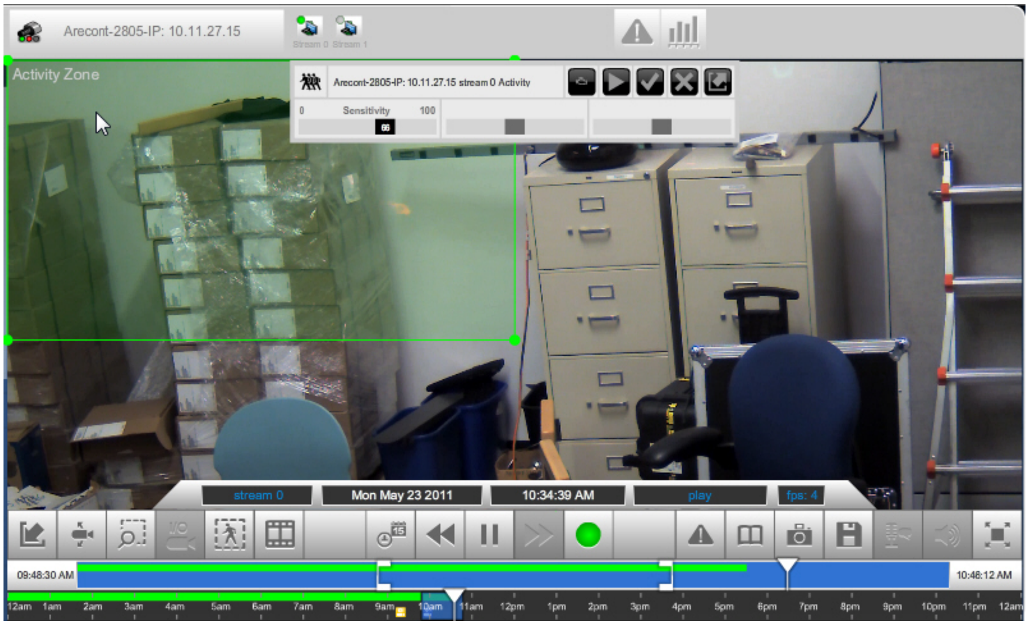
Activity detects movement within a selected area. Use edit mode for this analytic to draw the area to be monitored.

1. Click **Edit** 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. Drag the rectangle to move it to the area that you want to monitor.

3. Drag the rectangle's corner points to resize and reshape it to set the area to be monitored.


Arecont-2805-IP: 10.11.27.15
Stream 0
Stream 1
Activity Zone
Arecont-2805-IP: 10.11.27.15 stream 0 Activity
0
Sensitivity
100
66
stream 0
Mon May 23 2011
10:34:39 AM
play
fps: 4
09:48:30 AM
10:48:12 AM
12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm 12am

4. Adjust the **Sensitivity** slider to set the threshold of this video analytic. Higher values make this video analytic more sensitive to small movements and small objects.

5. Click **Save** to keep the changes.

6. Click **Start** to activate this video analytic. If someone (or something large enough) moves through the rectangle, a video analytic event is generated.

4.2.2.6.2 Direction

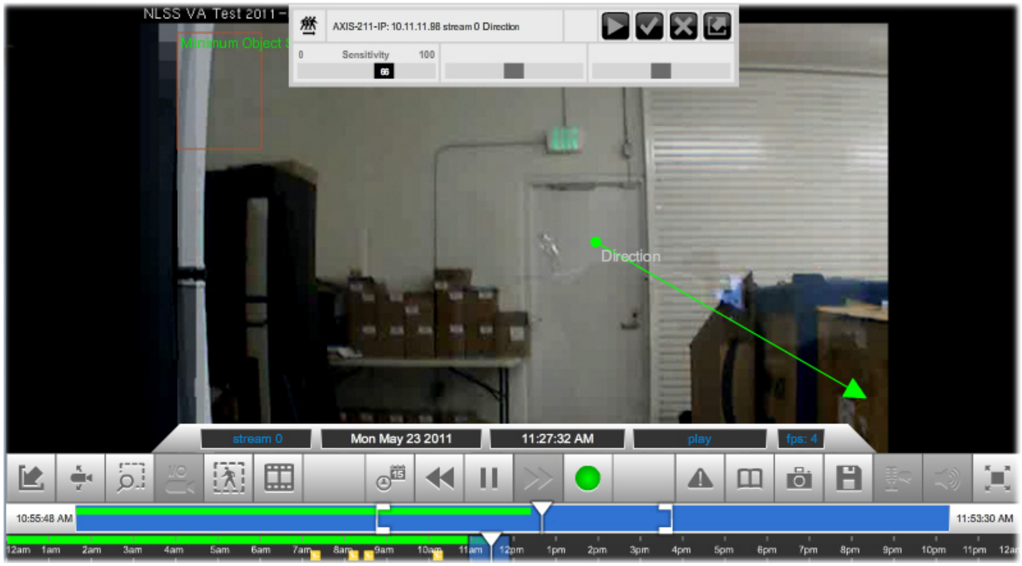
Direction detects movement toward a specific area within the video stream. The direction is defined by drawing a directional line in the video player.

1. Click **Edit** 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.

2. Drag the line to move its location in the video stream.

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


NLSS VA Test 2011 -
AXIS-211-IP: 10.11.11.88 stream 0 Direction
0
Sensitivity
100
66
Minimum Object S
Direction
stream 0
Mon May 23 2011
11:27:32 AM
play
fps: 4
10:55:48 AM
11:53:30 AM
12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm 12am

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 **Save** to keep the changes.
6. Click **Start** to activate this video analytic. A video analytic event is generated if a movement is detected for the set direction and distance.

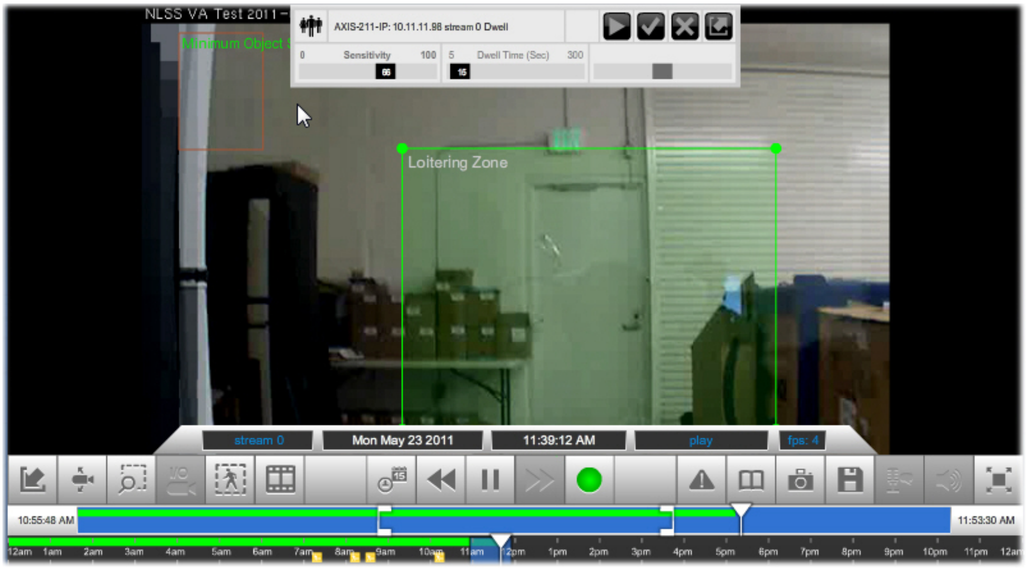
4.2.2.6.3 Dwell

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

1. Click **Edit** 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. Drag the rectangle to move the rectangle to the area that you want to monitor.

3. Drag the corner points of the rectangle to resize and reshape it to select 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 the lack of movement.

5. 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.

6. Click **Save** to keep the changes.

7. Click **Start** 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.

4.2.2.6.4 Face Capture

Face Capture records all clearly visible faces as events. The faces can be seen later by displaying the events referencing them.

1. Click **Edit** for **Face Capture** in the Video Analytics Configuration list.

   The video player is displayed with a rectangular *Face Capture Zone* highlighted.

2. Drag the rectangle to move the Face Capture Zone to the area that you want to monitor.

3. Drag the corner points of the rectangle to resize and reshape it to select the area to be monitored.

4. 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.

5. Click **Save** to keep the changes.

6. Click **Start** to activate this video analytic.

A square, labeled *Minimum Object Size*, is displayed to indicate the minimum size that a face image on the screen 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.

4.2.2.6.5 Line Crossing

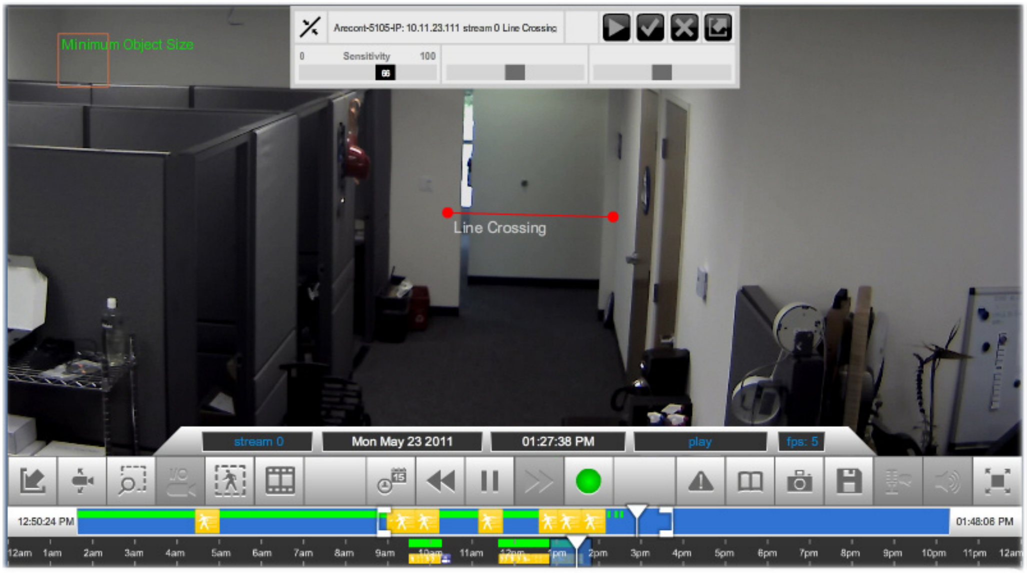
Line Crossing monitors movement that crosses a line drawn in the screen being monitored.

1. Click **Edit** for **Line Crossing** in the Video Analytics Configuration list.

   The video player is displayed with a red line labeled *Line Crossing* displayed.

2. Drag the line to move it to the location that you want to monitor, such as a door or hallway.

3. 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 detect must cross it.



Arecont-5105-IP: 10.11.23.111 stream 0 Line Crossinc

Sensitivity: 0 – 100, set to 66

Minimum Object Size
Line Crossing
stream 0
Mon May 23 2011
01:27:38 PM
play
fps: 5
12:50:24 PM
01:48:06 PM
12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm 12am

4. Use the **Sensitivity** slider to adjust the threshold of this video analytic. Higher values increase sensitivity to small movements.

5. Click **Save** to keep the changes.

6. Click **Start** to activate this video analytic. If a person or object crosses the line in either direction, a video analytic event is generated.

4.2.2.6.6 Object Moved

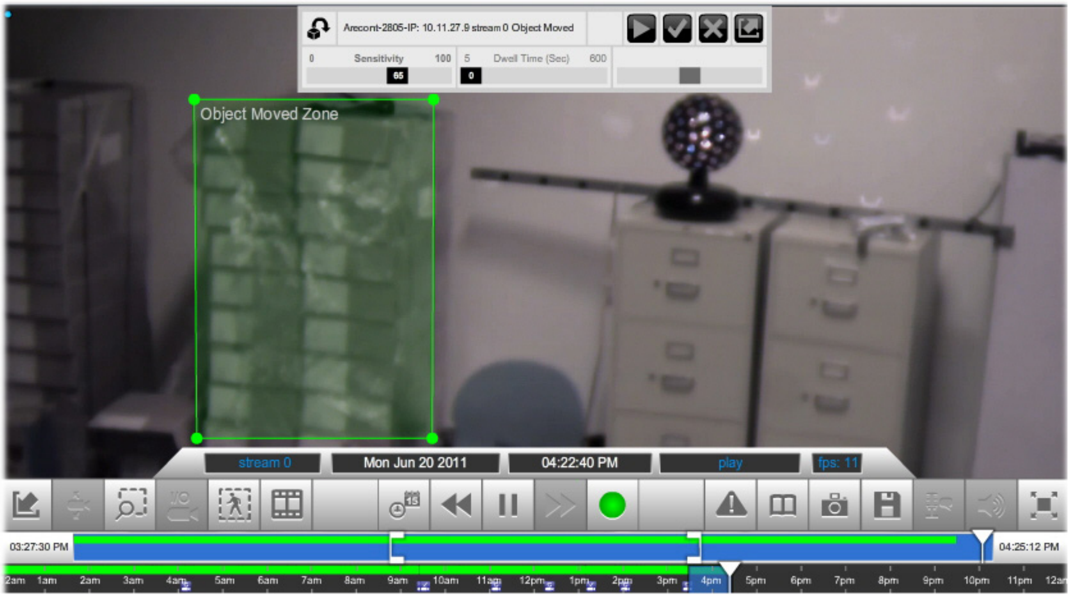
Object Taken monitors for objects that are placed in or removed from an area.

1. Click **Edit** 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. Drag the rectangle to move the rectangle to the area that you want to monitor. The smaller the box, the more precise the monitoring.

3. Drag the corner points of the rectangle to resize and reshape it to select the area to be monitored.



Arecont-2805-IP: 10.11.27.9 stream 0 Object Moved

0 Sensitivity 100: 65

5 Dwell Time (Sec) 600: 0

Object Moved Zone
stream 0
Mon Jun 20 2011
04:22:40 PM
play
fps: 11
03:27:30 PM
04:25:12 PM
2am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm 12am

4. 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.

5. 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.

6. Click **Save** to keep the changes.

7. Click **Start** 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.

4.2.2.6.7 Object Taken

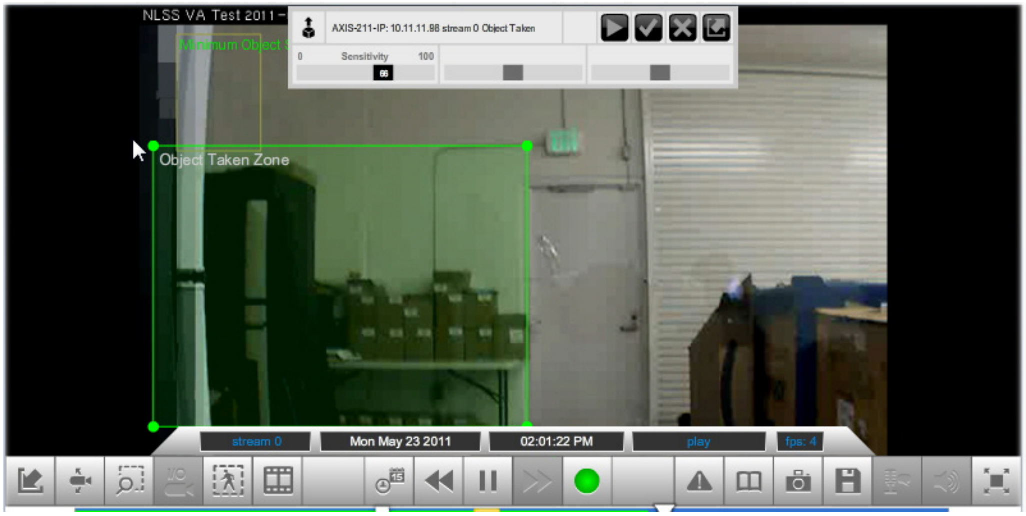
Object Taken monitors for objects removed from a selected area.

1. Click **Edit** 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.

2. Drag the rectangle to move the rectangle to the area that you want to monitor.

3. Drag the corner points of the rectangle to resize and reshape it to select 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 an object being removed.

5. Click **Save** to keep the changes.

6. Click **Start** to activate this video analytic. If an object is removed from the Object Taken Zone, a video analytic event is generated

4.2.2.6.8 People Count

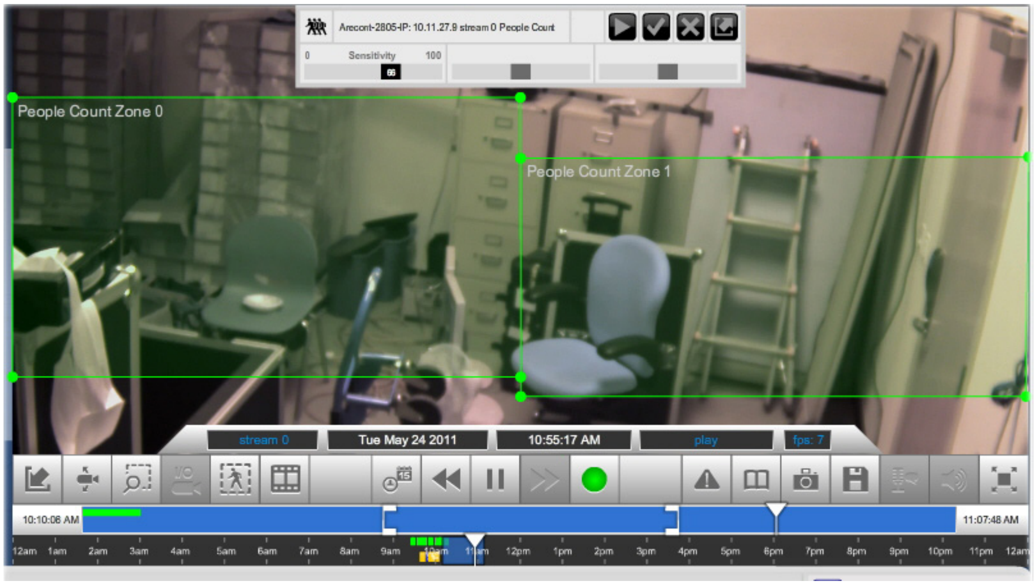
People Count monitors the number of people moving from one zone to another in the video stream. The count is done in either direction.

1. Click **Edit** 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*.

2. Drag each rectangle to move it where you want monitor in the video stream.

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



Arecont-2805-IP: 10.11.27.9 stream 0 People Count

Sensitivity: 66 (0–100)

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 **Save** to keep the changes.

6. Click **Start** to activate this video analytic. If someone moves from one zone to the other, in either direction, a video analytic event is generated.

4.2.2.6.9 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.

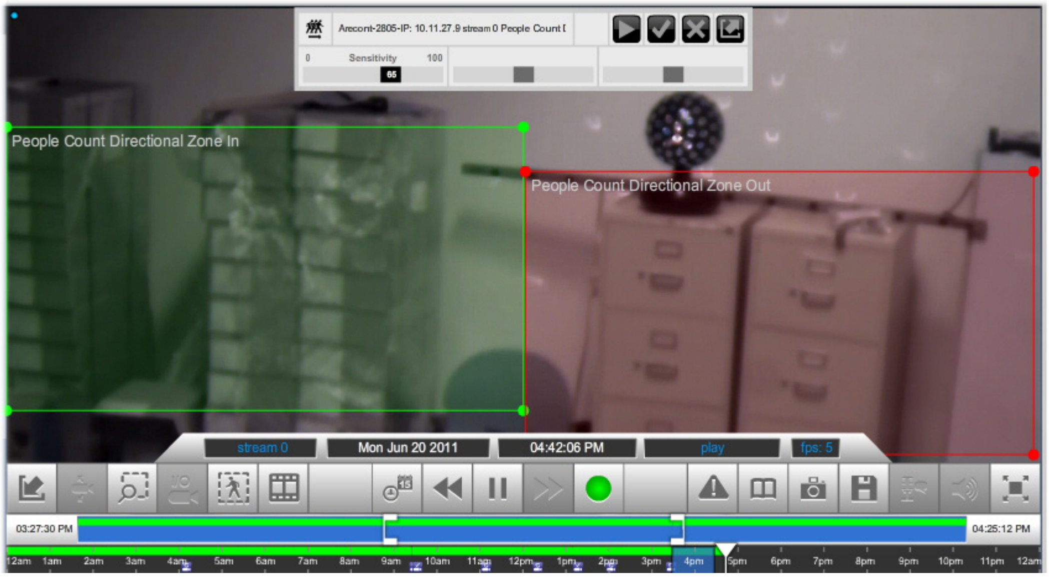
1. Click **Edit** for **People Count Directional** in the Video Analytics Configuration list.

   The video player is displayed with two highlighted areas: *People Count Zone 0* and *People Count Zone 1*.

2. Drag each rectangle to move it where you want monitor in the video stream.

Note: To register as a People Count Directional event, someone must move from the *Direction In* (green) rectangle to the *Direction Out* (red) rectangle. People moving in the other direction are not counted.

3. Drag the corner points of each rectangle to resize and reshape, so as to encompass the area to be monitored.


Arecont-2805-IP: 10.11.27.9 stream 0 People Count I
0
Sensitivity
100
65
People Count Directional Zone In
People Count Directional Zone Out
stream 0
Mon Jun 20 2011
04:42:06 PM
play
fps: 5
03:27:30 PM
04:25:12 PM
12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm 12am

4. 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.

5. Click **Save** to keep the changes.

6. Click **Start** to activate this video analytic. If someone moves from one zone to the other in the designated direction, a video analytic event is generated.

4.2.2.6.10 Perimeter

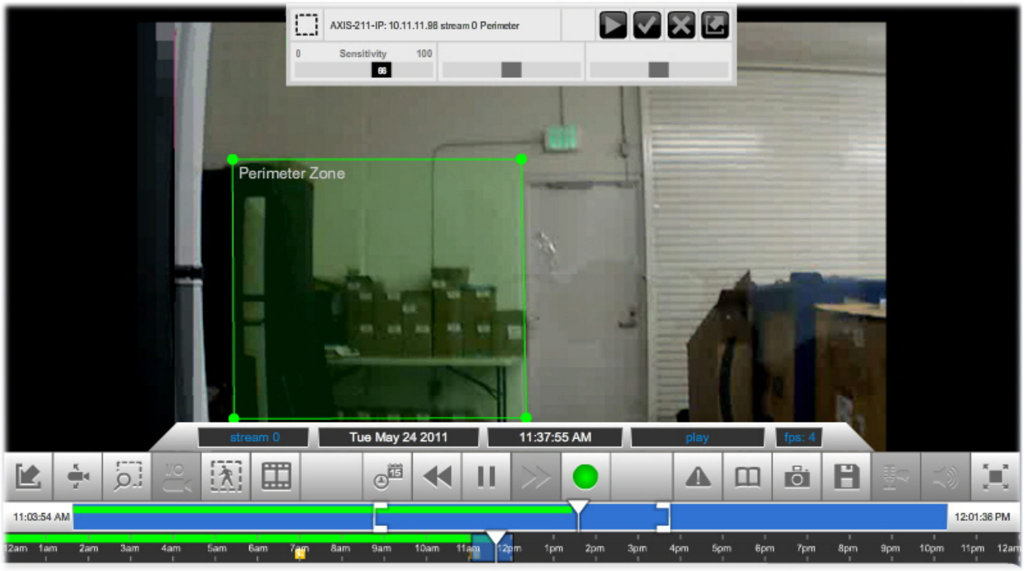
The Perimeter analytic functions similar to the Line Crossing analytic, but encompasses a four sides boundary. Any person or object that enters the Perimeter Zone from any direction is counted as an event.

1. Click **Edit** for **Perimeter** in the Video Analytics Configuration list.

   The video player is displayed with a highlighted area labeled *Perimeter Zone*.

2. Drag each rectangle to move it where you want monitor in the video stream.

3. Drag the corner points of the rectangle to resize and reshape it, so as to encompass the area to be monitored.


AXIS-211-IP: 10.11.11.98 stream 0 Perimeter
0
Sensitivity
100
66
Perimeter Zone
stream 0
Tue May 24 2011
11:37:55 AM
play
fps: 4
11:03:54 AM
12:01:38 PM
12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm 12am

4. Adjust the **Sensitivity** slider to set the threshold of this video analytic. Higher values increase the sensitivity.

5. Click **Save** to keep the changes.

6. Click **Start** to activate this video analytic. If a person or object crosses a perimeter zone boundary, a video analytic event is generated.

4.2.2.6.11 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.

4.2.2.6.12 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 or stream.
2. Click **Analytics** in the toolbar.
3. Select an analytic from the *Video Analytics Configuration* list.
   – Add and configure the analytic if it is not already in the list.
4. Click **Forensics** in the *Video Analytics Configuration* overlay. The analytic is added to the *Video Forensics Queue*.
5. 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 **arrows** to set the date and time.

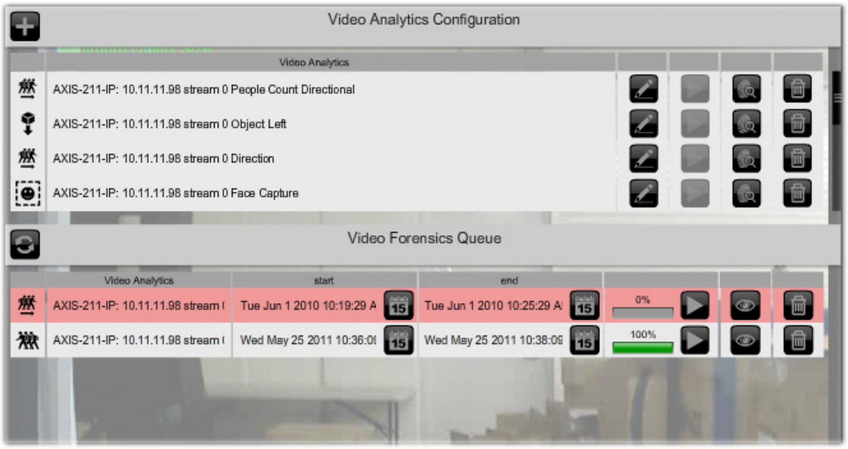
   The selected date and time are displayed in the **Start** and **End** fields.
6. Click **Play**.

   – A green bar indicates progress of the analytic. Click **Refresh** in the upper left corner of the queue to update the progress bar while 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 **Delete** (trash can) to remove the result from the queue.



Video Analytics Configuration

Video Analytics
AXIS-211-IP: 10.11.11.98 stream 0 People Count Directional
AXIS-211-IP: 10.11.11.98 stream 0 Object Left
AXIS-211-IP: 10.11.11.98 stream 0 Direction
AXIS-211-IP: 10.11.11.98 stream 0 Face Capture

Video Forensics Queue

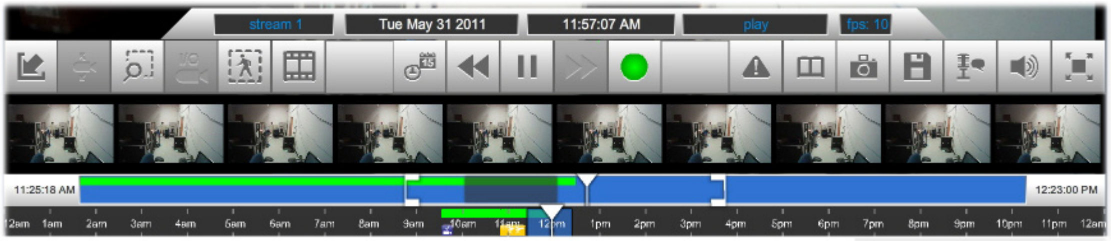
Video Analytics	start	end	
AXIS-211-IP: 10.11.11.98 stream (	Tue Jun 1 2010 10:19:29 A	Tue Jun 1 2010 10:25:29 A	0%
AXIS-211-IP: 10.11.11.98 stream (	Wed May 25 2011 10:36:0	Wed May 25 2011 10:38:09	100%

4.2.2.7 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 a camera or stream.
2. Click **Filmstrip** in the video player.

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


stream 1
Tue May 31 2011
11:57:07 AM
play
fps: 10
11:25:18 AM
12:23:00 PM
12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm 12am

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 **Filmstrip** to hide the dialog.
5. Click the **Live/Recorded Toggle** to return to live video.

4.2.2.8 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 **Date & Time**.

   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 calender.

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.

4.2.2.9 *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 **Play/Pause** in the toolbar to access recordings made from this camera.

2. In the toolbar, use the **Date & Time Selection** buttons, the **Time Sliders**, or both, 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 **Rewind** and **Fast Forward** buttons repeatedly to cycle between 0.5x, 2x, 5x, and 10x speed.

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

4.2.2.10 *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. Open a camera or stream 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, the **Time Sliders**, and the **Rewind and Fast Forward** buttons.

3. Toggle **Play/Pause** to start and stop playback.

4.2.2.11 *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 when the displayed video is live. The button turns red when playing a recorded stream.

1. Open the video player for a camera or stream.
2. In the Camera Toolbar, select the time to start playback with the **Date & Time Selection** button, the **Time Sliders**, the **Rewind and Fast Forward** buttons, or **Filmstrip** buttons.
3. To return to the live video stream, click the **Live/Recorded** toggle button.

4.2.2.12 Camera Events Toggle

Event markers can be displayed or hidden in the timeline.

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

4.2.2.13 Event Bookmark

A bookmark is a manually defined event.

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

4.2.2.14 Snapshot

A snapshot of a video clip can be grabbed from 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, 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.

4.2.2.15 *Save a Clip*

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

1. Select a camera or stream and open 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 **Save a Clip**. 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.

4.2.2.16 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. Select a camera or stream and open the video player.
2. Click **Microphone Control** in the toolbar.
3. Drag the slider up and down to increase or decrease the local microphone's volume.

4.2.2.17 *Volume / Mute*

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

1. Select a camera or stream and open the video player.
2. Click **Volume Control** in the toolbar.
3. Drag the slider up and down to increase or decrease the camera's microphone volume.

4.2.2.18 *Full Screen Toggle*

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

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

4.2.2.19 TIME SLIDERS

In the NLSS Web Interface, a pair of time sliders are located at the bottom of the toolbar, under the embedded video player: a **24-Hour Slider** and a **1-Hour Slider**.

4.2.2.19.1 24-Hour Slider

The lower time slider shows the 24-hour period of the current day, or an earlier date if the video is from an earlier date.

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 can be moved to an earlier hour on the 24-hour slider, triggering a recording to playback 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.

4.2.2.19.2 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 or stream 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**.

4.2.3 Additional Camera Controls

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

4.2.3.1 Select Stream

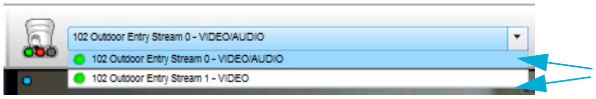
Some cameras simultaneously output more than one stream. Streams may have different codecs or resolution settings, or both. If a camera supports multiple streams, and the NLSS Web Interface is configured to handle more than one stream from that camera, then a stream can be selected to display in the video player.

A stream must be enabled in the Streams tab of the Configuration > Video > Cameras screen. See **Camera Details Stream Tab** for instructions.

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. Open the drop-down menu and select a stream to play it in the video player. A green dot next the menu item indicates the selected stream.

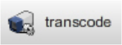

102 Outdoor Entry Stream 0 - VIDEO/AUDIO
102 Outdoor Entry Stream 0 - VIDEO/AUDIO
102 Outdoor Entry Stream 1 - VIDEO

Available Streams

The selected video stream is displayed. The drop-down and the Stream field in the toolbar list the selected stream.

4.2.3.2 Transcode/Native

If bandwidth becomes an issue for displaying video, the displayed video can be transcoded.

- Click **Transcode** in the top menu of the video player. 

The Gateway adjusts the frame rate, bit rate and resolution to alleviate bandwidth issues. The **fps** setting in the video information in the tool bar reflects the new setting. The Transcode button label now reads **Native**. The quality of the video also reflects the setting.

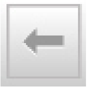
- Click **Native** to return to the camera setting for the video.

Important: Selecting these settings impacts all displayed video from the Gateway, not just the currently selected stream.

If the Gateway is accessed through RMS, only the video displayed from the selected Gateway is changed. The video displayed from the other Gateways is not effected.

4.2.3.3 Back

Click **Back** in the upper right corner of the player to return to the camera list.



4.2.4 Camera Reports and Events

1. Click **Operations >Cameras**.
2. Select a camera or video stream.
3. Click **Reports** or **Events** in the mini-pane.

   Reports

   Events

   The Reports or Events pane for the camera or video stream is displayed.

   See **Chapter 10: Operations with Reports** for instructions on using reports. See **Camera Events** and **Chapter 11: Monitoring and Handling Events** for instructions on using events.
4. Click **Return** to go back to the Cameras panel.

4.2.4.1 Camera Events

Five types of events are associated with a camera or stream:

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

An *Event Log* related to this camera or stream can be displayed. See **Camera Reports and Events**. Also, buttons of events related to this camera appear within the **Time Sliders** under the video player, offering quick access to **Playback Events**.

4.2.4.1.1 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.

4.2.4.1.2 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.

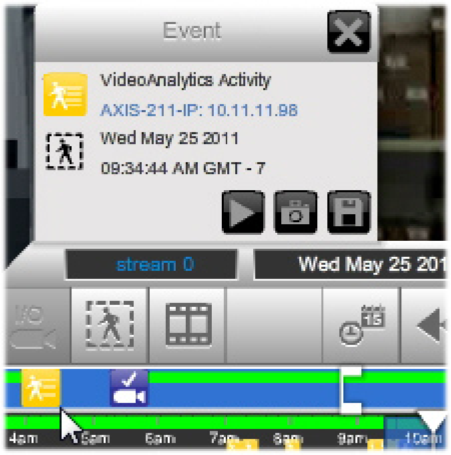
4.2.4.1.3 Viewing Events from the Timeline

Events are marked in the timeline for each camera.

1. Click the Camera Events Toggle if event markers are not displayed in the toolbar.

2. Place the 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.



Event

VideoAnalytics Activity
AXIS-211-IP: 10.11.11.98
Wed May 25 2011
09:34:44 AM GMT - 7

stream 0

Wed May 25 201

Note: If an event is clicked, the timeline cursor is placed at that location, and recorded video is played, as indicated by the red **Live/Recorded Toggle** in the timeline. Click the toggle again to return to live video, indicated by the green toggle.

3. In the dialog:

   – Click **Play** to replay the event in the video player.

   – Click **Snapshot** to take a screen shot of the event. Pause the playback in the timeline to get the exact moment to be captured.

   – Click **Save** to keep the event and prevent it from being groomed off (deleted) by the system. See **Configure Actions** for more information on grooming stored video.

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

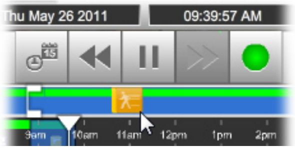
4. Click **Close** (**X**) to exit the dialog.

4.2.4.1.4 Playback Events

If the camera is set to record, then video can be played back from the time of the event.

1. Select a camera or stream and open the video player.

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.



hu May 26 2011

09:39:57 AM

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.

Chapter 5: Displaying Video

In the NLSS Web Interface, video streams from IP cameras, and RTSP and HTTP video feeds are displayed. Multiple streams can be displayed simultaneously using *Views*, and Multiple Views can be displayed in configured order using the *Sequence* feature.

Use the NLSS Web Interface to:

- **Create, Edit, and Display Views**
- **Create, Edit, and Display Sequences**
- **Push Views and Sequences to Decoders**

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, the recommended practice is to add one or more *NLSS HD Media Decoders* to the system. The NLSS Web Interface can **Push Views and Sequences to Decoders** installed in your system, and display video on HD monitors attached to those decoders.

Note: Presets, patrols, and video analytics assigned to individual cameras are preserved in Views and Sequences. See **Chapter 4: Controlling Cameras** for instructions on configuring those features.

5.1 CREATE, EDIT, AND DISPLAY VIEWS

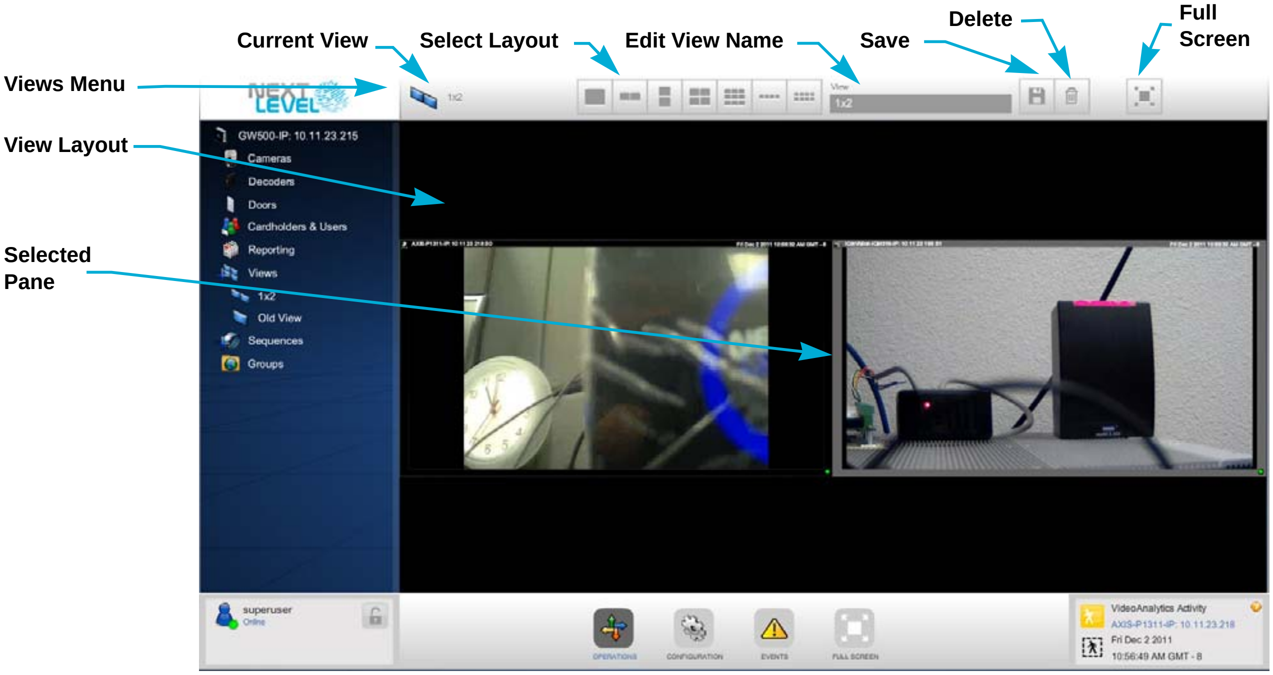
Views allows the simultaneous display of up to nine live cameras, and RSTP and HTTP streams. Use the Operations > Views menu to create, edit and display views.

Views can be used to build a Sequence. See **Create, Edit, and Display Sequences** for instructions.

Access to Views and Sequences operations and configurations, in general, is controlled by permissions. Access to specific, pre-configured Views and Sequences can be controlled by groups.

5.1.1 Views Menu and Layout

After **Operations > Views** is clicked, the *Views* menu and layout are displayed. Views can be created, edited, displayed, and deleted, using the menu options. These procedures are discussed in the following sections.



5.1.1.1 Menu Options

Use the menu options to configure the View.5

- **Current View**: the name given to the selected View.
- **Select Layout**: choose a layout from one of the seven options.

– 1x1	– 1x2 horizontal	– 2x1 vertical	– 2x2
– 3x3	– 1x4 horizontal	– 2x4 horizontal	

- **View Name**: editable field to assign a name to the current View.
- **Save**: keep any changes made to this View.

- **Delete**: remove current View from the list of Views.
- **Full Screen**: hides all menus to only display the Views Pane. When in Full Screen mode, click the Back button in the View Pane to return to the display with menus.
- **Layout**: displays the selected cameras and streams, depending on the layout selected. Cameras and video streams are assigned from the pane.
- **Selected Pane**: a light, gray frame highlights the selected pane.

5.1.2 Create Views

By default, no Views are configured for the NLSS Web Interface.

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

2. Click the **+** button next to **Views** to display a *New View* screen.
3. Select a **View Layout** to set the number and arrangement of panes in the new View.
4. Enter a **View Name**. By default *New View* is entered in the field.
5. Click in a pane to open a list of cameras and streams.
   – A light gray frame highlights the selected pane.
   – The Camera List has the same search, filter and display features as the list displayed from Operations > Cameras. See **Filtering the Camera List** for more information.
6. Select a camera or video stream to assign it to the pane.

Note: If a Pane already contains a camera or stream, then assigning a new camera or stream replaces the assignment for that pane.

7. Click **Save** in the Camera List.
8. Repeat steps 5 and 6 for the rest of the panes in the layout.
9. Click **Save** button to keep the new View.

5.1.3 Edit Views

An existing View can be edited.

1. Select **Operations > Views** from the Main Menu.
2. Select a View to display from the list in the Views menu.
3. Update the View, as needed. The **View Name** can be edited, a different layout can be selected, or a different camera or stream can be assigned to a pane or panes.
4. Click **Save** to keep the changes.

5.1.4 Delete Views

A View can be erased from the Views list.

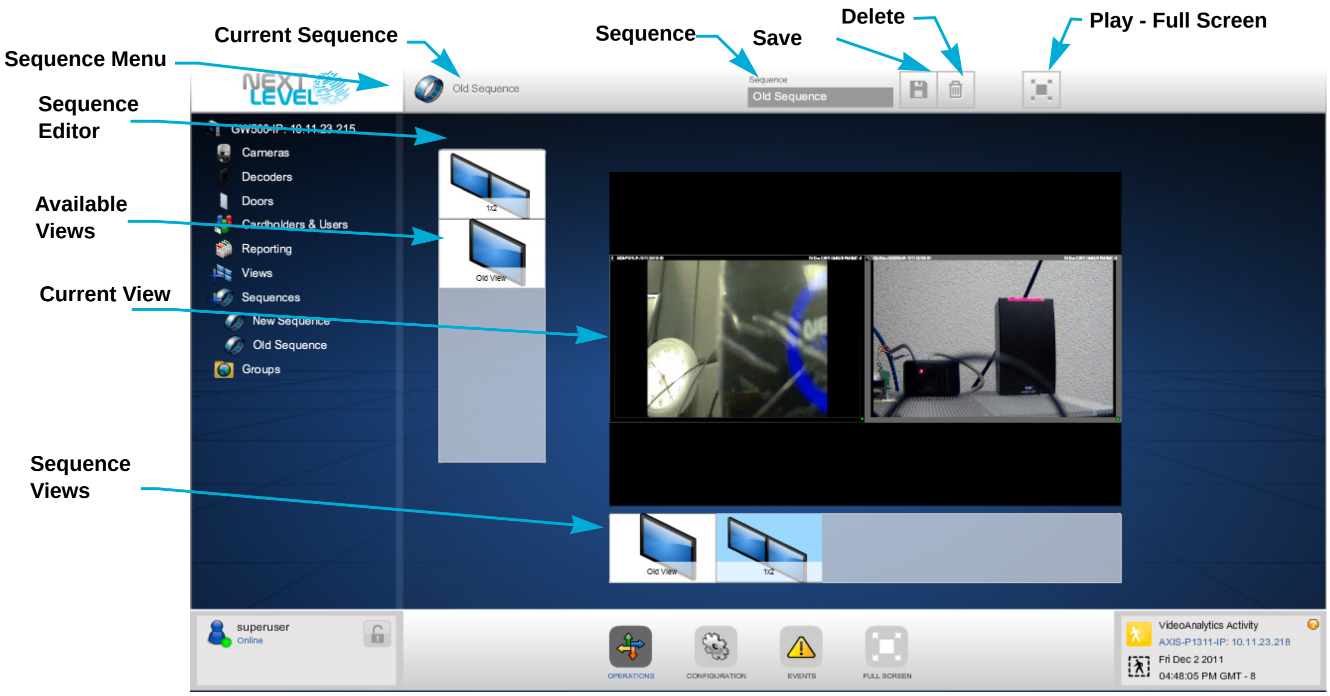
Note: A deleted View also is removed from any Sequence in which is was used.

1. Select **Operations > Views** from the Main Menu.
2. Select a View.
3. Click **Delete** (trash can) in the Views menu.

5.2 CREATE, EDIT, AND DISPLAY SEQUENCES

Sequences play a succession of Views. Sequences can be created, edited, deleted and displayed from the Sequences menu and editor.

5.2.1 Sequences Menu and Editor



- **Current Name**: the name of the currently selected Sequence.
- **Sequence**: an editable field used to assign a name to this Sequence.
- **Save**: keeps the changes made to a Sequence.
- **Delete**: erases the selected Sequence.
- **Play - Full Screen**: hides the menus and runs the Sequence
- **Available Views**: the vertical column listing the Views that have been created. See 5.1 Create, Edit, and Display Views for more information.
- **Sequence Views**: the horizontal list of the Views in this Sequence. You can add, remove, and rearrange these Views.
- **Current View**: the View selected in the Sequence Views.

5.2.2 Create New Sequences

1. Select **Operations > Sequence**.
2. Click **Add** (+) next to **Sequences**. The *Sequence Pane* is displayed.
3. Drag a View from the **Available Views** list to the **Sequence Views**.
   - To change the order of Views in the Sequence, drag-and-drop the Views into the desired order.
   - To remove a View from the Sequence, drag that View out of the Sequence Views.
4. Optionally, the duration a View is displayed can be changed. The default setting is 10 seconds.
   a. Click a View in the Sequence Views list. The *Edit Sequence Item* dialog is displayed.
   b. Enter a **Duration** (in seconds).
   c. Click **Update** ✓ to keep the change.
      » Click Cancel (X) the close the dialog without saving the change.
5. Click **Save** to keep the Sequence configuration.

5.2.2.1 EDIT A SEQUENCE

1. Select **Operations > Sequence**.
2. Select a Sequence from the list in the menu.
3. Adjust the Sequence as needed.
   - To add a View to the Sequence, drag it from the **Available Views** list to the **Sequence Views**.
   - To remove a View from the Sequence, drag that View out of the Sequence Views.
   - To change the order of Views in the Sequence, drag-and-drop the Views into the desired order.
4. To change the duration a View is displayed:
   a. Click a View in the Sequence Views list. The *Edit Sequence Item* dialog is displayed.
   b. Enter a **Duration** (in seconds).
   c. Click **Update** ✓ to keep the change.
      » Click Cancel (X) the close the dialog without saving the change.
5. Click **Save** to keep the Sequence configuration.

5.2.2.2 DELETE SEQUENCES

1. Select **Operations > Sequence**.
2. Select a Sequence from the list in the menu.
3. 🗑 Click **Delete** in the Sequence Pane.

5.2.2.3 Display Sequences

After a Sequence is created and configured, it can be played in full screen mode.

1. Select **Operations > Sequence**.
2. Select a Sequence from the list in the menu.
3. Click **Full Screen - Play**.

   The menus are hidden and the Sequence plays in the Next Level Web Interface.
4. Click **Back** to return to the menus.

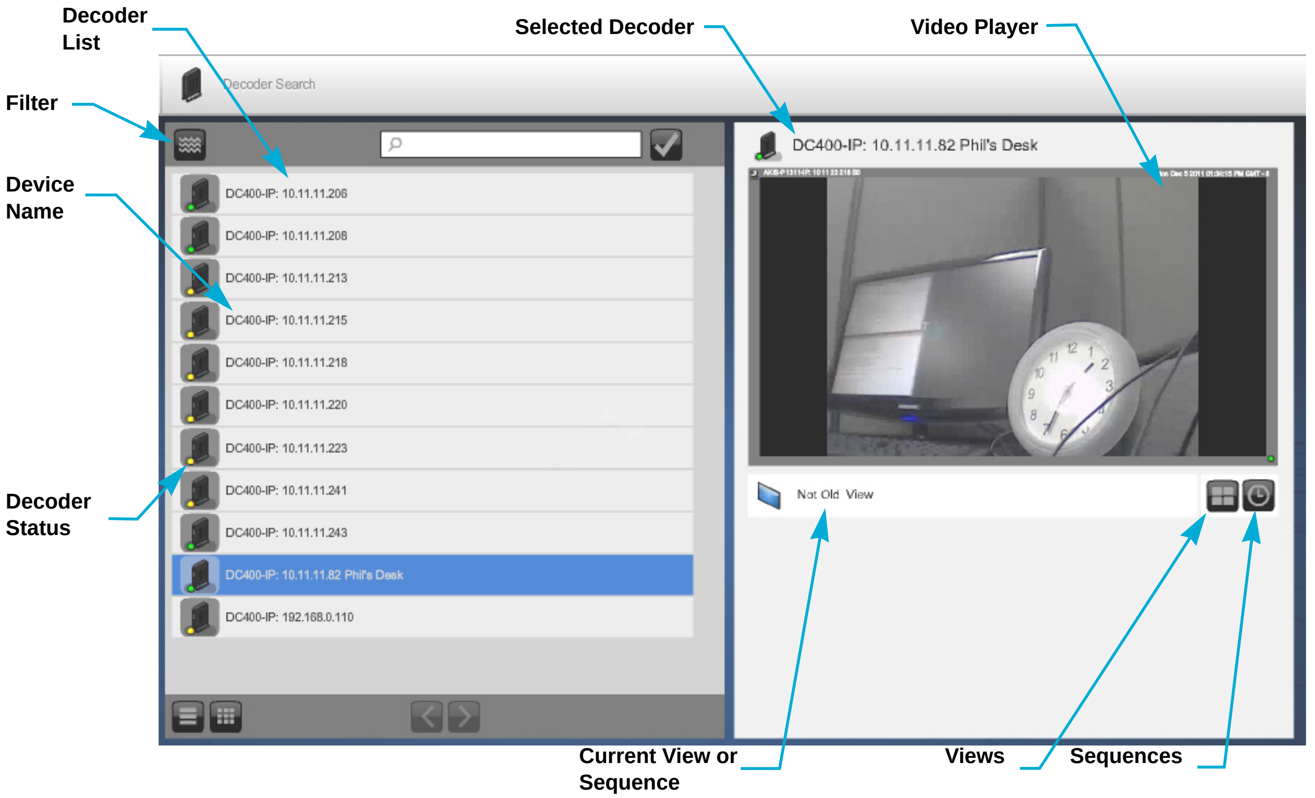
Note: Do not click the browser's Back button, as that returns to the NLSS Web Interface login screen.

5.3 PUSH VIEWS AND SEQUENCES TO DECODERS

Views and Sequences can be pushed from the Gateway to NLSS HD Media Decoders for display. Decoders can be connected to one or two monitors to display the streams. While each Decoder accepts one stream, different Views and Sequences can be pushed to other Decoders. See the *NLSS HD Media Decoder* documentation for more information.

5.3.1 Decoder Panel

When Operations > Decoders is clicked, the *Decoder Panel* is displayed. This panel contains a list of all Decoders discovered by the Gateway, plus options to push a View or Sequence from the Gateway to the Decoder. The video is also displayed.



DC400-IP: 10.11.11.206
DC400-IP: 10.11.11.208
DC400-IP: 10.11.11.213
DC400-IP: 10.11.11.215
DC400-IP: 10.11.11.218
DC400-IP: 10.11.11.220
DC400-IP: 10.11.11.223
DC400-IP: 10.11.11.241
DC400-IP: 10.11.11.243
DC400-IP: 10.11.11.82 Phil's Desk
DC400-IP: 192.168.0.110

DC400-IP: 10.11.11.82 Phil's Desk

Not Old View

The Decoder Configuration Pane contains:

- **Device List**:
  - **Device Name**: the name assigned under Configuration > Video > Decoders in this interface. The selected Device Name is displayed above the video player.
  - **Device Status**: colored dot under the Decoder icon that indicates if the Decoder is on line. Green indicates the Decoder is online; yellow indicates that the Decoder is off line.
- **Filter**: the list can be filtered on *Connection State*: **Connected** or **Not Connected**.
- **Video player**: displays the View or Sequence currently being pushed to the Decoder from this Gateway.

  A *Video Unavailable* message indicates no video is being pushed from this Gateway to the Decoder, or the Decoder is off line.
- **Current View or Sequence**: the View or Sequence being pushed to the Decoder.
- **Views**: accesses a list of Views on this Gateway.
- **Sequences**: accesses a list of Sequences on this Gateway.

Access to decoders operations and configurations, in general, is controlled by permissions. Access to specific, pre-configured decoders can be controlled by groups. See **Chapter 17: Configuring Permissions** for more information

5.3.2 Pushing a View or Sequence

1. Click **Operations > Decoders** from the Main Menu.
2. Select a Decoder.
3. Click **Views** or **Sequences**. A list of existing Views or Sequences is displayed.
   - Use the Search feature, if necessary, to locate the desired item.
   - The Views list can be filtered by layout type.
4. Select a View or Sequence.
5. Close the list.

   The selected View or Sequence is displayed in the mini-video player. This View or Sequence is now available to the Decoder.
6. Click the video player pane to hide the menus and display the View or Sequence full screen.
   - Click **Back** to return to the Operations menu.

Chapter 6: Operations with Doors

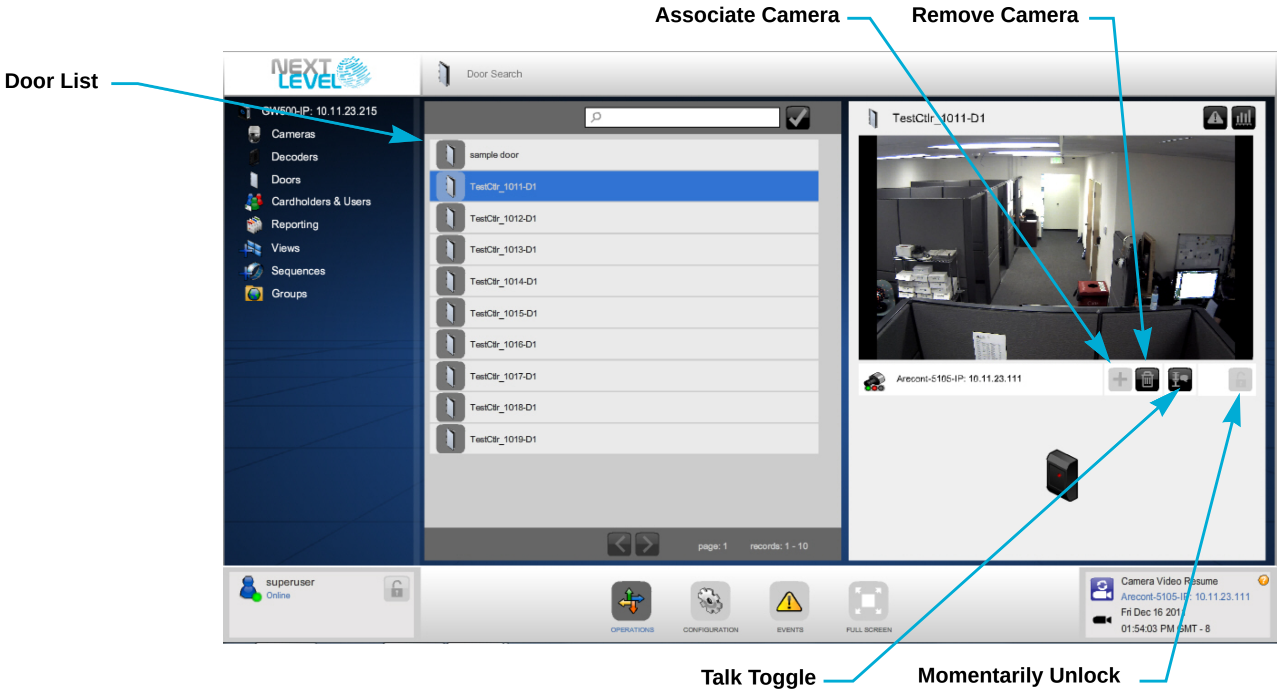
Configured doors are listed under the **Operations > Doors** menu. Operators can take the following actions with these doors:

- **Momentarily Unlock a Door**
- **Associate Cameras and Doors**
- **Open Camera Audio for an Associated Door**
- **View Event and Reports for a Door**

Access to door operations and configurations, in general, is controlled by permissions. Access to specific pre-configured doors can be controlled by groups.

6.1 DOORS PANEL

Select **Operations > Doors** to display the *Doors* panel. The panel includes a list of doors discovered by the Gateway, and a mini-pane with video, talk back, and unlock features.



6.2 MOMENTARILY UNLOCK A DOOR

If a locked door needs to be temporarily unlocked outside its scheduled time, NLSS Web Interface users can manually send a momentary unlock command to the door.

1. Click **Operations > Doors**.
2. Select a door from the list.

   The *Doors Panel* is displayed.
3. Click **Open** to unlock the door for its configured *strike time*. See **General Tab** for information on the Default Strike Time.

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

6.3 ASSOCIATE CAMERAS AND DOORS

A camera can be associated with a specific door. The camera's stream can be viewed directly from the Doors mini-pane.

6.3.1 Associating and Viewing Cameras with Doors

BY default, doors do not have cameras associated with them.

1. Click **Operations > Doors**.
2. Select a door from the list.
3. Click **Associate Camera** to display the Camera list in the mini-pane. See **Selecting Cameras** for more information about the list.
4. Select a camera or video stream.

   The video is displayed in the video player in the mini-pane.
5. Click on the video to view it in the full NLSS Web Interface Video Player.

6.3.2 Disassociate Cameras from Doors

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

1. Click **Operations > Doors**.
2. Select a door from the list.
3. Click **Disassociate Camera** to remove the link between the camera and the door.

6.4 OPEN CAMERA AUDIO FOR AN ASSOCIATED DOOR

A user can communicate via the camera speaker and a local microphone, if a camera supports audio. The **Talk** toggle allows the user to be heard through the camera's speaker.

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

1. Click **Operations > Doors**.
2. Select a door.
3. Click **Talk** to speak.
4. Click Talk again to cancel the microphone feed to the camera.

6.5 VIEW EVENT AND REPORTS FOR A DOOR

Event and Reports for a specific door can be accessed from the Doors panel.

1. Click **Operations >Doors**.
2. Select a door.
3. Click **Reports** or **Events** in the mini-pane.

   The Reports or Events pane for the door is displayed.

   See **Chapter 10: Operations with Reports** and **Chapter 11: Monitoring and Handling Events** for more instructions.
4. Click **Return** to go back to the Doors panel.

Chapter 7: Operations with Cardholders & Users

Operations > Cardholders & Users lists the people who have been assigned an access card, as well as the administrative personnel who operate the system through the NLSS Web Interface.

See **Chapter 14: Configure Identity and Credentials** for instructions on configuring cards and adding Cardholders.

See **Chapter 17: Configuring Permissions** for instructions on configuring users.

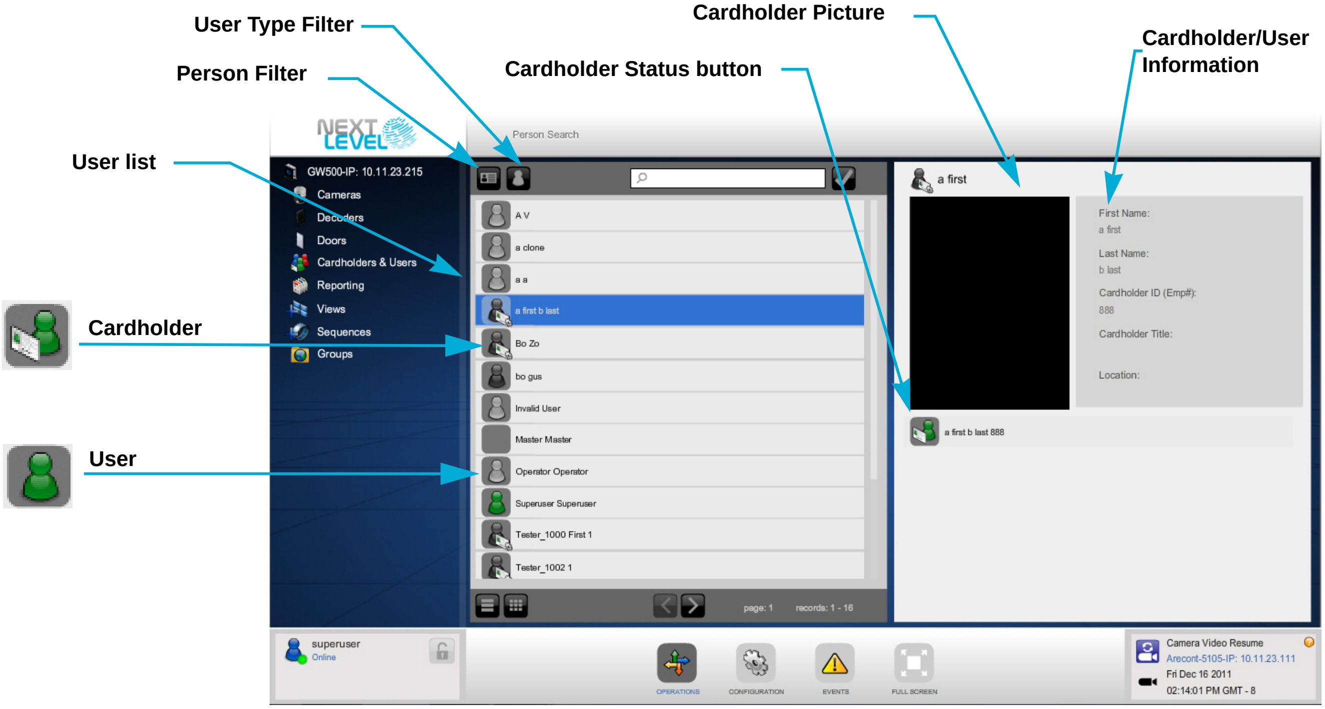
7.1 CARDHOLDERS & USERS PANEL

The *Cardholder & Users panel* contains a list of people who use or are monitored by the system, and a mini-pane that provides details about the selected person. See **Operations Panels** for more information on using this panel.

A Cardholders card can be *Enabled* or *Disabled* from the mini-pane. No actions can be taken on a user record from this panel.

Access to Cardholders/Users operations and configuration, in general, is controlled by permissions. Access to specific Cardholders/Users can be controlled by groups. See **Chapter 17: Configuring Permissions** for more information.

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



First Name:
a first

Last Name:
b last

Cardholder ID (Emp#):
888

Cardholder Title:

Location:

7.1.1 Filtering Cardholders & Users List

- **Person Type**: select either **Cardholder**, **User**, or **All**
- **User Type**: select from the configured User Types, or **All**. See **Users** in **Chapter 17: Configuring Permissions** for instructions on creating and configuring User Types.

7.2 ACTIONS WITH CARDHOLDERS

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

- **Cardholder Information**
- **Cardholder Photo**
- **Activate / Deactivate Cardholders**
- **Cardholders & Users Reports and Events**

7.2.1 Cardholder Information

These fields are populated in the Configuration > Identity > Cardholders screen. See **Cardholders Tabs** in **Chapter 14: Configure Identity and Credentials**.

The **First Name**, **Last Name**, and **Cardholder ID (Emp #)** identify the Cardholder. The Cardholder ID is a unique identifier. **Cardholder Title** and **Location** are organizational identifiers.

7.2.2 User Information

These fields are populated in the Configuration > Permissions > Users screen. See **Users**in **Chapter 17: Configuring Permissions**.

The **First Name**, **Last Name**, and **User ID (Email)** identify the Cardholder. The User ID is a unique identifier. The **User Type** identifies the permission level of this user in the NLSS system.

7.2.3 Cardholder Photo

If a photo was uploaded for the Cardholder (see **Credentials Tab**), the photo is displayed in the Cardholders mini-pane.

7.2.4 Activate / Deactivate Cardholders

Cardholders access can be activated or deactivated from the mini-pane.

1. Click **Cardholder Status** below the Information fields.

   The current status of the Cardholder is displayed, either:

   – **Card Activated**

   – **Card Deactivated**

2. Reset the Cardholder’s status.

   ☒ If the Cardholder’s status is active, click **Deactivate** to disable the card.

   ☑ If the selected card is currently inactive, click **Activate** to disable the card.

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

After Cardholder Status is clicked, the Events and Reports buttons are displayed.

7.2.5 Cardholders & Users Reports and Events

1. Click **Operations >Cardholders & Users**.
2. Select a camera or video stream.
3. Click **Reports** or **Events** in the mini-pane.

   📊 **Reports**

   ⚠ **Events**

   The Reports or Events pane for the Cardholder or user is displayed.

   See **Chapter 10: Operations with Reports** and **Chapter 11: Monitoring and Handling Events** for more instructions.

4. Click **Return** to go back to the Cardholders & Users panel.

Chapter 8: Using Floor Plans

If the NLSS Gateway is being upgraded from a previous version, and floor plans are part of the configuration, note that floor plans are now included under the Groups menu

See **Chapter 17: Configuring Permissions** for information on including floor plans or maps with a group.

See **Adding and Using Maps** in **Chapter 9: Using Groups** for instructions on uploading and using floor plans with a group.

Chapter 9: Using Groups

Groups are collections of cameras, decoders, doors, users, cardholders, views and sequences. In RMS, Groups consist of Gateways and Multiviews on the RMS Level. Groups can have different types of objects in the same group. Groups are used for access to devices and operations, not for bulk configuration of like objects.

Groups on a Gateway are used to enable and disable access to certain devices and operations for users.

Using Configuration > Permissions, items are assigned to. Groups are then assigned to *roles*, which set permissions for using the system's features. *Users* are assigned a role, defining the parameters of their permissions. If a user's role provides permission to see a group, it is displayed in Operations > Groups.

For example, a series of cameras and doors on the first floor could be placed in a group. That group is assigned to a role responsible monitoring that floor. Users are then assigned that role. Those users only would be able to operate the cameras and doors for the first floor, and would not be able to see cameras and doors from other floors.

See **Chapter 17: Configuring Permissions** for more information on how permissions work together, and instructions on setting up permissions.

9.1 GROUPS PANEL

Groups are accessed under Operations > Groups.

Two options are available for display in the Groups panel: *List View* and *Map View*.

- *List View*: a list of the grouped items is displayed. Click on an item to launch a mini-pane or viewer, depending on the item's Device Type. The display and features are the same as if the camera, door, decoder, or other device was selected from its respective Operations menu list.

  See **Groups** in **Chapter 17: Configuring Permissions** for more information on creating and maintaining groups.

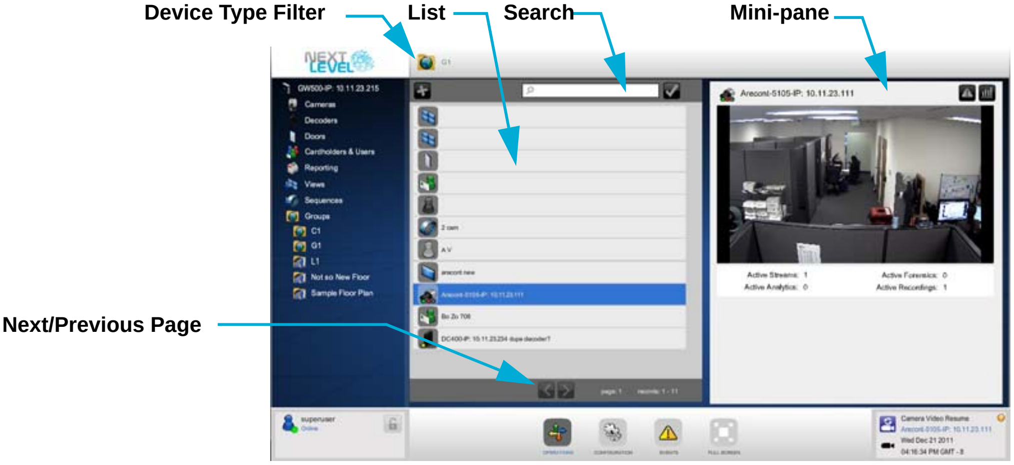
- *Map View*: if **Show Maps** was selected in Configuration > Permissions > Groups, a JPEG of a map, floorplan or graphic can be uploaded as a background graphic. Click an icon to launch a mini-pane or viewer, depending on the Device Type of the item.

  See **Adding and Using Maps** in this chapter, and **Create a Group** in **Chapter 17: Configuring Permissions** for more information.

9.2 LIST VIEW

Select **Operations > Groups > *group name***, where *group name* is the specific group.

Select a group with a globe on the folder from a List view.



- **Device Type Filter**: displays the filter dialog. The list can be filtered on a device type, or multiple types, that make up the group. Options include: Cameras, Cardholders, Decoder, Door, Group, Sequence, User, and View.

  The **Group** option allows the filter to show or hide sub-groups of the selected group.

- **List**: the items are added under Configuration > Permissions >Groups. See **Groups** in **Chapter 17: Configuring Permissions** for more information.

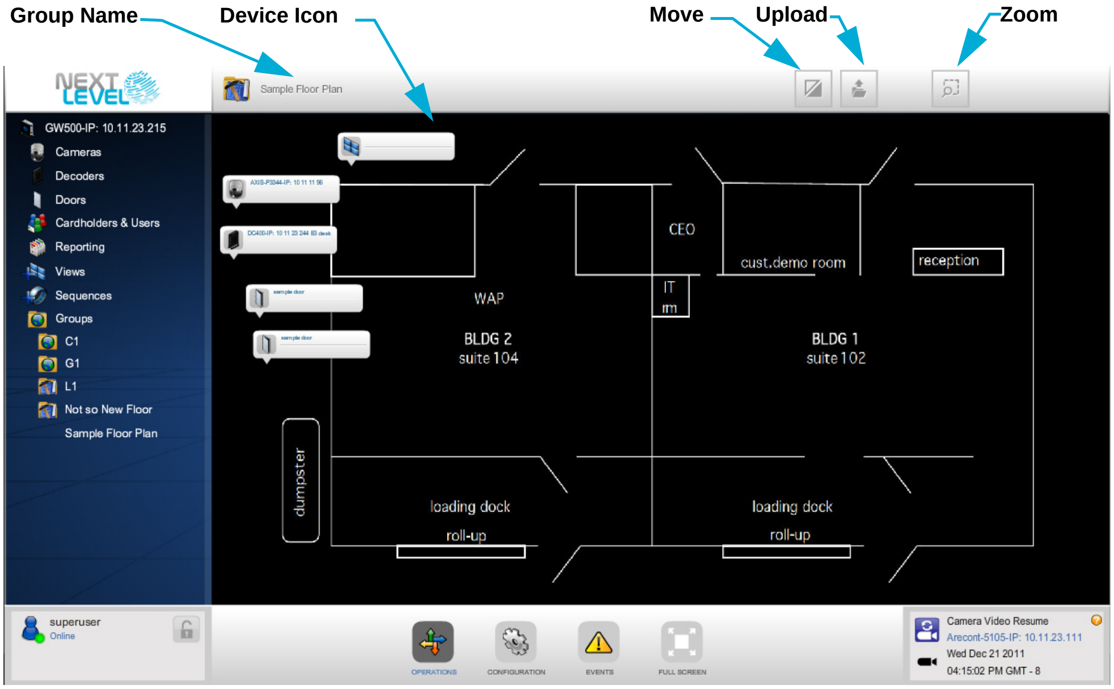
- **Search**: enter the name or part of a name of a device or multiple devices to locate in the list.

- **Mini-pane**: the display is dependent on the device type of the selected item. Views and Sequences display full screen video players.

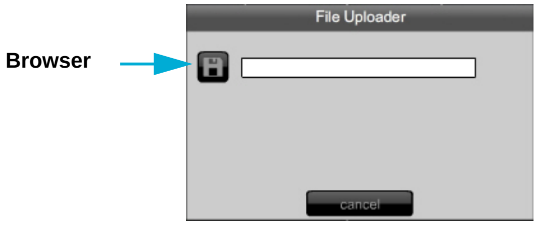
9.2.1 Adding and Using Maps

Maps allow a background image such and a map or a floorplan to be added to the group display. Devices included in the group are represented by icons. These icons can be placed in desired spots on the background to represent the device’s location. For example, door and camera icons can be placed on a floorplan to show a security layout for an office.

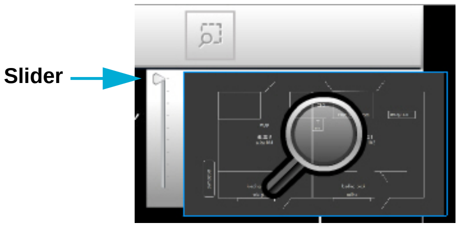
Select a group with a map on the folder for a List view.



- **Device icon**: click an icon to launch the same viewer or mini-pane that is accessed from the respective Operations menu option for that device type. For example, if a camera icon is clicked, the camera mini-pane is displayed, from which the full video player, events and reports for the camera can be accessed.
- **Move**: click **Move** to rearrange icons. Click **Move** again to lock the icons in place.
- **Upload**: click to launch the *File Uploader* dialog.
  - Click **Browser** to launch a file browser to locate the desired JPEG file.



  - Select a file and click **Open** to upload it. The image is displayed as a background when the group is selected under Operations > Groups.
- **Zoom**: Click **Zoom** to launch the Zoom feature. The *Zoom* dialog is opened.



  - Drag the slider down to enlarge the background image.

- Drag the magnifying glass to the desired location on the image.
- Click **Zoom** again to close the dialog.

Note: The image display maintains the larger size when the dialog is closed, unless the slider is dragged back to the top.

Chapter 10: Operations with Reports

Reports collect information from events tracked by the NLSS Unified Security Suite. The information displayed depends on the report type, the date/time range, and other filters.

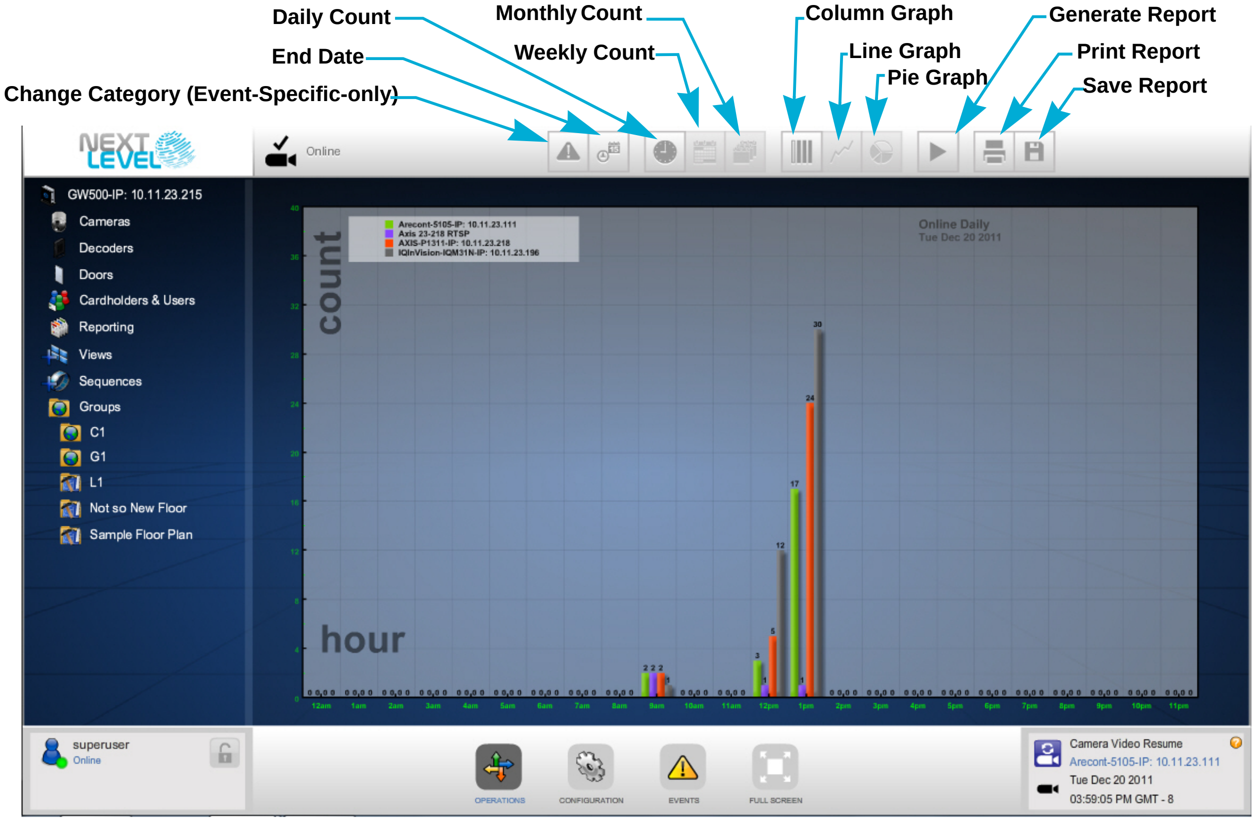
10.1 GENERATING REPORTS

Two types of reports are available.

- **Event-Specific Reports** display all instances of an event type detected in the system. These reports are accessed from Operations > Reporting, and can be tailored to specific categories and Event Types.
- **Device-Specific Reports** display activity reports for the selected items. These reports can be selected from the mini-panes for Cameras, Doors, or Cardholders & Users.

10.1.1 Reports Panel

Most features are the same for both types of reports on the Reports Panel.



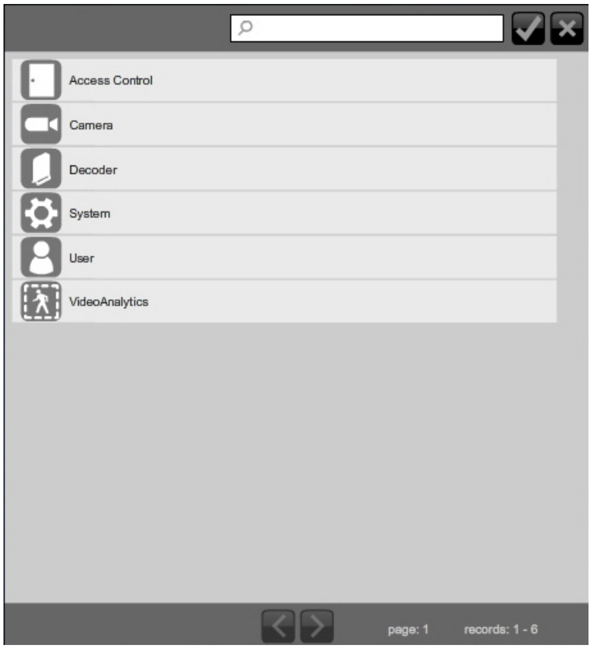
10.1.2 Event-Specific Reports

Reports generated for events tracked across the entire system are accessed from the Operations > Reporting menu.

Access to Reports, in general, is controlled by permissions.

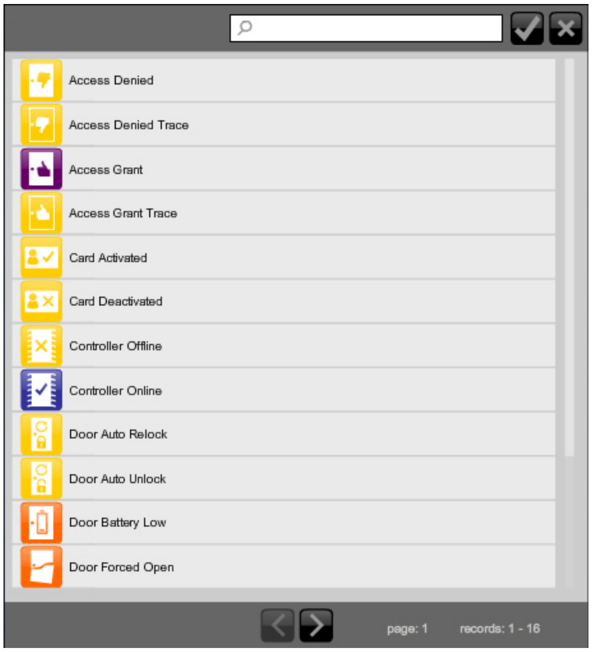
1. Select **Operations > Reporting** from the Main Menu.

   The Reports panel is opened with a Report Category list.



2. Select a category.

The *Event Type* list is displayed.



Access Denied

Access Denied Trace

Access Grant

Access Grant Trace

Card Activated

Card Deactivated

Controller Offline

Controller Online

Door Auto Relock

Door Auto Unlock

Door Battery Low

Door Forced Open

page: 1 records: 1 - 16

3. Select an Event Type from the list.
4. Click **End Date**. The Date dialog box is displayed.

   Use the arrows to select the last day and time 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.
5. Click **Save** (check mark) to set the date and time.
6. 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.
7. Select a graph type for the report: **Column**, **Line**, or **Pie**.
8. Click **Generate Report** to create the report.
   - Click **Print** to print the report.
   - Click **Save** to keep a .csv version of the report.

Report Category, **End Date**, **Counts**, and **Graphs** can be clicked at any time to create a different report.

10.1.3 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 and users, select that device and run a report.

1. Open **Operations >Cameras**/**Doors**/**Cardholders & Users**.
2. Select an item in the list.
3. Click **Reports** in the mini-pane.
4. Click **End Date**. The Date dialog box is displayed.

   Use the arrows to select the last day and time 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.
5. Click **Save** (check mark) to set the date and time.
6. 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.
7. Select a graph type for the report: **Column**, **Line**, or **Pie**.
8. Click **Generate Report** to create the report.
   - Click **Print** to print the report.
   - Click **Save** to keep a .csv version of the report.

End Date, **Counts**, and **Graphs** can be clicked at any time to create a different report.

10.2 CATEGORIES OF EVENT-SPECIFIC REPORTS

Several categories of event-specific reports are available in the Operations > Reporting menu.

10.2.1 Access Control Reports

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

10.2.2 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.

10.2.3 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.

10.2.4 System Reports

Reports on external storage and recording events.

10.2.5 User Reports

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

10.2.6 Video Analytics Reports

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

Chapter 11: Monitoring and Handling Events

Through the Events menu, incidents can be detected and tracked by an NLSS Gateway.

11.1 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.

Access to Events, in general, can be controlled by Permissions.

Events can be accessed from the Main Menu, or from Operations > Cameras/Decoders/ Doors/Cardholders & Users.

- Click **Events** in an Operations mini-pane for a selected device to access the **Event Log** only for that device.

  ⚠

- Click **Events** in the Main Menu to access the **Event Log**.

  ⚠
  EVENTS

The Event Log view provides 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.

Important: If the Events button is pulsating, an Emergency event has been generated. See **Emergency Events** for instructions.

Event Type and Event Severity are set under Configuration > Global. See **Configure Event Types** and **Configure Event Severity** in **Global Configurations** for instructions and more information.

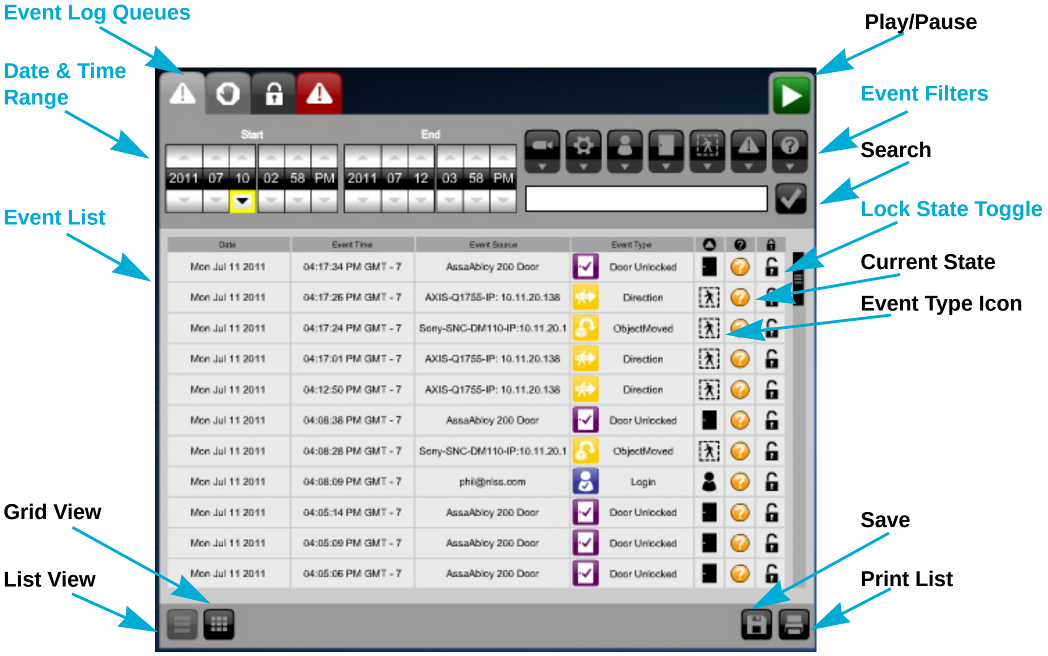
11.1.1 Event Log

The *Event Log* lists events over a specified time period. Event Details can be accessed from the Event Log List to take action and view the particulars of an event.

11.1.1.1 Event Log List

The Event Log List provides high level information on events.

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



Start: 2011 07 10 02 58 PM

End: 2011 07 12 03 58 PM

Date	Event Time	Event Source	Event Type			
Mon Jul 11 2011	04:17:34 PM GMT - 7	AssaAbloy 200 Door	Door Unlocked	■	?	🔓
Mon Jul 11 2011	04:17:26 PM GMT - 7	AXIS-Q1755-IP: 10.11.20.138	Direction	🚶	?	🔓
Mon Jul 11 2011	04:17:24 PM GMT - 7	Sony-SNC-DM110-IP:10.11.20.1	ObjectMoved	🚶	?	🔓
Mon Jul 11 2011	04:17:01 PM GMT - 7	AXIS-Q1755-IP: 10.11.20.138	Direction	🚶	?	🔓
Mon Jul 11 2011	04:12:50 PM GMT - 7	AXIS-Q1755-IP: 10.11.20.138	Direction	🚶	?	🔓
Mon Jul 11 2011	04:08:38 PM GMT - 7	AssaAbloy 200 Door	Door Unlocked	■	?	🔓
Mon Jul 11 2011	04:08:28 PM GMT - 7	Sony-SNC-DM110-IP:10.11.20.1	ObjectMoved	🚶	?	🔓
Mon Jul 11 2011	04:08:09 PM GMT - 7	phil@nlss.com	Login	👤	?	🔓
Mon Jul 11 2011	04:05:14 PM GMT - 7	AssaAbloy 200 Door	Door Unlocked	■	?	🔓
Mon Jul 11 2011	04:05:09 PM GMT - 7	AssaAbloy 200 Door	Door Unlocked	■	?	🔓
Mon Jul 11 2011	04:05:06 PM GMT - 7	AssaAbloy 200 Door	Door Unlocked	■	?	🔓

11.1.1.1.1 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.

The event is not groomed, but video eventually may be groomed. Event video only is guaranteed to be saved if total disk usage remains below 90%.

Emergency: lists events with an emergency status. See Emergency Events.

11.1.1.1.2 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.

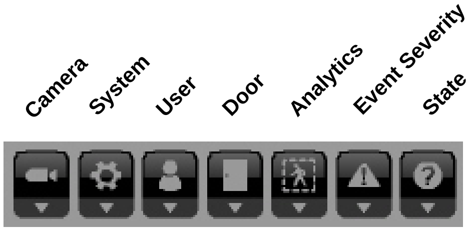
The events that occurred within that range are displayed.

11.1.1.1.3 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 applies 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.

11.1.1.1.4 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. See **Configure Actions** in **Global Configurations**.
  - 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**.

11.1.1.1.5 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.

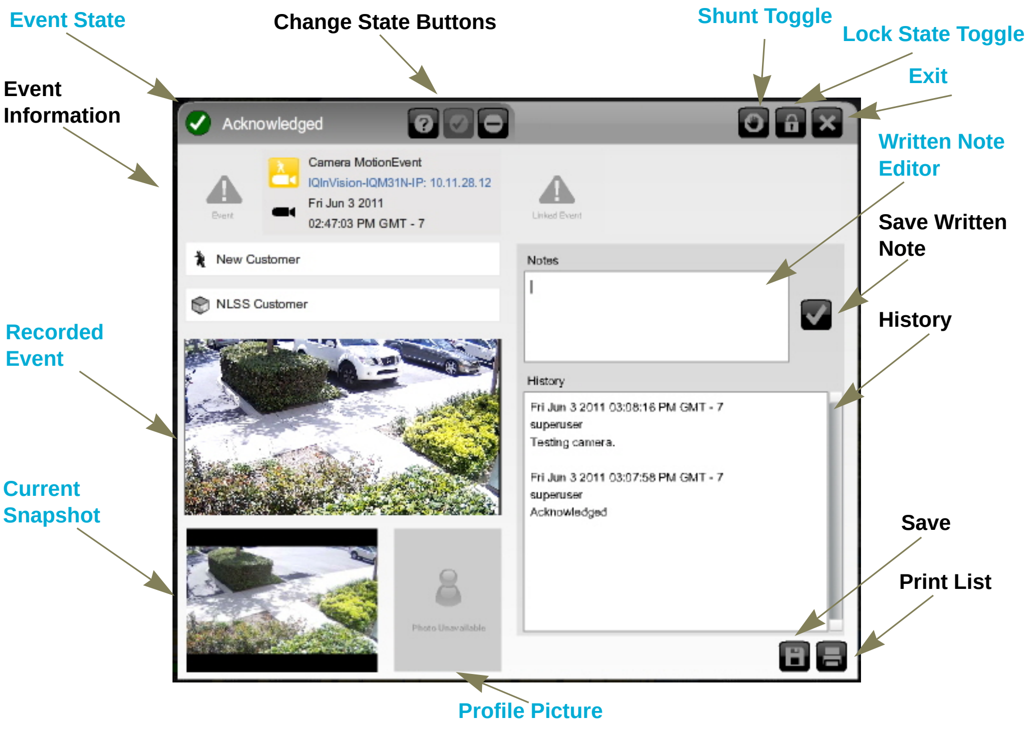
11.2 EVENT DETAILS

When an event is selected in 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.

11.2.1 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.



Camera MotionEvent
IQinVision-IQM31N-IP: 10.11.28.12
Fri Jun 3 2011
02:47:03 PM GMT - 7

New Customer

NLSS Customer

History

Fri Jun 3 2011 03:08:16 PM GMT - 7
superuser
Testing camera.

Fri Jun 3 2011 03:07:58 PM GMT - 7
superuser
Acknowledged

11.2.1.1 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.

11.2.1.2 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.

11.2.1.3 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.

11.2.1.4 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.

11.2.1.5 RECORDED EVENT

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

11.2.1.6 CURRENT SNAPSHOT

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

11.2.1.7 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.

11.2.1.8 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.

11.2.1.9 Exit

The **Exit** button only is available in the Event Detail dialog if the dialog is launched from the video player. In the Event Log, the Detail dialog cannot be closed.

11.2.2 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.

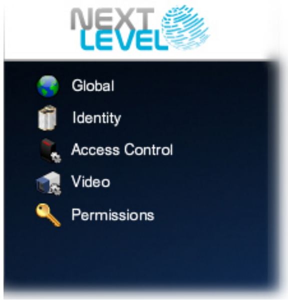
1. Click the **Events** button.
2. In the *Event Log*, click the **Emergency** tab.
3. Click the event item in the list with an *Open* status.

   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 13: Global Configurations**.
2. Configure identity related information, as described in **Chapter 14: Configure Identity and Credentials**.
3. Configure Access Control, as described in **Chapter 15: Configure Access Control**.
4. Configure video sources, as described in **Chapter 16: Configure Video, Storage, & Decoders**.

Permissions can be set at any time. Prior to configuring a new user, a role must be cloned that can be applied to new users. See **Chapter 17: Configuring PermissionsChapter 17: Configuring Permissions**

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

Chapter 12: 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.

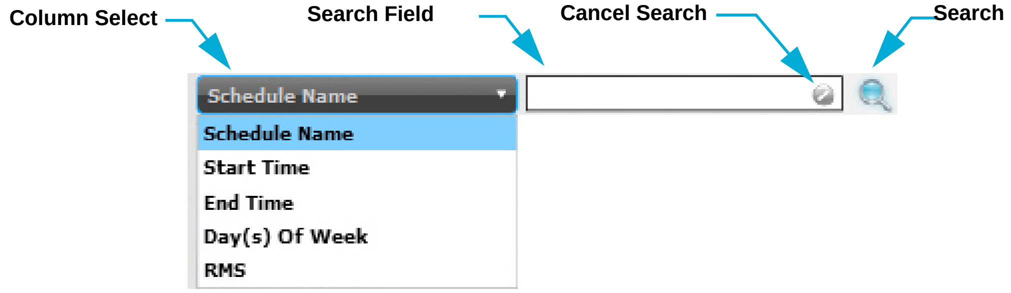
🔄 **Refresh**: click **Refresh** to update the list.

▲▼ **Sort**: click a column header to sort the results in ascending (up arrow) or descending (down arrow) order.

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

12.1 SEARCHING TABLES

The tables at the top of the Configuration panes can be filtered with the search function above the table. Only the items matching the search criteria are listed.



1. From the **Column Select** drop-down list, select the column on which you want to search.
2. Enter a value in the **Search** field.
   – If the column has a limited number of options, such as Connected or Not Connected, then a drop-down list is displayed with the options.
3. Click **Search** (magnifying glass) to run the search.

   A list of matching items is displayed.

   – If necessary, click a column header to sort the results in ascending (up arrow) or descending (down arrow) order.
4. Click **Cancel Search** or select another column to display the entire list again. The Cancel Search button is only displayed after a search is run.

12.2 ADDING, EDITING AND DELETING ITEMS

Many items under the **Configuration** menu options can be added, edited and deleted. The steps for each of these procedures are basically the same. If an Add, Edit, or Delete procedure contains additional steps, instructions are included in the applicable section.

12.2.1 Adding Items

An item can be added manually, if necessary.

1. Select **Configuration >** ***menu item*** **>** ***option*** from the Main Menu, where menu item is the area to be configured, such as Global, Identity, Access Control, Video, or Permissions. *Option* is the menu choice, such as Schedules, Access Levels, Controllers, Cameras, Roles, etc.

   The table for that option is displayed listing the current items. The list is empty if no items have been added.

2. Click **Add** 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. Some 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.

12.2.2 Edit Items

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

1. Select **Configuration >** ***menu item*** **>** ***option*** from the Main Menu.

2. Select an item from the table.

   The item’s *Details* are displayed in the bottom pane.

3. Select a tab, if applicable.

4. Edit the Details fields, as needed.

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

12.2.3 Delete Items

1. Select **Configuration >** ***menu item*** **>** ***option*** from the Main Menu.

2. Select an item from the table.

   The item’s *Details* are displayed in the bottom pane.

3. Click **Delete**.

   A confirmation dialog is displayed.

4. Click **Yes** to verify the deletion.
   - Click **Cancel** to close the dialog without deleting the item.

Chapter 13: Global Configurations

NLSS recommends doing global configurations in the following order:

1. **Configure RMS** (if applicable)

Note: *If no Gateway is registered with RMS*, *NLSS recommends configuring a Gateway locally before installing RMS across the system.* Settings can be tested on that Gateway, before applying those settings to multiple Gateways via 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 Actions**
10. **Configure Event Linkages**
11. **Configure Actions**

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.

Access to any Configuration category, in general, can be controlled by permissions. Permissions also can be set down to the view, add, edit and delete functions for an item. See **Chapter 17: Configuring Permissions** for more information.

13.1 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. A Partner is the organization that provides the NLSS service to customers. The token must be entered manually.

1. Access **Configurations > Global > RMS** from the Main Menu.
2. 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 after the token is saved.
3. Click **Save** to record the token.
   – Click **Cancel** to clear the token.

13.2 CONFIGURE CUSTOMER

Unless this gateway is a managed by RMS (Remote Managed Services), details about the Customer (site owner) are not critical for operation.

These settings cannot be modified at the local level when a Gateway is managed by RMS.

13.2.1 Customer Details

These parameters define the specific customer that is selected in the table in the top pane of the *Customer Details* screen.The fields are not editable if RMS is enabled.

- **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 sites are managed by RMS, the same customer data is entered for each site.

13.2.2 Customer Configuration

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.

13.3 CONFIGURE SITES

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

These settings cannot be modified at the local level when a Gateway is managed by RMS. The *Configuration* > *Global* > *Sites* screen accessed from the RMS level has additional tabs. See **Sites** in **Chapter 18: Remote Management Services** for more information.

13.3.1 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.

If the site is managed by RMS, these fields are edited at the RMS (top) level. See **Sites** in **Chapter 18: Remote Management Services** for RMS instructions.

- **Site Name**: the name of this particular site.
- **Site Address**: physical location of this site.

13.3.2 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.

13.4 CONFIGURE NLSS GATEWAYS

NLSS Gateways can be managed and configured via the NLSS Web Interface.

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

The *Gateways* screen is displayed with a list and a *Gateway Details* pane with four tabs:

- **General Tab**
- **Wired Network Tab**
- **Email Tab**
- **Time Tab**

13.4.1 General Tab

1. Select a Gateway from the list in the top pane of the *Gateways* screen.

   The *Gateway Details* pane is displayed.

2. Open the **General** tab.

13.4.1.1 General Tab Parameters

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

- **Device Name**: a unique name for this NLSS Gateway.
- **Device Type**: (read-only) the model of the selected NLSS Gateway.
- **Firmware Version**: (read-only) the firmware version running on the Gateway.
- **Available Firmware Version**: (read-only) indicates the latest version available, which can be updated via **Check Update** or **Firmware Update**. The value in field blinks if a newer version is available.
- **Hardware Version**: (read-only) the hardware version of the Gateway.
- **Serial Number**: (read-only) the Gateway’s serial number.
- **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 can 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 with the SSH password.

13.4.1.2 General Tab Buttons and Links

- Configuration Backup
- Configuration Restore
- Download System Logs
- Reboot
- Shut Down
- File System Check
- Check Update
- Factory Reset
- Firmware Update
- NLSS Gateway End User License Agreement

13.4.1.2.1 Configuration Backup

Running a *Configuration Backup* saves the Gateway's configuration settings to a backup file. This backup includes events, plus the configuration for related decoders, doors, access cards, and other hardware and software settings as set on the Gateway.

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. Click the **Configuration Backup** in the **General** tab.
2. Click **Yes** when prompted to create a copy of the current configuration settings.
3. Select **Save File** when prompted to open the *.nlss* file.

The backup file is saved to the *Downloads* directory for the browser. Each time a backup is run, a new file is created with the naming format of:
nlssdb2*-gateway model-MAC address-yyyy-mm-dd-time*.***nlss***

Important: 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 running Configuration Restore, the file must be in a *compressed* format. If the browser uncompressed the configuration file, then the file must be recompressed before being used to restore system configurations.

13.4.1.2.2 Configuration Restore

Selecting *Configuration Restore* returns the Gateway to the configuration settings that were last saved via a **Configuration Backup**.

Note: **Configuration Backup** must have created a backup file to run a restoration.

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.

1. Select **Configuration > Global > Gateways** from the Main Menu.
2. Select a Gateway from the list. The *Gateway Details* pane is displayed.
3. Click **Configuration Restore** in the **General** tab.
4. Follow the prompts to locate the backup file and restore the previous settings.

13.4.1.2.3 Download System Logs

When contacting NLSS or an authorized representative for support, a technician may request the Gateway’s system logs to help with troubleshooting.

1. Select **Configuration > Global > Gateways** from the Main Menu.
2. Select a Gateway from the list. The *Gateway Details* pane is displayed.
3. Click **Download System Logs** In the **General** tab.
4. Follow the prompts to save the log file locally.

A zipped *logs* folder is saved to the *Downloads* directory for the browser. The folder contains a series of text and log files. Each time a System Log is created, a new file is created with the naming format of:
logs*-gateway model-MAC address-yyyy-mm-dd-time*.***zip***

13.4.1.2.4 Reboot

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

1. Select **Configuration > Global > Gateways** from the Main Menu.
2. Select a Gateway from the list. The *Gateway Details* pane is displayed.
3. Click **Reboot** in the General tab.

   A confirmation dialog is displayed.
4. Click **Yes** to confirm the reboot.
   - Click **No** to abort the reboot.

13.4.1.2.5 Shut Down

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

1. Select **Configuration > Global > Gateways** from the Main Menu.
2. Select a Gateway from the list. The *Gateway Details* pane is displayed.
3. Click **Shut Down** in the **General** tab.

   A dialog box is displayed asking for confirmation.
4. Click **Yes** to confirm the process.
   - Click **No** to abort the shut down.

13.4.1.2.6 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 locates 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 the file system check is running. The length of time to run a File System Check depends the amount of data stored on the Gateway's internal hard drive.

1. Select **Configuration > Global > Gateways** from the Main Menu.
2. Select a Gateway from the list. The *Gateway Details* pane is displayed.
3. Click **File System Check** in the **General** tab.

   A dialog box is displayed asking for confirmation.
4. Click **Yes** to confirm the process.
   - Click **No** to abort the File System Check.

After the File System Check is complete, the NLSS Gateway is rebooted.

13.4.1.2.7 Check Update

The value in the Available Firmware Version field blinks if a newer version is available. Selecting Check Updates triggers the Gateway to check the NLSS web site for firmware updates.

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

1. Select **Configuration > Global > Gateways** from the Main Menu.
2. Select a Gateway from the list. The *Gateway Details* pane is displayed.
3. Click **Check Updates** in the **General** tab.
4. Follow the prompts to check for updated firmware. If a more recent version of the Gateway's firmware is found, the firmware is updated and the Gateway reboots automatically when done.

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

13.4.1.2.8 Firmware Update

If an Internet connection is not available for firmware updates via the Check Updates button, or if a manual update is preferred, a newer firmware version can be downloaded outside the Gateway and then installed.

1. Download the latest Gateway firmware file from the NLSS web site, or obtain it from an authorized NLSS representative.
2. Copy the firmware file to a drive of any computer on the same network as the Gateway.
3. Open the NLSS Web Interface in a browser.
4. Select **Configuration > Global > Gateways** from the Main Menu.
5. Select a Gateway from the list. The *Gateway Details* pane is displayed.
6. Click the **Firmware Update** in the **General** tab to open a file loader.
7. Click **Browse** to locate the new firmware file on the PC.
8. Click **Upload** to copy the file to the Gateway.
9. After the upload is complete, the Gateway automatically reboots.

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

Note: After updating the firmware for the NLSS Gateway, clear the browser's cache to see new features in the NLSS Web Interface for that Gateway.

13.4.1.2.9 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 network, as the IP address is reset to DHCP. See **Install NLSS Gateways**.

Important: Before restoring an NLSS Gateway to its factory state, **Configuration Backup** can be run to save the configuration settings.

Factory Reset deletes the system configurations and records saved by the Gateway.

1. Select **Configuration > Global > Gateways** from the Main Menu.
2. Select a Gateway from the list. The *Gateway Details* pane is displayed.
3. Click **Factory Reset** in the **General** tab.
4. Follow the prompts to restore the Gateway to its factory state.
5. If a previous configuration is desired, click **Configuration Restore** in the **General** tab. See **Configuration Restore** for more information.

Follow the prompts to restore the previous configuration settings.

Note: After resetting the NLSS Gateway, clear the browser's cache to fully restore the NLSS Web Interface for that Gateway.

13.4.1.2.10 NLSS Gateway End User License Agreement

Click **End User License Agreement** to open the agreement in a separate window or tab, depending on the browser's configuration.

The End User Agreement also is available at:
nextls.net/nlss/eula/EndUserLicenseAgreement.html

13.4.2 Wired Network Tab

The GW-3000 and GW-5000 Gateways have two Ethernet ports and two sets of network parameters. The GW-500 has only one Ethernet port with one set of parameters.

- **Enable DHCP**: DHCP automatically assigns an IP address to the NLSS Gateway.

  DHCP is enabled by default. If DHCP is disabled, manually define the network location of the NLSS Gateway with the following fields. These fields are editable only if DHCP is disabled.

Important: Verify the network settings with the network administrator.

If DHCP is enabled, some access control devices may lose connectivity with the Gateway if the Gateway's IP address is changed.

Note: The following fields are read-only if DHCP is enabled. Edit the fields if DHCP is disabled.

- **IP Address**: enter a static IP address for the Gateway.

- **Subnet Mask**: enter the subnet mask to identify the subnet on which the NLSS Gateway resides, such as 255.255.255.0

- **Default IP Gateway**: enter the IP address of the *network gateway* used by the NLSS Gateway to access the network.

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

- **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 unique identifier hard-coded into the NLSS Gateway's network interface.

- **Link Speed**: (read-only) the data transfer rate (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.

13.4.3 Email Tab

An email message can be sent by the Gateway to notify a user when a certain event occurs. 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 identifies the email server through which the Gateway can send a message when triggered by an event. The setting can be tested in this tab.

1. Select **Configuration > Global > Gateways** from the Main Menu.
2. Select the **Email** tab under *Gateway Details*.
3. Select a **Mail Server**: either **Sendmail** or **SMTP**.
   - If an SMPT server is installed, enter the **SMTP Server** name and **Password**, if required.
4. Enter an email address in **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.

13.4.4 Time Tab

The clock for the Gateway is set in the Time tab.

- **Time Zone**: the time zone in which this Gateway is located.
- **Current Gateway Time**: the current setting of Gateway’s internal clock.
- **Time Mode**: the method is used to set the Gateway’s clock: either **Manually** or via **NTP Time** (Network Time Protocol Time Server).
  - **NTP Server**: URL or IP address of the NTP server from which the Gateway gets its time setting. Check with the network administrator for this address.
  - **Manually Set on Gateway**: set the calendar date and the current time.

13.5 CONFIGURE HOLIDAYS

In the *Configuration* > *Global* > *Holidays* screen, the configured Holidays are listed. Initially, the screen is empty. Holidays an be added, edited, searched and deleted. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions.

Holidays are only used for scheduled auto unlock/lock. See **Configure Schedules** for more information.

These settings cannot be modified at the local level when a Gateway is managed by RMS.

13.5.1 Holidays Table

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

13.5.2 Holiday Details

- **Name**: enter the Holiday's name.
- **Start Date**: click the **Calendar** to select a start date for the Holiday. The time the Holiday begins is 12:01 a.m. on the Start Date.
- **End Date**: click the **Calendar** to select an end date of the Holiday. 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.

13.6 CONFIGURE SCHEDULES

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

These settings cannot be modified at the site level when a Gateway is managed by RMS.

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 a door 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.

1. Select **Configuration > Global > Schedules** from the Main Menu.

   The *Schedules* screen is displayed.

2. Select a schedule from the list.

   The *Schedule Details* pane is displayed.

Schedules can be added, edited, deleted and searched.

Note: **Always** and **Never** are default schedules that cannot be edited.

13.6.1 Schedule Details

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

- **Schedule Name**: a unique name to identify the schedule.
- **Start Time**: use the arrows to select 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**: use the arrows to select 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.

13.6.2 Create New Schedules

1. Select **Configuration > Global > Schedules** from the Main Menu.
2. Click **Add** in the top pane.
3. Enter the **Schedule Details**.
4. Optionally, to **Disable Schedules on Holidays** select the **Disable** flag.

   This option prevents an auto-unlock of doors on Holidays.
5. Click **Save** to keep the settings.
   - Click **Cancel** to return to the previous settings.

See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for edit, delete and search instructions.

13.7 CONFIGURE EVENT TYPES

The NLSS Unified Security Suite comes with pre-defined event types that are 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 added or deleted, but can be edited and searched. See **Chapter 12: General Configuration Functions** for instructions.

These settings cannot be modified at the site level when a Gateway is managed by RMS.

13.7.1 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 11: Monitoring and Handling Events** for more information.

13.7.2 Event Type Details

- **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.

13.8 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. An Event Severity cannot be created or deleted. Only the Description can be modified.

Event Severity can be searched. See **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions.

These settings cannot be modified at the local level when a Gateway is managed by RMS.

13.8.1 Event Severity Table

This table lists the default severity levels, and their descriptions. Click on an item to display the **Event Severity Details**.

13.8.2 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).

Note: Click **Save** after modifying the **Description**.

13.9 CONFIGURE ACTIONS

Configuration > *Global* > *Action* allows specific behaviors to be associated with a device or item. An **Action Type** can be associated with a device such as a door or a camera. The action is triggered when a linked event occurs.

Actions are listed in a table at the top of the page, with editable parameters available in the lower pane, under *Action Details*.

Actions can be added, edited, searched and deleted. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions.

13.9.1 Action Type

An Action is defined by an *Action Type*. Action Types are available for Access Control, Decoders, Email notices, PTZ Cameras, Streams, and Video Analytics.

For many Action Types, a device must be selected to be associated with the action.

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.
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.
VAStart	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 *active* for a camera.
VAStop	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.

13.9.2 Creating an Action

1. Select **Configuration > Global > Action** from the Main Menu.
2. Click **Add**.
3. Enter a descriptive **Action Name**.

   The name must be unique. If the same action applies to multiple devices, include an 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 door, camera or stream, or a decoder, a drop-down list shows the applicable devices.
   - **EmailSend** provides fields to enter a recipient, subject and body (message).
5. Select an item from the device list. Depending on the Action Type, a secondary drop-down menu is displayed with possible settings.
6. Select a setting from the drop-down list to apply the action.
7. Click **Save** to add the Action.
   - Click **Cancel** to clear the settings.

See **Adding, Editing and Deleting Items** in **Chapter 12: General Configuration Functions** for edit and deletion instructions.

13.10 CONFIGURE EVENT LINKAGES

Configuration > *Global* > *Event Linkages* is one of the most powerful features of the system. Event Linkages allow specific events to be linked with one or more specific *Actions*. Event Linkages allow the system to be customized for specific applications and installations.

When an Event Type occurs on a selected Source, selected Actions are triggered.

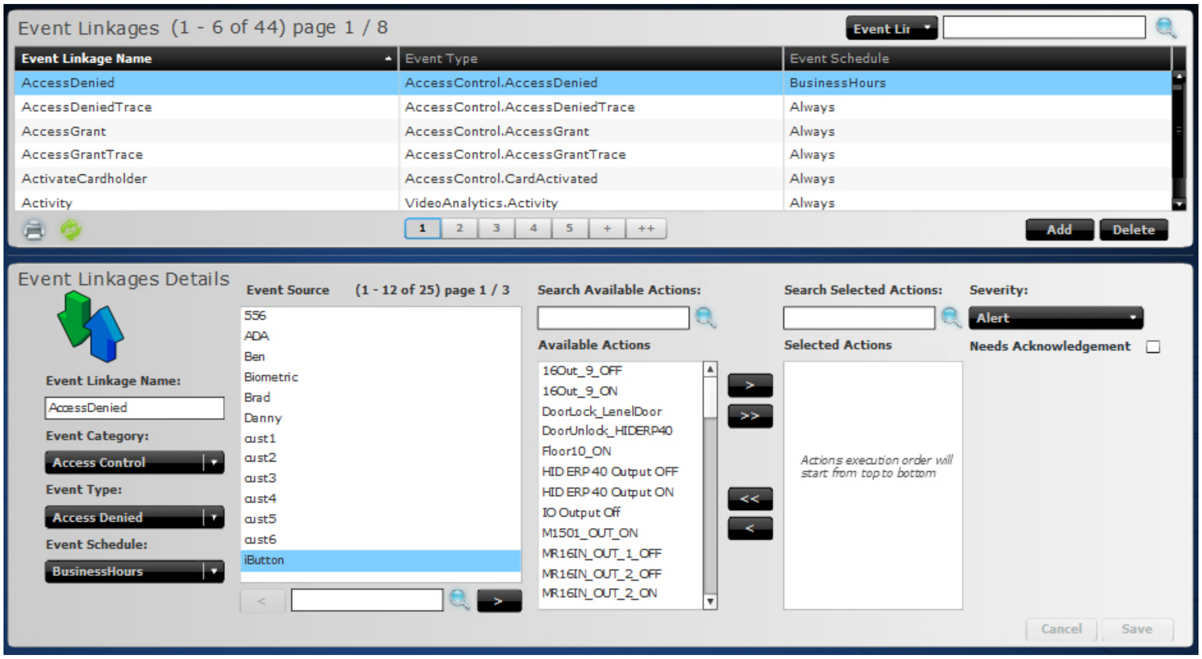
Event Linkages allow you to associate one more or actions with an event. An Event Type, Source, and Schedule, as well as Severity can be associated with a defined Action. See **Configure Actions**.

Note: Only one source can be selected for each Event Linkage.

Event Linkages can be added, edited, searched and deleted. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions

13.10.1 Event Linkage Details

When an Event Linkage is selected from the list or Add is clicked in the top pane, editable parameters are displayed in the *Event Linkage Details* pane.



Event Linkages (1 - 6 of 44) page 1 / 8

Event Linkage Name	Event Type	Event Schedule
AccessDenied	AccessControl.AccessDenied	BusinessHours
AccessDeniedTrace	AccessControl.AccessDeniedTrace	Always
AccessGrant	AccessControl.AccessGrant	Always
AccessGrantTrace	AccessControl.AccessGrantTrace	Always
ActivateCardholder	AccessControl.CardActivated	Always
Activity	VideoAnalytics.Activity	Always

Event Linkages Details

Event Linkage Name: AccessDenied

Event Category: Access Control

Event Type: Access Denied

Event Schedule: BusinessHours

Event Source (1 - 12 of 25) page 1 / 3

556
ADA
Ben
Biometric
Brad
Danny
cust1
cust2
cust3
cust4
cust5
cust6
iButton

Search Available Actions:

Available Actions

16Out_9_OFF
16Out_9_ON
DoorLock_LenelDoor
DoorUnlock_HIDERP40
Floor10_ON
HID ERP 40 Output OFF
HID ERP 40 Output ON
IO Output Off
M1501_OUT_ON
MR16IN_OUT_1_OFF
MR16IN_OUT_2_OFF
MR16IN_OUT_2_ON

Search Selected Actions:

Selected Actions

Actions execution order will start from top to bottom

Severity: Alert

Needs Acknowledgement ☐

- **Event Linkage Name**: a unique identifier for the linkage.
- **Event Category**: a drop-down menu that determines the area under which the linkage is applied: **Access Control**, **Camera, Decoder**, **System**, **User**, **Video Analytics**.
- **Event Type**: a drop-down menu that selects the Event Type applied to the linkage. See the table below and Configure Event Types for more information. The Event Type is determined by the Event Category selected.

Event Category	Event Types
Access Control	Access Denied, Access Denied Trace, Access Grant, Access Grant Trace, Card Activated, Card Deactivated, Controller Offline, Controller Online, Door Auto Relock, Door Auto Unlock, Door Battery Low, Door Forced Open, Door Held Open, Door Not Unlocked, Door Secured, Door Unlocked, Input Active, Input Inactive, Reader Comm Loss, Reader Comm Restored
Camera	Channel Loss, Clip Exported, Discovered, Export Failed, IO Event, Motion Event, Offline, Online, Snapshot Exported, Video Bookmark, Video Loss, Video Resume
Decoder	Decoder Offline, Decoder Online
System	Ext Storage Offline, Ext Storage Online, Recording Failover, Recording Failure
User	Card Activated, Card Deactivated, Door Opened, Login, Logoff
Video Analytics	Activity, Direction, Dwell, Face Capture, Line Crossing, Object Taken, Object Moved, People Count, Perimeter

- **Event Schedule**: a drop-down menu that selects the Schedule applied to the linkage. See **Configure Schedules** for more information.
- **Event Source**: select an to apply the Event Linkage. The list is determined by the Event Type that is selected.
- **Available Actions**: a list of Actions, dependent on the selected Event Type. Use the arrow keys to move selections to the **Selected Actions**. See **Configure Actions**.
- **Selected Actions**: the Action or Actions executed when the event occurs.
- **Severity**: a drop-down menu that selects the Event Severity for the Event Linkage. This setting overrides the Severity setting in Configuration > Event Types. See **Configure Event Types**.
- **Needs Acknowledgement**: when the linked event occurs, an acknowledgement is required from a user in the Events Log. This setting overrides the Needs Acknowledgement setting in Configuration > Event Types. See **Event Log** in **Monitoring and Handling Events**.

13.10.2 Creating an Event Linkage

1. Select **Configuration > Global > Event Linkages** from the Main Menu.
2. Click **Add**.
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. Click an **Event Source** to use with the linkage. The selection is indicated by the blue highlight.
7. Select the actions to include with the Event Linkage.
   a. Click on an Action 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 keep the Event Linkages.
    – Click **Cancel** to clear the settings.

See **Adding, Editing and Deleting Items** in **Chapter 12: General Configuration Functions** for edit and deletion instructions.

13.11 CONFIGURE GROOMER SETTINGS

Saving video clips can use a lot of disc space. *Groomer Settings* allow the system to automatically delete older audio-video clips to preserve space. If the Gateway's storage hits 90% of capacity, the groomer deletes older clips first to make room for new clips.

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.

Chapter 14: Configure Identity and Credentials

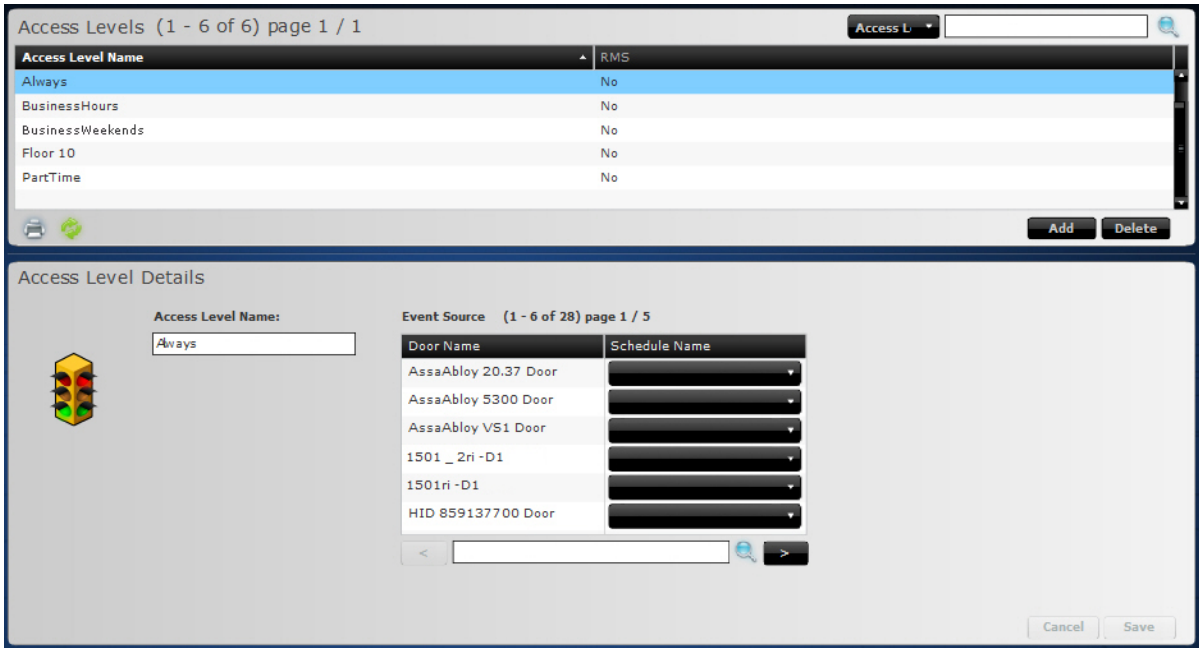
Superuser permissions are required to configure identity and credentials for new Cardholders.

NLSS recommends Identity 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 Fields** for Cardholders. This step is optional.
6. **Users** of the NLSS Unified Security Suite software.

14.1 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.



Access Levels (1 - 6 of 6) page 1 / 1

Access Level Name	RMS
Always	No
BusinessHours	No
BusinessWeekends	No
Floor 10	No
PartTime	No

Access Level Details

Access Level Name: Always

Event Source (1 - 6 of 28) page 1 / 5

Door Name	Schedule Name
AssaAbloy 20.37 Door	
AssaAbloy 5300 Door	
AssaAbloy VS1 Door	
1501 _ 2ri -D1	
1501ri -D1	
HID 859137700 Door	

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

- Schedules and Doors must be configured before Access Levels can be applied to them. See **Configure Schedules** and **Configure Doors** in **Chapter 13: Global Configurations**.
- Access Levels are assigned to Cardholders in two areas to grant access.
  - The Global Badge Profile for Default Access Level.
  - In the Configuration > Identity > Cardholder > Access Level tab, Access Levels can be added to supplement the Default Access Level. See **Access Levels Tab**.
- Up to 32 Access Levels are allowed per Cardholder, depending on the access control manufacturer. For example: Assa Abloy allows 1 level, HID Edge allows up to 8 levels, and Mercury allows up to 32 levels.

1. Select **Configuration > Identity > Access Levels** from the Main Menu.

   The *Access Levels* table is displayed.

2. Select an Access Level.

   The Access Level Details are displayed.

Access Levels can be added, configured, and deleted, as described below. Access Levels also can be.searched. See **Searching Tables** for search instructions. If the site is managed by RMS, the Access Levels are pushed from the RMS level, and only can be viewed and searched at the site level.

14.1.1 Access Level Details

After an Access Level from the list, the *Access Level Details* pane is displayed.

- **Access Level Name**: a unique name identifying the access level.
- **Door Name**: all the doors in the system are listed. Use the arrow buttons to page through the list, or locate a door with the search field.
- **Schedule Name**: select a schedule from the drop-down list to associate it with the door to the left. See **Configure Schedules** in **Chapter 13: Global Configurations** for more information.

  No schedules are assigned to doors by default.

14.1.2 Create a New Access Level

1. Select **Configuration > Identity > Access Levels** from the Main Menu.
2. Click **Add**.
3. Select **Schedule Names** from the drop-down lists for each door to which a schedule is to be added.
   - Multiple doors can use the same access level.
   - Multiple Access Levels can be assigned to a door, using the same or different schedules.
4. Click **Save** to keep the settings.
   - Click **Cancel** to clear the values.

See **Adding, Editing and Deleting Items** in **Chapter 12: General Configuration Functions** for edit and deletion instructions.

14.2 CONFIGURE CARD PROFILES

Cardholders 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 used in the system. These technical aspects of the card are *Type*, *Bit Format* and *Facility Code*.

Important: Card Profiles must be configured before Badge Profiles, as Card Profiles are used to **Configure Badge Profiles**. Card and Badge Profiles must be configured before access cards can be assigned to Cardholders.

Card Profiles can be added, configured, searched and deleted. See **Adding, Editing and Deleting Items** in **Chapter 12: General Configuration Functions** instructions.

14.2.1 Card Profiles Table

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

See **Searching Tables** for search instructions.

14.2.2 Card Profile Details

- **Card Profile Name**: a unique, editable field assigning a label to the profile.
- **Facility Code**: a unique number assigned to a group of cards by the 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**: use the drop-down list to select a data structure for this card profile.
  - **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.
    - Reserved for customers with a requirement for a large number of cards.

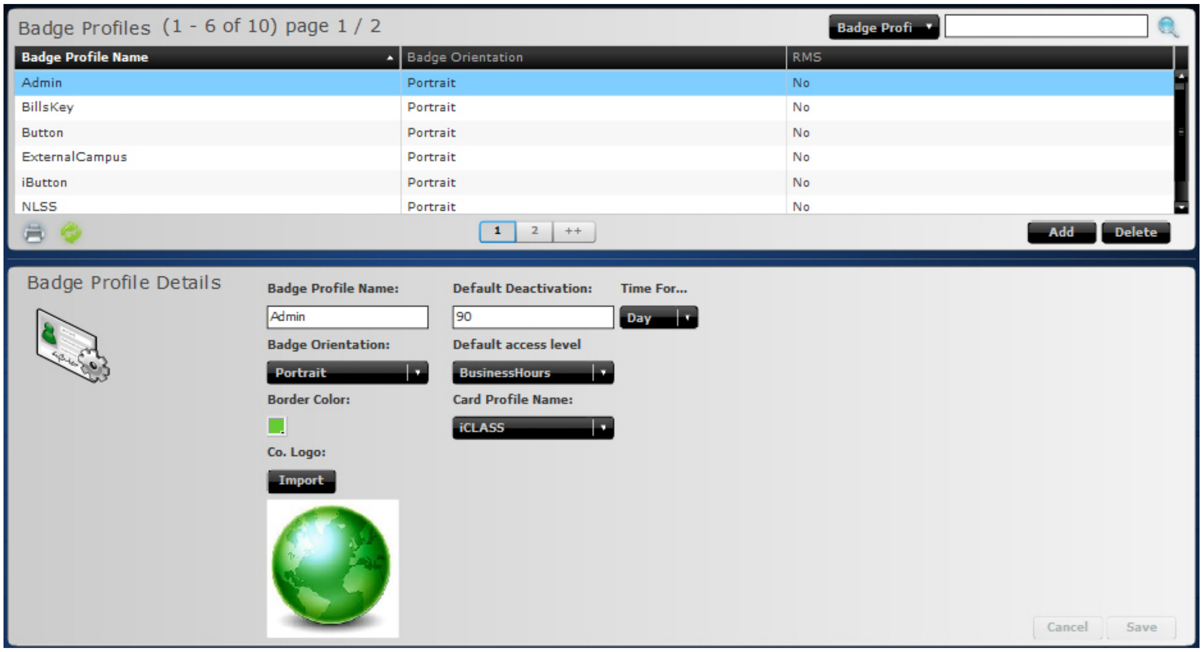
  See **http://www.hidglobal.com/page.php?page_id=10** for more information.

  - **Generic Format**
    - Proprietary, variable length format.
    - Check with the card manufacturer for card format information.

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

14.3 CONFIGURE BADGE PROFILES

Configuration > *Identity* > *Badge Profile* completes the generic information required for Cardholder badges. Any additional information required to produce badges is unique to the each Cardholder, and is entered in the Cardholder configuration screens.



Badge Profiles (1 - 6 of 10) page 1 / 2

Badge Profile Name	Badge Orientation	RMS
Admin	Portrait	No
BillsKey	Portrait	No
Button	Portrait	No
ExternalCampus	Portrait	No
iButton	Portrait	No
NLSS	Portrait	No

Badge Profile Details

Badge Profile Name: Admin

Default Deactivation: 90

Time For...: Day

Badge Orientation: Portrait

Default access level: BusinessHours

Border Color: 🟩

Card Profile Name: iCLASS

Co. Logo:

Important: Before configuring a Badge Profile, at least one Card Profile must be configured, as described in **Configure Card Profiles**.

Badge Profiles can be added, configured, searched and deleted. See **Adding, Editing and Deleting Items** in **Chapter 12: General Configuration Functions** instructions.

14.3.1 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.

See **Searching Tables** for search instructions.

14.3.2 Badge Profiles Details

- **Badge Profile Name**: an editable field with a unique identifier for the profile.
  - NLSS recommends creating a unique badge profile for each category or personnel-type at a company.

    For example: Employee, Contractor, Temporary, Vendor, Maintenance, Manager, Security, etc. The model provides templates from which to add new employees quickly and easily.

- **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 upload 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 with this Badge Profile automatically deactivate.
  - **Time Format**: a drop-down list to select either **Day**, **Month** or **Year** to set the units for the Default Deactivation.
- **Default Access Level**: a drop-down list to select a system-provided Access Level when a this Badge Profile is applied to a Cardholder. Other Access Levels can be applied when configuring a Cardholder. See **Configure Access Levels** and **Configure Cardholders** for more information.
- **Card Profile Name**: a drop-down list to select the Card Profile to apply to this Badge Profile.

14.4 CONFIGURE CARDHOLDER-USER DEFINED FIELDS

In the *Configuration > Identity > Cardholder–User Defined* screen, custom fields can be edited to appear in the User Defined tab of the Cardholders screen. See **User Defined Tab**.

- **Text**: allows a combination of text and numbers. Examples: emergency contact person
- **Number**: for numbers only. Examples: Social Security Number; Driver’s License
- **Date**: for dates only. Example: birth date
- **Boolean**: for true/false values. Example: Telecommuter: Yes/No

The User Defined screen defines these fields by assigning labels.

The User Defined screen has a limit of five of each field type.

14.4.1 Editing a User Defined Field for Cardholders

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.

14.5 CONFIGURE CARDHOLDERS

Configuration > *Identity* > *Cardholders* provides the fields needed to set up access and details for individuals with access badges.

In an NLSS Security System, *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.

Configure each Cardholder in the following order, using the *Configuration* > *Identity* > *Cardholder* screen.

1. Create a new Cardholder. Then configure the following parameters of the new Cardholder.
2. **General Tab**
3. **Credentials Tab**
4. **Access Levels Tab**
5. **Contacts Tab**
6. **Organizational Tab**
7. **User Defined Tab**
8. **Options Tab**

Cardholders can be added, configured, searched and deleted. See **Adding, Editing and Deleting Items** in **Chapter 12: General Configuration Functions** instructions.

14.5.1 Cardholders Table

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

See **Searching Tables** for search instructions.

14.5.2 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.

14.5.2.1 GENERAL TAB

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

- **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**: a drop-down list to select the current status of this Cardholder. Only **Active** enables a Cardholder's access. All other selections disable access.

Note: The **Inactive** status is useful for preparing cards prior to activation. Cardholder Status can be changed to **Active** when it comes time to print the card and provide it to a new Cardholder.

- **HR Cardholder Type**: a drop-down list to select a Human Resources category for this person: **Employee**, **Contractor**, **Intern**, **Temporary**, and **Student**.
- **Cardholder Vehicle**: optional fields that include the **Type** (make and model), **Color**, and **License Plate** number of the Cardholder's vehicle.

14.5.2.2 Credentials Tab

The Credentials tab has the security credentials and other details required for printing badges assigned to this Cardholder.

- **PIN**: a number (1 to 5 digits long) entered in keypads to open doors that are controlled by readers with keypads. PIN capabilities are enabled under *Reader Type* and *Reader Mode* and in the *Configuration > Access Control > Readers > General* tab. See **Reader Details** in **Chapter 15: Configure Access Control** for more information.

  Reader/keypad combinations are currently supported in Sargent and Mercury configurations.

  The PIN is optional, and does not require a value if no keypads are installed in the system.
- **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**: a list of one or multiple cards configured for a Cardholder.
  - Click an existing card in the list to update credentials for that card.
  - Click **Add Card** (**+**) below the list to add a new card to the selected Cardholder.
  - Click **Delete Card** (**-**) below the list to remove a card for the selected Cardholder.

Important: Only one card can be active at a time for a user.

- **Card Details**: aspects of the card used to define the card.
  - **Badge Profile Name**: a drop-down menu to select a Badge Profile for this card. At least one Badge Profile must created before cards can be created. See **Configure Badge Profiles** for more information.
  - **Card Number**: a unique identifier for the card. The number can be added to the field by either typing the number or by swiping the card through an OmniKey reader. See **Automatic Input with OmniKey Readers** for more information.
  - **Embossed Number**: an optional field to define a number printed on the outside of the card. This number does not have to match the Card Number.

- **Card Status**: the status of the selected card, not the Cardholder: **Active**, **Inactive**, **Returned**, **Lost**, and **Damaged**.

  When set to **Active**, the card can be used to open doors according to the access level assigned to it in the **Access Levels Tab**. All other designations disable the card.

Important: A cardholder can be active in the system and have deactivated cards. Only one card can be active at a time.

Card Status applies to a selected card, whereas Cardholder Status applies to the Cardholder’s access. If Cardholder Status is not set to Active, a card cannot provide access, even if the Card Status is set to Active. See **General Tab** for more information.

- **Activation Date**: sets the date on which this card become active. This date is set automatically when the Badge Profile Name is selected, but can be manually changed using the Calendar tool next to the field.
- **Deactivation Date**: the Badge Profile sets the default deactivation date when this card automatically becomes inactive. This date is set automatically when the Badge Profile Name is selected, but can be manually changed using the Calendar tool next to the field.

Automatic Input with OmniKey Readers

Since card numbers are not always printed on physical access control cards, an Omnikey reader can be used to enter the Card Number in the **Credentials Tab**.

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**.
3. Select a Cardholder.
4. In the **Credentials Tab**, click the plus (**+**) under the Cards list. Blank **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 **Credentials Tab**.
8. Click **Save** to keep the changes.
   - Click **Cancel** to restore the previous settings.

14.5.2.3 Access Levels Tab

Access Levels are assigned to Cardholders in the Access Levels tab. This setting informs the system as to the schedule that a selected Cardholder can open doors. See **Configure Access Levels** for more information.

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

- The left list contains the Access Levels available for the Cardholder.
- The right list contains the Access Levels assigned to the selected Cardholder.

Note: If a Cardholder has multiple cards, the Access Levels are assigned to the active card.

A Cardholder inherits a default Access Level from the Badge Profile assigned in the **Credentials Tab**. The default assignments can be overridden.

1. Select **Configuration > Identify > Cardholders** from the Main Menu.
2. Select a Cardholder.
3. Open the **Access Levels** tab.
4. Select an Access Level in the left column.
5. Click the right arrow button (**>**) to move the access level to the assigned (right) column.
   - Remove access levels from the assigned list by selecting them and clicking the left arrow button (**<**).
   - The double arrows (**<<** and **>>**) move all items between lists.
6. Click **Save** to keep the changes.
   - Click **Cancel** to restore the previous settings.

14.5.2.4 Contacts Tab

The optional Contacts tab stores communication information for a Cardholder.

- **Email Address**: enter one or more email addresses can be added for the Cardholder, tagged as either Work or Home.
- **Phone Numbers**: enter one or more Home, Work, or Mobile telephone numbers for this Cardholder.
- **SMS**: enter one or more numbers to send text messages to this Cardholder.

14.5.2.4.1 Add an Entry

1. Click **Add** (**+**) to the right of the column.
2. Select a **Type** from the drop-down list.
   - **Email Address**: select either **Work** or **Home**.
   - **Phone Numbers**: select either **Home**, **Work**, or **Mobile**

   No Type is needed for **SMS**.
3. Enter the **Address** or **Number** in the text box in the column.

4. Click **Save** to keep the changes.
   – Click **Cancel** to restore the previous settings.

14.5.2.4.2 Edit an Entry

1. Select an item in the **Email Address**, **Phone Number** or **SMS** lists.
2. Click **Edit** below the column.
3. Select a new **Type** or change the entry.
4. Click **Save** to keep the changes.
   – Click **Cancel** to restore the previous settings.

14.5.2.5 Organizational Tab

The optional Organizational tab contains company or organization information for this Cardholder.

- **Location**: the address of the site where the Cardholder is based.
- **Cardholder Department**: the department to which the Cardholder belongs.
- **Cardholder Supervisor**: the name of the Cardholder’s superior.
- **Cardholder Title**: the Cardholder’s job title.

14.5.2.6 User Defined Tab

Custom fields created in the *Configuration > Identity > Cardholder-UserDefined* screen to help further define a Cardholder. Data for these optional fields is entered in the User Defined tab. See **Configure Cardholder-User Defined Fields**.

1. Select **Configuration > Identify > Cardholders** from the Main Menu.
2. Select a Cardholder.
3. Open the **User Defined** tab.
4. Enter values in the fields.
5. Click **Save** to keep the changes.
   – Click **Cancel** to restore the previous settings.

14.5.2.7 Options Tab

The Options tab contains three miscellaneous options.

- **ADA**: the ADA flag is used to allow extra time for the 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 **General Tab** under **Controller Details** in **Chapter 15: Configure Access Control**.

  – In the Controller Details screen, the **DHO Time** is the time (in seconds) that a normally closed door can be held open before activating an alarm.

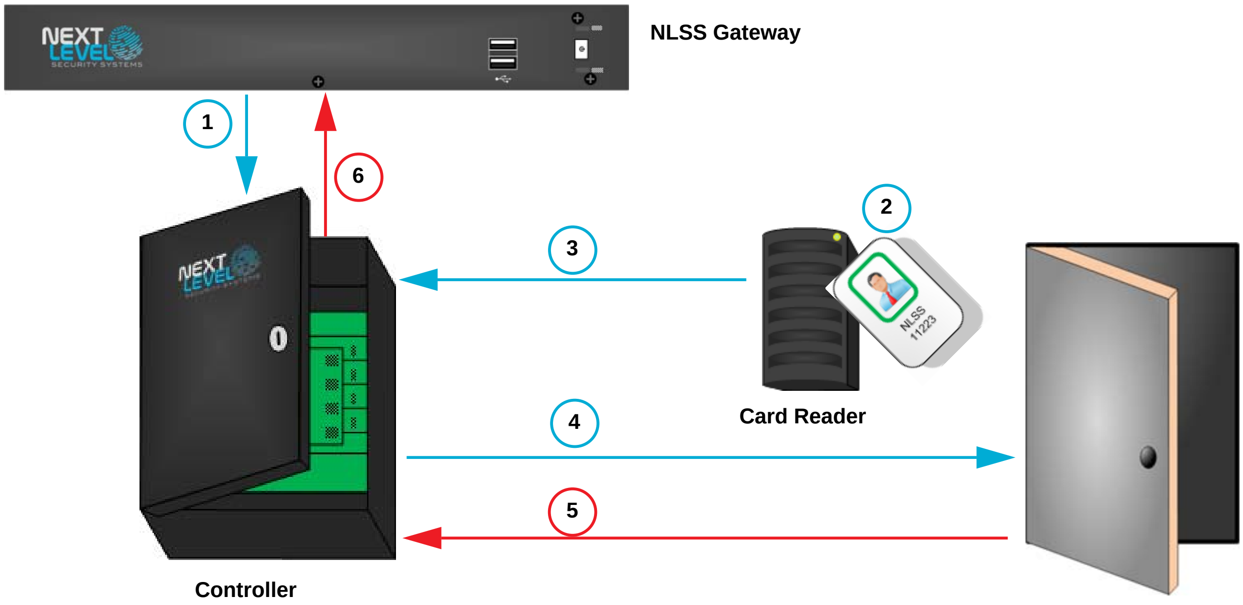
  - **Strike Time** is the time (in seconds) that a normally locked door stays unlocked after receiving an unlock signal.

- **Enable Trace**: if selected, all access attempts of this Cardholder (successful or not) are to be tagged as *trace* events, even if the Event Filter is masked.

- **Notes:** Optional comments.

Chapter 15: Configure Access Control

When an access card is tapped on a card reader, the NLSS Unified Security Platform records the action and determines if the accompanying door can be opened. Behind the scenes, a more complex interaction takes place.



1. Controller downloads access card information from the NLSS Gateway. The access card credential is loaded on the controller when the controller is configured or when controller comes on line.
2. Cardholder taps an access card on a card reader for a door.
3. The request is sent to the controller.
4. Controller decides whether to unlock the door, based on the Cardholder’s configuration. See **Configure Cardholders** in **Chapter 14: Configure Identity and Credentials**.
5. If the door is forced open, the controller is notified.
6. The incident is sent to the NLSS Gateway, which generates an event. See **Chapter 11: Monitoring and Handling Events**

Note: The Gateway pushes access changes to the controller. Controllers are only notified of applicable changes. These changes include Badge Profiles, Card Profiles, and Cardholder information and credentials.

Access control devices must be configured in the following order.

1. **Configure Controllers**

2. **Configure Reader Interfaces**
3. **Configure Readers**
4. **Configure Doors**
5. **Configure I/O Interfaces**
6. **Configure I/O Linkages**

Important: To remove a device from service without removing its record:

1. Select **Out of Service** under Administrative state in the **General** tab.
2. **Save** the change.

15.1 CONFIGURE CONTROLLERS

Each controller needs to be associated with an NLSS Gateway. 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. Configure these controllers from their user interfaces, following the manufacturer's instructions. Fields are included for 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.

Once a controller is online, reader interfaces and readers and doors are added automatically to the Gateway. The controller, reader interfaces, reader, and door have all names automatically assigned to them when they are discovered by the Gateway.

Other differences between Mercury, HID, and Assa Abloy controllers:

- Different Mercury controllers vary in the number of reader interfaces and other I/O devices that a controller supports. Most Mercury controllers support at least one external reader
- Assa Abloy controllers typically embed reader interfaces and readers in the controller.
- HID either embeds a reader interface and reader in a controller; or only embeds a reader interface in the controller.

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 a controller to see its details.

Controllers can be added, edited, searched and deleted. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions.

15.1.1 Controller Details

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

15.1.1.1 General Tab

When an NLSS Gateway discovers an access controller, the Gateway automatically populates most of the fields in this tab. Some 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 unique, user-friendly name for this controller.
- **Gateway Name**: the NLSS Gateway to which this controller is associated.
- **Access Controller Type**: Read-only after the controller has been added.

  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.

  – 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.

  – HID Edge/ EDGE EVO is for any HID product.

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:

1. Program the Controller.
2. Program the Reader Interface.
3. Program the Reader.

- **Description**: enter an optional 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.

  – **Out of Service** removes the controller from the NLSS system, but does not delete its records from the system. The

  – **Pre-provisioned** is the default setting when the controller has been discovered by the Gateway, but has not been placed in service.

- **IP Address**: shows the numeric IP address of this controller. Do *not* change this value in this screen.
- **MAC Address**: (read-only) the hard-coded 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 for a Gateway to connect to an HID or Assa Abloy controller.

- **Password**: the password required for a Gateway to connect to an HID or Assa Abloy controller.

- **DHO Time Default**: enter the default time—in seconds—that a door can be held open until an alarm activates. This default can be overridden for individual doors. See **Door Details** for more information.

- **Extended DHO Timeout**: for Cardholders with ADA enabled access. Enter the default time—in seconds—that a door can be held open until an alarm activates
  - *ADA* stands for *American Disabilities Association*. Enabling ADA is done typically for Cardholders with disabilities.
  - ADA is enabled in the Cardholders' **Options Tab**.
  - Extended DHO Timeout also can be applied to Cardholders who need to hold doors open for a longer time, such as loading dock or a mail room employees.

- **Strike Time Default**: the default time—in seconds—that a locked door stays unlocked after receiving an unlock signal. This default can be overridden for individual doors. See **Door Details** for more information.

- **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. See the **Extended DHO Timeout** parameter for ADA details.

- **System Contact**: optionally enter the name of the system manager or administrator.

- **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. This setting is not displayed for wired controllers.

- **Baud Rate**: from the drop-down 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**. This setting is not displayed for wireless controllers.

- **Installer**: the name of the person or company that installed the controller.

- **Install Date**: the date the controller was installed (for warranty purposes).

15.1.1.2 Controller Details: Diagnostics Tab

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

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

15.1.2 Associating a Mercury Controller with an NLSS Gateway

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

   After the NLSS Gateway discovers this Mercury controller, the Controller table lists the controller with a default **Administrative State** of **Preprovisioned**.

   Preprovisioned indicates that the system discovered the controller, but no attempts have been made from the NLSS Web Interface to connect to it.
3. Select the controller from the list.
4. Enter a unique name in the **Access Controller Name** field.
5. If multiple Gateways are installed, 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.

15.2 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 the reader interface configurations of the HID or Assa Abloy. The HIS and Assa Abloy 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 *Reader Interfaces* screen is displayed with a list of Reader Interfaces in the system.

2. Select a Reader Interface

3. The *Details* pane is displayed with three tabs: General, Aux Input, and Aux Output.

Reader Interfaces can be added, edited, searched and deleted. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions.

15.2.1 Reader Interface Details

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.

15.2.1.1 GENERAL TAB

These parameters are applicable to Mercury reader interfaces only. Not all of these 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**: select a type from the drop-down list of pre-configured values:
  - **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 controllers available for this reader interface.

- **Description**: enter an optional description.

- **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) Enter the IP address of this reader interface. Contact the network administrator for a static IP address.
- **MAC Address**: (for MR51e only) Enter the MAC address of this reader interface. This address is found on the board.
- **Installer**: the name of the person or system integrator who installed this reader interface.
- **Install Date**: the date this reader interface was installed.

Notes:

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.

  (REX means Request to Exit, which can take many forms such as a passive infrared or sensor on the exit hardware)
- 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.

15.2.1.2 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.

- **Aux Inputs Available**: a list inputs on the reader interface. Connect an input device to a port on the interface.
- **Input Port**: select an **Aux Input** and enter the port to which the input 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** from the drop-down list. Supervised reader interfaces can detect a change in resistance in the line.
- **Enabled**: select **Enabled** or **Disabled** from the drop-down list to activate or deactivate the input. Select Enabled to process signals from the attached device.
- **Normal State**: select the default state of the input. Select **Open** or **Closed** from the drop-down list to indicate whether the input's relay is normally off (open) or on (closed).

15.2.1.2.1 Reader Interface 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, 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.

15.2.1.3 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.

- **Aux Output Available**: a list of outputs on the reader interface.
- **Output Port**: select an **Aux Output** and enter 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**: select the default state of the output device that is being handled by this reader interface. Select **Normally Active** or **Normally Inactive**.

15.2.1.3.1 Reader Interface 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.

15.2.2 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 often used to expand EP1501 systems.

15.2.2.1 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 the **General Tab**.
3. If you are connecting input/output devices (other than door readers) to this reader interface, then enter values for **Aux Input Tab**, and then **Aux Output Tab**.
4. Click **Save** to keep the settings.
   - Click **Cancel** to restore the previous settings.

15.2.2.2 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 database 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.

15.3 CONFIGURE READERS

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

When a Controller/Reader Interface is added to a system, the Readers table is automatically populated in the *Configuration > Access Control > Readers* screen.

1. Select **Configuration > Access Control > Readers** from the Main Menu.

   The *Readers* screen is displayed listing the readers in the system.
2. Select a Reader.
3. The *Readers Details* pane is displayed.

Readers can be added, edited, searched and deleted. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions.

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

15.3.1 Reader Details

The Reader Details pane contains two tabs, General and Aux Output. The fields differ slightly between different reader types. The Aux Output tab is only available for HID readers.

- **Reader Name**: enter a unique name to identify this reader.
- **Reader Interface Name**: select an interface from the drop-down list of discovered and configured reader interfaces, if available for the selected reader.
- **Access Controller Name**: select a controller from the drop-down list to associate with the reader.
- **Description**: optional description of this reader.

15.3.1.1 GENERAL TAB

- **Reader Style:** select a style or kind of reader from the drop-down list:
  – **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**: Wiegand is the only supported format for now.
- **Reader Mode**: from the drop-down list, select an input type accepted by this reader. The 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 **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**: select a port number from the drop-down list 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**: optional text field. Enter the name of person or system integrator who installed the reader.
- **Install Date**: optional field. Enter the date this reader was installed. Click on the **Calendar** button to select a date.

15.3.1.2 Aux Outputs Tab

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.

Set the parameters to enable the outputs.

- **Output Devices Available**: a list of outputs on the reader.
- **Output Port**: select an **Output Device** and enter the port to which the connection was made.
- **Output Name:** give this output device a unique name.

- **Output Duration**: enter a length of the output signal, in seconds.
- **Enabled**: select **Enabled** to activate the output.
- **Normal State**: select the default state of the output. From the drop-down list, select either: **Normally Active** or **Normally Inactive**.

15.4 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 listing the Doors in the system.

2. Select a Door from the list.

   The *Door Details* are displayed

Doors can be added, edited, searched and deleted. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions.

Notes:

- Configure schedules *before* associating schedules with doors or other items in the system that uses schedules. See **Configure Schedules** in **Chapter 13: Global Configurations** for instructions.
- Holidays can override schedules associated with doors. See **Configure Holidays** in **Chapter 13: Global Configurations** for more information.
- If a door is physically removed from the system, then it must be deleted from the database 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.

15.4.1 Door Details

The *Door Details* contains two tabs: **General** and **Strike**.

15.4.1.1 GENERAL TAB

- **Door Name**: enter a unique name to identify the door.
- **Door Type**: an optional drop-down list of available types of doors, including **glass**, **solid wood**, **hollow metal**, **store front** and **fire door**.
- **Reader Name**: from the drop-down list of readers available in the system, 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** in **Chapter 13: Global Configurations** for more information.

- **Door Contact Mode**: from the drop-down list, select whether the door is **Normally Open** or **Normally Closed**.
- **REX 1 Type**: from the drop-down list, select devices to send 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 1 Mode**: the normal (default) state of a Request to Exit device on this door, either is **Normally Open** or **Normally Closed**.
- **Unlock on REX 1**: check this box to unlock the door when the action occurs that is selected in REX 1 Type.
- **DHO Time Override (Sec)**: select a *door held open* value only to override the default DHO value set in the **Configure Controllers** screen.
- **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**: optional text field to enter the person who installed the door lock.
- **Install Date**: optional field to enter the date this door lock was installed. Click on the **Calendar** button to select a date.

15.4.1.2 STRIKE TAB

Strike parameters pertain to the locking mechanism of the door:

- **Lock Type**: from the drop-down list, select the type of lock used on this door, such as **Mag Lock**, **Electric Lockset**, etc.
- **Lock Voltage**: from the drop-down list, select the voltage used on the lock, either **12v DC** or **24v DC**.
- **Strike Time Override**: optionally provide an 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.

15.5 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 and outputs for general purpose use. Configuration of these I/O interfaces varies, based on the capabilities of the parent controller and the specific I/O device. This section includes general instructions for most configurations.

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. Select an I/O Interface from the list.

   The *I/O Interface Details* are displayed in the bottom pane.

I/O Interface can be added, edited, searched and deleted. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions.

15.5.1 I/O Interface Details

The *I/O Interface Details* pane contains general parameters plus two tabs: **Aux Input** and **Aux Output**.

15.5.1.1 I/O Interfaces: General Parameters

- **IO Interface Name**: enter a unique name to identify this I/O board.
- **IO Interface Type**: from the drop-down list, select the type of I/O board. For example, the Mercury 1502 controller supports the Mercury MR16IN and MR16OUT boards.
- **Access Controller Name**: from the drop-down list, select the controller to which the I/O board is attached. The list contains all of the 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.

15.5.1.2 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, configure the remaining fields 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 provide a descriptive name for the selected input port. The name can indicate the type of device to which the port 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 two options: **Supervised** or **Unsupervised**. Supervised I/O boards detect a change in resistance in the line that affects the device.

- **Enabled**: a drop-down list to activate or deactivate the port. Two options are available: **Enabled** or **Disabled**.
  - The system ignores inputs to disabled ports. **Disabled** also 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.

15.5.1.3 I/O Interface Details: Aux Output Tab

The Auxiliary Output tab lists the available output ports. 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 I/O device. After a port is selected, configure the remaining fields 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 to activate or deactivate the port. Two options are available: **Enabled** or **Disabled**.
  - The system ignores disabled ports. **Disabled** 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.

15.6 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.

Note: 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 table at the to of the screen is empty until an I/O Linkage is created.

   After I/O Linkages are created, the table lists the I/O Linkages found in the system.

2. Select a linkage or click Add to create an I/O linkage.

   The I/O Linkages details are displayed in the bottom pane.

I/O Interfaces can be added, edited, searched and deleted. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for 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. 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 from 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**.

15.6.1 I/O Linkages Details

- **Linkage Rule Name**: enter a unique name to identify the link.
- **Schedule Name**: from the drop-down list, select a schedule to apply to the linkage. Schedules must be configured first. See **Configure Schedules** in **Chapter 13: Global Configurations**.
- **Input Name**: select an input port from the drop-down list. This list contains all input ports configured in the system. An input port is selected to serve as the *in* side of the linkage.
- **Output Name**: select an output port from the drop-down list. This list contains all outputs ports configured in the system. An output port is selected to serve as the *out* side of the linkage.

Chapter 16: Configure Video, Storage, & Decoders

Configure video cameras and related devices in the following order:

1. **Configure External Storage Devices**
2. **Configure Cameras and Streams**
3. **Configure NLSS HD Media Decoders**

Cameras are controlled via the *Operations* > *Cameras* menu. See **Chapter 4: Controlling Cameras** for instructions on operating cameras.

If the Gateway is managed by RMS, Configuration > Video can only be accessed from the Gateway (Sites) menu level.

16.1 CONFIGURE EXTERNAL STORAGE DEVICES

NLSS supports external storage connected directly or 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.

16.1.1 Storage Table

The Storage table provides an overview of the status of each drive. Items in the table can be can be added, configured, searched and deleted.

1. Select **Configuration > Video > Storage** from the Main Menu.

   The *Storage* table is displayed.

2. Select a storage device from the table. The *Storage Details* pane is displayed.

Storage devices can be added, edited, searched and deleted. See **Adding Storage Devices**. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for edit, delete, and search instructions.

16.1.2 Storage Details

- **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.

Note: 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.

16.1.3 Adding Storage Devices

The following devices can be added from the Configuration > Video > Storage screen:

- **USB Storage Devices**
- **eSATA Storage Devices**
- **iSCSI Storage Devices**
- **NAS Storage Devices**

16.1.3.1 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 Gateway automatically discovers and configures an attached USB storage device.
3. Optionally, to change the **Disc Name** in the Storage Details.
   a. Select the device in the Storage table.
   b. Enter the new **Disc Name**.
   c. Click **Save** to keep the change.
      » Click **Cancel** to restore the previous setting.

16.1.3.2 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 **Disc Name** in the Storage Details.
   a. Select the device in the Storage table.
   b. Enter the new **Disc Name**.
   c. Click **Save** to keep the change.
      » Click **Cancel** to restore the previous setting.

16.1.3.3 iSCSI Storage Devices

1. Click **Add** in the Storage table.

   is displayed.
2. Enter a **Disc Name** in the *Storage Details* pane.
3. Select **iSCSI** from the **Device Type** drop-down list.
4. Enter the **Target IP Address**.
5. Click plus (**+**) 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.

16.1.3.4 NAS Storage Devices

1. Click **Add** in the Storage table.
2. Enter a **Disc Name** in the *Storage Details* pane.
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.

16.2 CONFIGURE CAMERAS AND STREAMS

The NLSS Gateway discovers cameras and lists them 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** in **Chapter 13: Global Configurations**.
- Holidays do *not* override schedules associated with cameras and other video streams.

The Cameras table provides an overview of the status for each camera and stream monitored by the system.

1. Select **Configuration > Video > Cameras** from the main menu.

   The *Cameras* table is displayed
2. Select a camera from the table.

The *Camera Details* are displayed in the bottom pane, with 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.

Video streams can be added manually. see **Add RTSP and HTTP Streams** for instructions. Cameras and streams can be edited, searched and deleted. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions.

16.2.1 Camera Details General Tab

Discovering a camera does not guarantee the system is able to connect to that camera. Set the parameters in the General tab for the system connect to the camera.

When you select a camera from the list in the *Configuration* > *Video* > *Cameras* screen, a series of parameters appear in the Camera Details' General tab, even if the camera is not currently connected to the system.

16.2.1.1 EDITABLE PARAMETERS

- **Admin State**: a drop-down list of the operational states for the selected camera. Select a different state from the list, as needed.
  - **Pre-Provisioned**: the system discovered this camera, but has not attempted to connect to it. This option cannot be reselected after In Service or Out of Service has been selected.
  - **In Service**: the system is 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. A common cause is an incorrect username or password for logging into this camera.

- **Username**: the user name for accessing this camera. User name is set locally on the camera, and then entered in this field to authorize the connection.

Note: Not all cameras require the user name to be changed.

- **Password**: the password for accessing this camera. The password is set locally on the camera, and then entered in this field to authorize the connection.

- **Device Name**: the system provides a default name, constructed when the camera is discovered. This default name includes the model and IP address of the selected camera. This default name can be kept or customized in this field.

- **Device Location**: optional text field to enter the physical location of this camera.

16.2.1.1.1 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 connect to the system.

Parameters for HTTP streams are the same as RTSP streams, except for the removal of the **Use Multicast** parameter.

16.2.1.2 READ-ONLY PARAMETERS

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 serial number of this camera.

- **IP Address**: the IP address of this camera. Click the IP address to open the camera's web page.

- **Firmware Version**: the firmware version running on this camera.

- **Hardware Version**: the hardware version, if any, of this camera.

- **MAC Address**: the MAC address of this camera.

16.2.2 Camera Details Stream Tab

The Stream tab is available only after the NLSS Gateway successfully connects to a camera, and that camera as **In Service**.

1. Select **Configuration > Video > Cameras** from the Main Menu.
2. Select a camera from the table.
3. Open the **Stream** tab.

The Stream tab contains three sections:

- List of Streams
- Video Stream Parameters
- Audio Stream Parameters

16.2.2.1 List of Streams

Some cameras have multiple outputs, each with a different codec and/or resolution. For example: Stream0 and Stream 1.

1. To enable a stream, check the box next to a Stream in the **Stream** tab.
   – Repeat this step for additional streams, if any.
   – Clear a check box to disable a stream.
2. 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.

Only selected streams in the Stream tab are available for viewing and recording, as discussed in **Monitor Cameras from the Operations Menu** in **Chapter 4: Controlling Cameras**.

16.2.2.2 Video Stream Parameters

When a specific stream is selected, the Video Stream and Audio Stream fields update to match the selection.

The NLSS Gateway receives this data from the camera. These fields are dependent on the type of camera and stream. Most of these fields are 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.
- **Advanced**: click to display two check boxes.
  - **TCP**: select to change the stream protocol from UDP to TCP for better bandwidth usage.
  - **SkipToKeyFrame**: select to optimize video in a congested network.

  Save any changes made to these settings.

16.2.2.3 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.

16.2.3 Camera Details Recording Tab

The Recording tab is available only after the NLSS Gateway successfully connects to a camera, and that camera as **In Service**.

1. Select **Configuration > Video > Cameras** from the Main Menu.
2. Select a camera from the table.
3. Open the **Recordings** tab.

The Recording tab enables recording for a selected camera and its streams. Configure recording in the **Stream Settings** and **Camera Settings** in this tab.

16.2.3.1 Stream Settings

If the selected camera outputs more than one stream, Stream Settings lists all available streams. A Schedule can be associated with a stream for recording, if the stream was enabled (checked) and the setting was saved in the Stream tab.

- **Stream**: available streams output from the selected camera.
- **Recording Schedule**: a drop-down list of the Schedules configured for the system, such as **Never**, **Always**, etc. Select a Schedule to associate with the selected stream. A stream must be selected in the Stream tab to set a Recording Schedule.

  See **Configure Schedules** in **Chapter 13: Global Configurations** for more information on Schedules.

After a stream is enabled in the Stream tab, associate a Schedule 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.

16.2.3.2 Camera Settings

Camera Settings apply to all streams output by the selected camera.

Note: These settings override the default Groomer settings. See **Configure Actions** in **Chapter 13: Global Configurations**.

- **Recording to Volume**: from the drop-down list, select a storage device 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): t**he maximum number of days a recording from the selected camera is saved on disc before being auto-deleted by the Groomer.

The Camera Settings apply to all streams that are 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.

16.2.4 Cameras Actions

The *Configuration* > *Video* > *Cameras* screen provides these options:

- **Connect to a Camera**
- **Add RTSP and HTTP Streams**

Cameras and video streams also can be edited, searched and deleted. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions.

16.2.4.1 Connect to a Camera

1. Select **Configuration > Video > Cameras** from the Main Menu.
2. Select a camera from the table.
3. In the **General** tab, enter the **Username** and **Password** allow the system to log into the camera.

Note: A camera’s user names and passwords are set locally at the camera, not from the NLSS Web Interface. Consult the camera’s manufacturer to determine the 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.

16.2.4.2 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.
2. Click **Add** to add a stream.
3. Complete the fields in the **General** tab.
   – Enter a name for the camera in the **Device Name** field.
   – 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.

16.3 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.

Starting in NLSS Unified Security Suite 2.3, decoders also can be added manually.

For details on NLSS decoders, see the *NLSS HD Media Decoder (DC-400, DC-400-2): User Manual* available at **www.NLSS.com**.

16.3.1 Decoder Table

The Decoder table provides an overview of the decoder.

1. Select **Configuration > Video > Decoder** from the Main Menu.

   The *Decoder* table is displayed.

2. Select a Decoder from the table.

   The *Decoder Details* pane is displayed.

Decoders can be added, edited, searched and deleted. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions.

Note: Decoders only need to be added if the device is located on a different network than the Gateway. The Gateway auto-discovers decoders on the same network.

16.3.2 Decoder Details

Some fields in the Decoder Details can be edited, while others cannot.

- **Editable Parameters**
- **Read-Only Parameters**

16.3.2.1 EDITABLE PARAMETERS

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**: enter a unique name to identify the decoder
- **Device Location**: optional text field to enter the physical location of this decoder.
- **Device Model**: select the model number of the NLSS Decoder from the drop-down list.

Note: The NLSS Gateway can access a decoder only if the correct values are entered in the Username and Password fields. The correct values are those that the decoder has been configured to accept.

16.3.2.2 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.
- **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.

Chapter 17: Configuring Permissions

Permissions is a new feature in NLSS Gateway version 2.3. Permissions are configured using **Groups**, **Roles**, and **Users**.

Permissions allow a system administrator to configure *Roles* that permit or deny *Users* the ability to operate or configure specific devices and use specific functions.

Permissions for specific devices are controlled by *Groups*. When an item is added to a group, access is allowed to that item. Groups are applied to roles. Roles are also used to configure other permissions that allow access to Gateway modules (Operations, Configuration, Events) and their menu options.

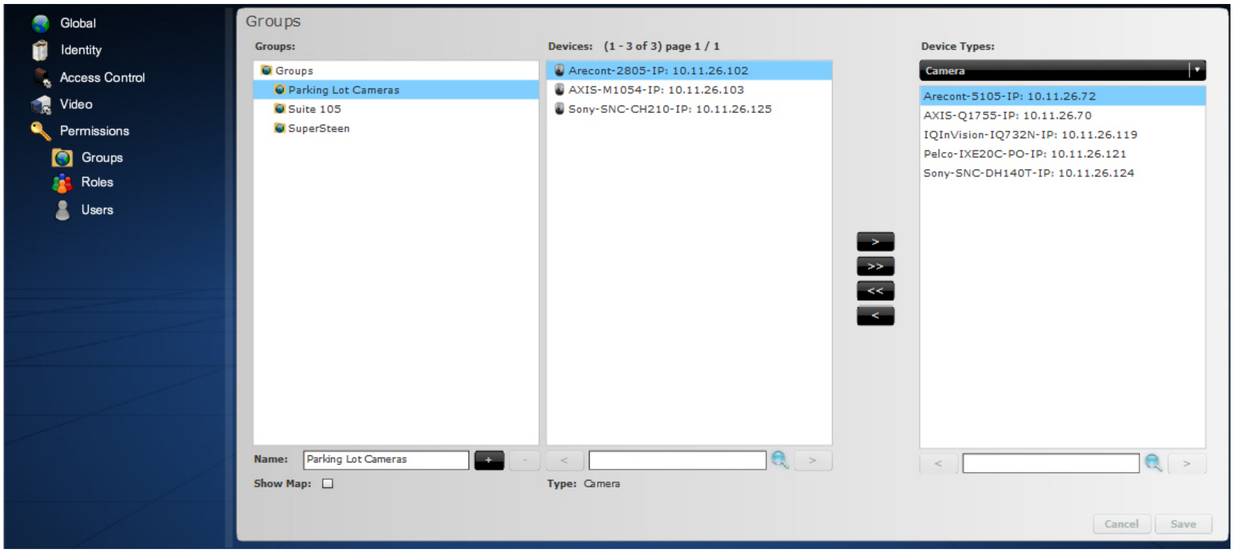
Roles are applied to users to define their permissions. Three default roles are included with the system: Superuser, Admin, and Operator. Before new users can be added to the system, a role must be cloned to apply to that user. The cloned role can be edited to provide the desired permissions. When a new user is added, a cloned role must be applied to that user.

17.1 APPLYING PERMISSIONS EXAMPLE

A parking lot security guard may only need to view cameras covering the parking lot. However, this user does not need access to create Views or Sequences, or access to Doors, Cardholder/User, Reporting, and Events screens. Use the Configurations > Permissions options to set up this user.

Note: The following example provides a high level overview of applying permissions to a user. Specific instructions for each step are provided in this chapter.

1. Open **Configuration > Permissions > Groups**.
   a. Create a group called *Parking Lot Cameras*.
   b. Add the desired cameras, views and sequences.



Groups:
- Groups
  - Parking Lot Cameras
  - Suite 105
  - SuperSteen

Devices: (1 - 3 of 3) page 1 / 1
- Arecont-2805-IP: 10.11.26.102
- AXIS-M1054-IP: 10.11.26.103
- Sony-SNC-CH210-IP: 10.11.26.125

Device Types: Camera
- Arecont-5105-IP: 10.11.26.72
- AXIS-Q1755-IP: 10.11.26.70
- IQInVision-IQ732N-IP: 10.11.26.119
- Pelco-IXE20C-PO-IP: 10.11.26.121
- Sony-SNC-DH140T-IP: 10.11.26.124

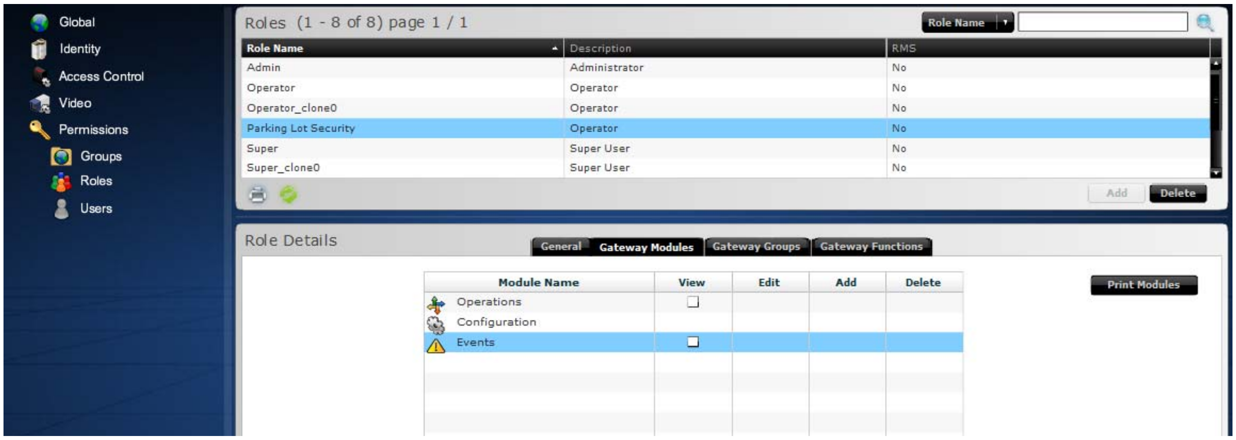
Name: Parking Lot Cameras

Show Map: □

Type: Camera

See **Groups** for instructions.

2. Open **Configuration > Permissions > Roles**.
   a. Create a clone of the Operator role, and name it *Parking Lot Security*.
   b. In the Gateway Modules tab for the cloned role, disable View permissions for Operations and Events. By default, the Operator has no Configuration permissions. Top level permissions must be disabled before permissions configured by groups can be applied.



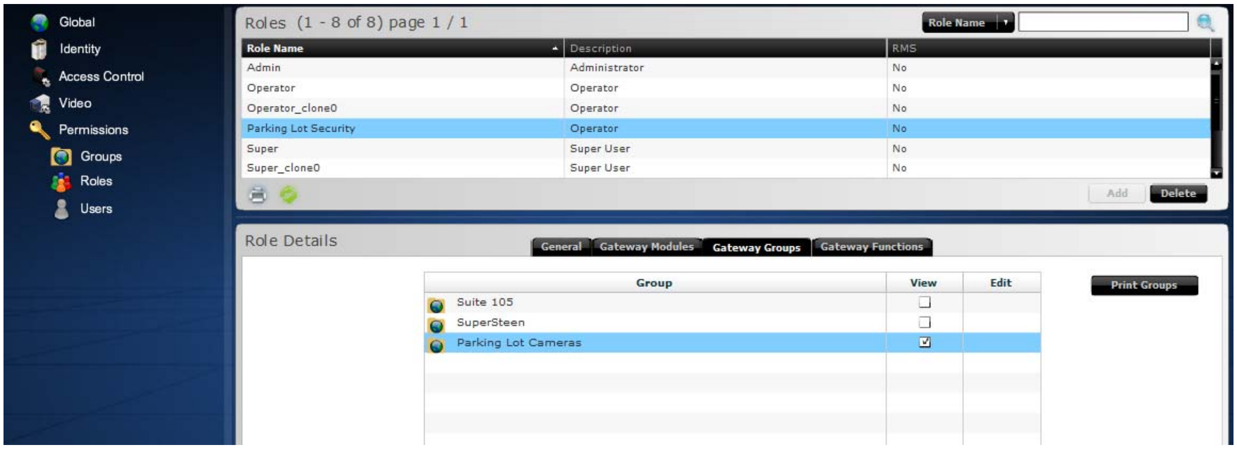
Roles (1 - 8 of 8) page 1 / 1

Role Name	Description	RMS
Admin	Administrator	No
Operator	Operator	No
Operator_clone0	Operator	No
Parking Lot Security	Operator	No
Super	Super User	No
Super_clone0	Super User	No

Role Details

Module Name	View	Edit	Add	Delete
Operations	□			
Configuration				
Events	□			

c. In the Gateway Groups tab, add the *Parking Lot Cameras* group to the for this role.



Roles (1 - 8 of 8) page 1 / 1

Role Name	Description	RMS
Admin	Administrator	No
Operator	Operator	No
Operator_clone0	Operator	No
Parking Lot Security	Operator	No
Super	Super User	No
Super_clone0	Super User	No

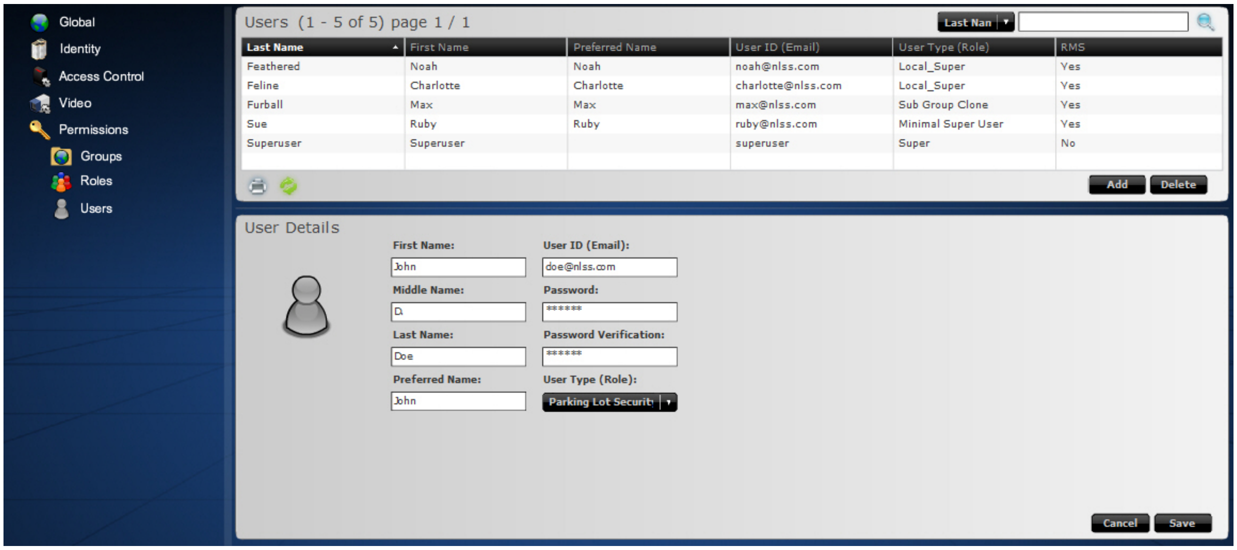
Group	View	Edit
Suite 105	☐	
SuperSteen	☐	
Parking Lot Cameras	☑	

See **Roles** for instructions.

3. Open **Configuration > Permissions > Users**.

a. Create a new user.

b. Select the User Type (Role) of *Parking Lot Security*.



Users (1 - 5 of 5) page 1 / 1

Last Name	First Name	Preferred Name	User ID (Email)	User Type (Role)	RMS
Feathered	Noah	Noah	noah@nlss.com	Local_Super	Yes
Feline	Charlotte	Charlotte	charlotte@nlss.com	Local_Super	Yes
Furball	Max	Max	max@nlss.com	Sub Group Clone	Yes
Sue	Ruby	Ruby	ruby@nlss.com	Minimal Super User	Yes
Superuser	Superuser		superuser	Super	No

User Details

First Name: John
User ID (Email): doe@nlss.com
Middle Name: D.
Password: ******
Last Name: Doe
Password Verification: ******
Preferred Name: John
User Type (Role): Parking Lot Securit

See **Users** for instructions.

This new user can log into the Gateway, and watch the cameras, views and sequences assigned in the Parking Lot Cameras group, plus the events associated with these cameras.

17.2 GROUPS

A group is a collection of cameras, decoders, doors, users, cardholders, views and sequences. In RMS, groups consist of Gateways and Multiviews on the RMS Level.

Groups can be created, edited and deleted. Maps or other JPEG images can be used as a background. The Device lists can be searched.

Groups are collections of cameras, decoders, doors, users, cardholders, views and sequences. In RMS, groups consist of Gateways and Multiviews on the RMS Level. Groups can have different types of objects in the same group. Groups are used for access to devices and operations, not for bulk configuration of like objects.

Groups can be used to enable and disable access to certain devices and operations for users. Groups are assigned to roles, which set permissions for using the system's features. Users are then assigned a role, defining the parameters of their permissions.

Important: Cameras, Views, and Sequences operate in a hierarchy. If a camera is not included in a group, then Views and Sequences containing that camera are not available. If a View is not included in a group, then Sequences with that View are not available.

17.2.1 Example

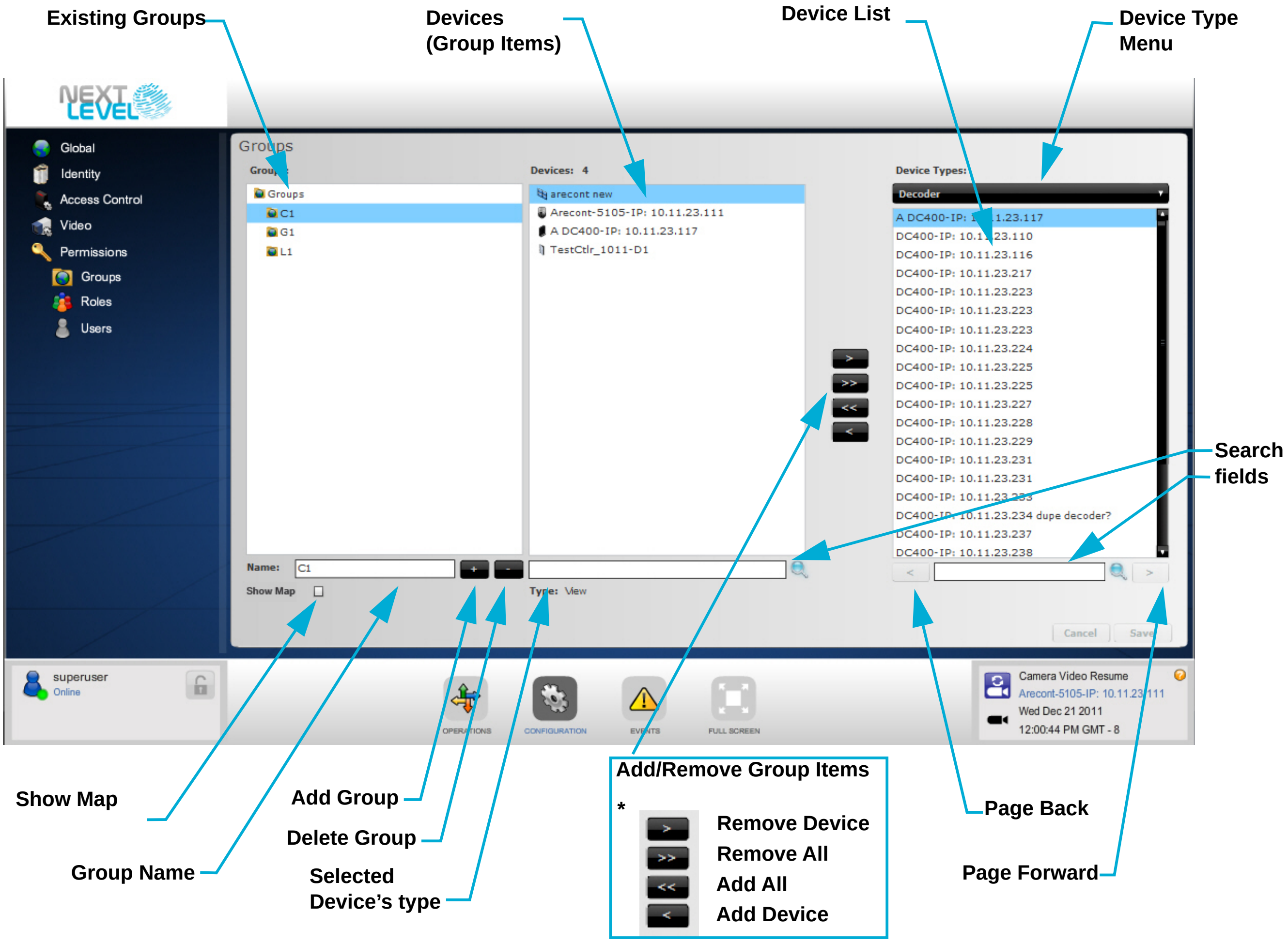
For example, a series of cameras and doors on the first floor could be placed in a group. That group is assigned to a role responsible monitoring that floor.

Users are then assigned that role.

Those users only would be able to operate the cameras and doors for the first floor, and would not be able to see cameras and doors from other floors.

17.2.2 Groups Panel

Groups are created and maintained from **Configuration > Permissions > Groups**.



17.2.3 Create a Group

1. Select **Configuration > Permissions > Groups** from the Main Menu.
2. Click **Groups** in the Groups list.
   - Click a group name to create a sub-group under an existing group.
3. Click **Add Group** (**+**).

Note: By default, **New Group** is displayed in the Groups list when a group is added. The name is not changed until it is entered in the **Name** field and the changes are saved.

4. Enter a group **Name**.
5. Optionally, select **Show Map** to enable adding a map or floor plan as a background for this group.

   The graphic is imported in **Operations > Groups >** ***group name***, where *group name* identifies the group. See **Adding and Using Maps** in **Chapter 9: Using Groups**.

6. Select a category from the **Device Type** drop-down menu.
7. Click the desired device.
   – Use **Search** to narrow the list.
   – Use **Page Forward** and **Page Back** to toggle between pages of the list.
8. Click **Add Device** (**<**) to include the item in the group.
   – Click **Add All** (**<<**) to include all list items in the group.
   – Click **Remove Device** (**>**) to take an item out of the group.

Note: Click **Remove All** (**>>**) to delete all items from the group. This action cannot be undone, and the group items have to be added again.

9. Click **Save** to keep the changes. The name is updated in the Groups list.
   – Click **Cancel** to clear the fields and not create the new group.

17.2.4 Edit a Group

1. Click **Configuration > Permissions > Groups**.
2. Select a **Group**.
3. Edit the **Group Name**, if desired.
4. Add a device, if desired.
   a. Select a category from the **Device Type** drop-down menu.
   b. Click the desired device.
   c. Click **Add Device**.
      » Click **Add All** to include all list items in the group.
5. Click **Remove Device** to take an item out of the group, if desired.
   – Click **Remove All** to delete all items from the group.
6. Click **Save** to keep the changes.
   – Click **Cancel** to ignore the changes and restore the settings.

17.2.5 Delete a Group

1. Click **Configuration > Permissions > Groups**.
2. Select a **Group**.
3. Click **Delete Group**.
4. Click **Yes** to confirm the deletion when prompted.
   – Click **No** to abort the deletion and keep the group.

17.3 ROLES

Roles define the capabilities of the users operating the NLSS Gateway. The *Configuration > Permissions > Roles* screen provides capabilities to manage roles.

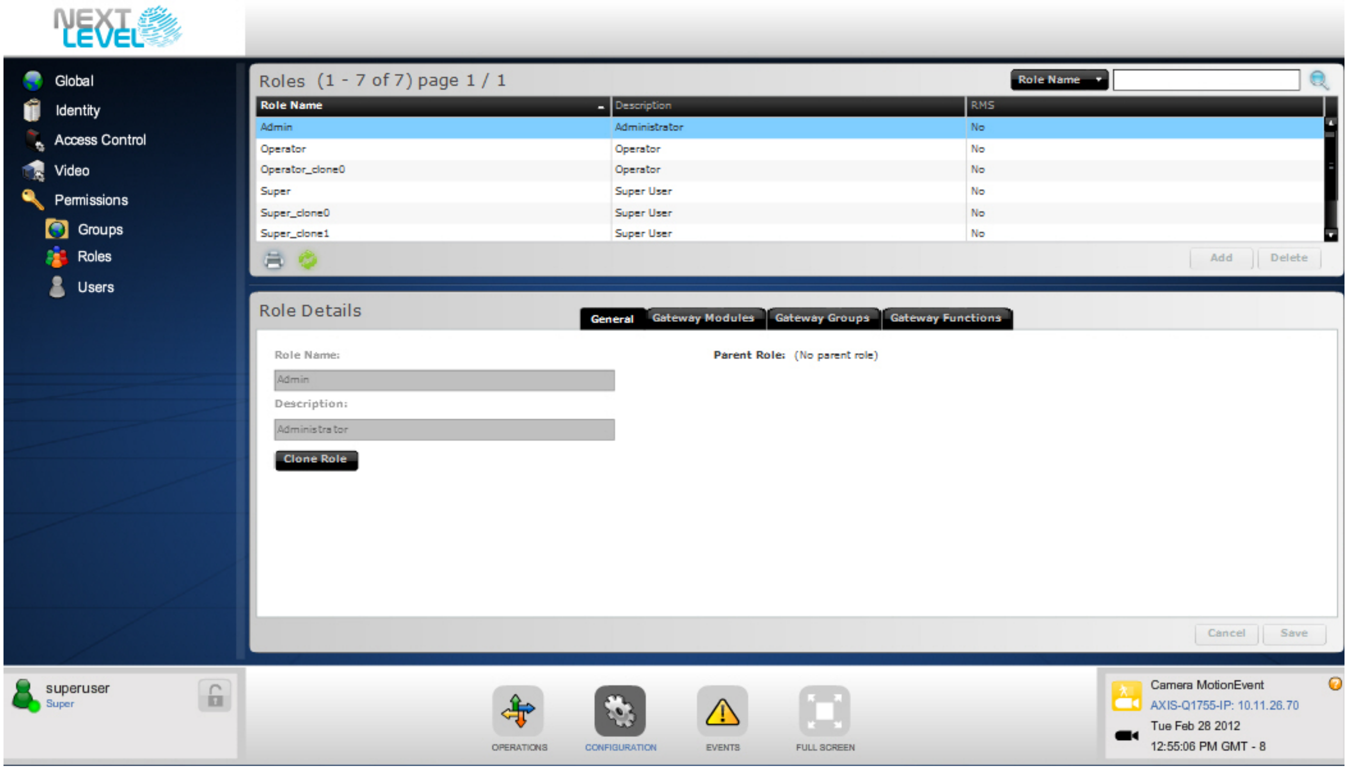
If a Gateway is managed via RMS, roles are configured at the RMS level, not at site level.

1. Select **Configuration > Permissions > Roles** from the Main Menu. Access the Configuration menu from the *Sites* screen, if running RMS.

   The *Roles* screen is displayed listing the default and created (cloned) roles.

2. Select a role.

   The *Roles Details* pane is displayed.



Roles (1 - 7 of 7) page 1 / 1

Role Name	Description	RMS
Admin	Administrator	No
Operator	Operator	No
Operator_clone0	Operator	No
Super	Super User	No
Super_clone0	Super User	No
Super_clone1	Super User	No

Role Details

Role Name: Admin

Description: Administrator

Parent Role: (No parent role)

The NLSS Gateway has four pre-defined roles, three of which are only available at the RMS level. These default roles cannot be edited or deleted.

- **Superuser**: the *root* or Primary User at the Gateway. Superuser is the only default role at the local Gateway level. The Superuser has full access to all menus and features in the NLSS Web Interface.
- **Administrator**: run and modify features under the Configuration menu. This role can be cloned at the RMS level and transferred to the Gateways.
- **Operator**: run and modify camera features under the Operations menu.This role can be cloned at the RMS level and transferred to the Gateways.
- **Master** (RMS only): the *root* or Primary User at RMS. Only one Master can be included in a system, and this role *cannot* be cloned.

Note: The Master role is transferred to the Gateways controlled by RMS, but the default Superuser role for each Gateway is not transferred up to the RMS level. These default roles do not have edit permission for each other, but can edit all clone roles based on Superuser, Operator or Administrator. No clone can edit either Primary User role.

New roles are created by cloning and editing an existing role. Roles that are created can be edited, clones and deleted, as described in this section. The Roles list can be searched. See **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions.

Before new users can be added to the system, a default role must be cloned to apply to the user. The default roles cannot be applied to users.

17.3.1 Roles Details

Settings in the *Roles Details* pane determine whether a menu option is available to users assigned a role, and the permissions that each role has in using an option.

- **View**: the menu option is visible to users assigned this role.
- **Edit**: users assigned this role can change items listed under this menu option.
- **Add**: users assigned this role can create new items to list under this menu option.
- **Delete**: users assigned this role can remove items listed under this menu option.

Note: Edit, Add, and Delete capabilities are not available for some options. For example, Event Types cannot be added or deleted. These limitations are described in the respective sections for each option.

If View is not selected for an option, the corresponding menu item is not displayed when a user assigned to that role logs in.

The Roles Details pane contains four tabs: General, Gateway Modules, Gateway Groups, and Gateway Functions.

17.3.1.1 General Tab

The General tab allows a role to be identified and cloned.

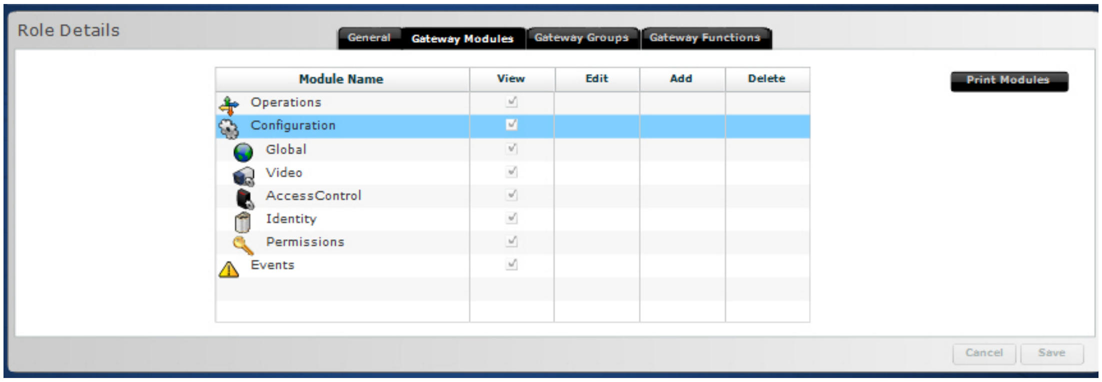
- **Role Name**: enter a unique identifier for the role. This field cannot be edited for the default roles.
- **Description**: enter text to clarify the role to a user. This field is left blank for the default roles.
- **Clone Role**: click this button to create an editable copy of the selected role. Default and created roles can be cloned.
- **Parent Role**: the role from which the selected role was cloned.

Click **Save** to keep any changes, or **Cancel** to return the fields to their previous settings.

17.3.1.2 Gateway Modules Tab

Modules are the top level options selected from the Main Menu: Operations, Configuration, and Events. Permissions for the modules are set in this tab. This tab is labeled as **RMS Modules** at the RMS level.

1. Select **Configuration > Permissions > Roles** from the Main Menu.
2. Select a role.
3. Open the **Gateway Modules** tab.
4. Click on a **Module Name** to expand the list to show the menu options available.
   - The Operations module expands one level.
   - The Configuration module expands two levels into groupings (Global, Video, etc.) and individual menu options.
   - Events does not expand.



Module Name	View	Edit	Add	Delete
Operations	☑			
Configuration	☑			
Global	☑			
Video	☑			
AccessControl	☑			
Identity	☑			
Permissions	☑			
Events	☑			

5. Click the check box to enable (checked) or disable (unchecked) a desired permission.

Note: Some Menu options, especially under the Operations module, only have a View permission to enable or disable.

6. Optionally, click **Print Modules** to print the settings for a selected module.
7. Click **Save** to keep the settings.
   - Click **Cancel** to return to the previous settings.

Important: If a role does not have access to cameras or other devices, the user can still see cameras and doors via Events and Reports, if Events and Reports have not been denied to that role.

A system administrator with appropriate permissions must choose how to handle this situation by either permitting or denying access to Events and Reports for the particular role.

Because of this, Cameras, Views, and Sequences operate in a hierarchy. If Cameras are disabled, then Views and Sequences are not available. If Views are disabled, then Sequences are not available.

Note that if Events and Reports are denied in general, the user can still access Events and Reports on a per device basis via the device mini pane.

The following table provides a quick reference to the Gateway Module tab settings for the default roles.

Default Role	Operations Module Options	Configuration Module Options	Events Module
Administrator	• Cameras: *View video only* • No access to remaining options	• Global: – RMS, Customer, Sites, Gateways, Event Type, Event Severity, Groomer Settings: *View, Edit* – Holidays, Schedules, Event Linkages, Action: *View, Edit, Add, Delete* • Video: *View, Edit, Add, Delete for all options* • Access Control: *View, Edit, Add, Delete for all options* • Identity: – Access Levels, Card Profiles, Badge Profiles, Cardholders: *View, Edit, Add, Delete* – Cardholder - User Defined: *View, Edit* • Permissions: – Groups: *View, Edit, Add, Delete* – Roles: *No access* – Users: *No access*	*No access*
Operator	• Cameras: *View* • Decoders: *View* • Doors: *View* • Cardholders/Users: *View* • Reporting, Groups: *View* • Views and Sequences: *View, Edit, Add, Delete* • Groups: *View*	*No access*	*View*
Superuser	• Cameras: *View* • Decoders: *View* • Doors: *View* • Cardholders/Users: *View* • Reporting: *View* • Views: *View, Edit, Add, Delete* • Sequences: *View, Edit, Add, Delete* • Groups: *View, Edit*	• Global: – RMS, Customer, Sites, Gateways, Event Type, Event Severity, Groomer Settings: *View, Edit* – Holidays, Schedules, Event Linkages, Action: *View, Edit, Add, Delete* • Video: *View, Edit, Add, Delete for all options* • Access Control: *View, Edit, Add, Delete for all options* • Identity: – Access Levels, Card Profiles, Badge Profiles, Cardholders: *View, Edit, Add, Delete* – Cardholder - User Defined: *View, Edit* – Permissions: *View, Edit, Add, Delete for all options*	*View*

17.3.1.3 GATEWAY GROUPS

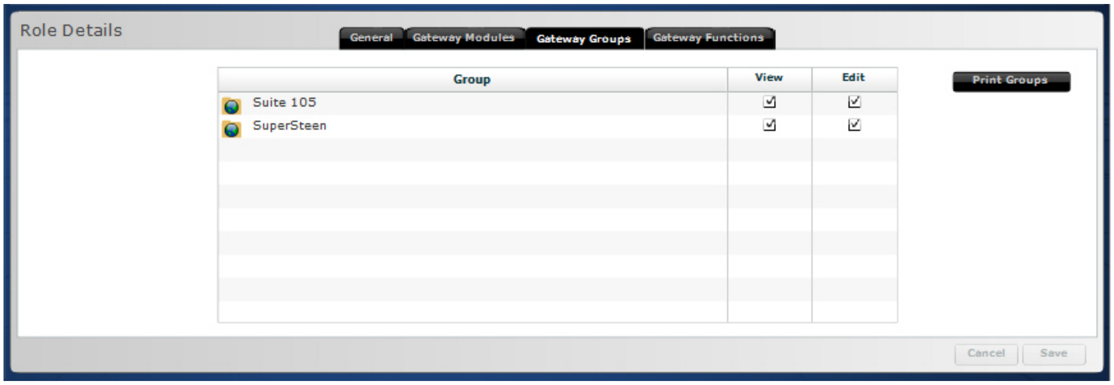
The Gateway Groups tab lists all groups created under Configuration > Permissions >Groups. View and Edit permissions are set for each group in this tab.

Default Role	Permissions
Administrator	• *View, Edit*
Operator	• *View only*
Superuser	• *View, Edit*

This tab is labeled as **RMS Groups** at the RMS level.

Important: Before a group can be applied to a role, the module options applicable to the items in that group must be disabled. For example, if a group includes doors, then the Doors permissions under the Operations module, must be deselected. The items in the groups that are applied to a role set up permissions for that role.

1. Select **Configuration > Permissions > Roles** from the Main Menu.
2. Select a role.
3. Open the **Gateway Groups** tab.



Group	View	Edit
Suite 105	☑	☑
SuperSteen	☑	☑

4. Click the **View** and **Edit** check boxes to enable (checked) or disable (unchecked) a desired permission.
5. Optionally, click **Print Groups** to print the Gateway Groups settings.
6. Click **Save** to keep the settings.
   – Click **Cancel** to return to the previous settings.

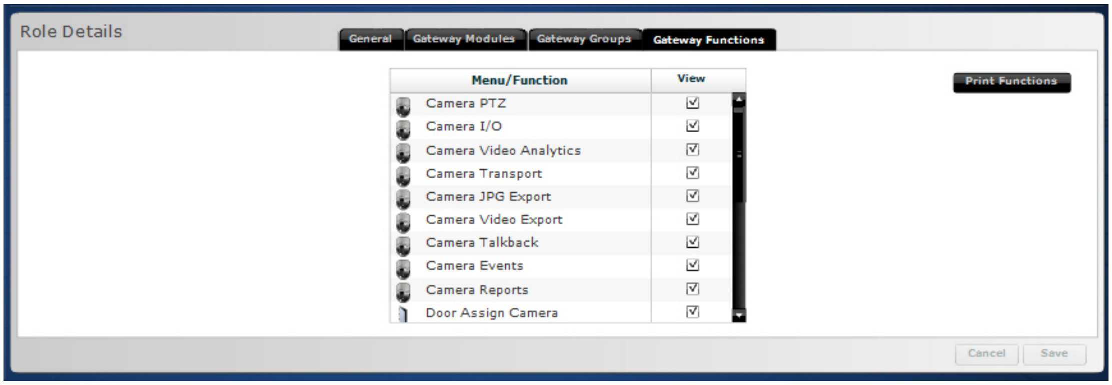
17.3.1.4 Gateway Functions

The Gateway Functions tab sets permissions for Operations menu functions for Cameras, Doors, Cardholders, Decoders, and Users. Only a View permission is set in this tab.

Not all roles have access to these functions.

Default Role	Permissions
Administrator	• *No access*
Operator	• *View*
Superuser	• *View*

1. Select **Configuration > Permissions > Roles** from the Main Menu.
2. Select a role.
3. Open the **Gateway Functions** tab.



Menu/Function	View
Camera PTZ	☑
Camera I/O	☑
Camera Video Analytics	☑
Camera Transport	☑
Camera JPG Export	☑
Camera Video Export	☑
Camera Talkback	☑
Camera Events	☑
Camera Reports	☑
Door Assign Camera	☑

4. Click the **View** check box to enable (checked) or disable (unchecked) a desired permission.
5. Optionally, click **Print Functions** to print a list of functions indicating which are selected.
6. Click **Save** to keep the settings.
   – Click **Cancel** to return to the previous settings.

17.3.2 Cloning a Role

Only cloned roles can be applied to users. Cloned roles can be edited to customize permissions and what menu options users can see.

The default roles cannot be applied to users.

Note: When a role is cloned, permissions cannot be added for an area that the parent role could not see. Permissions can only be subtracted.

For example, a cloned Administrator role cannot be given access to Operation menu options. If a new role is requires permissions in Operations and Configuration, clone Superuser or a similar role and adjust the permissions accordingly. Cloned roles also can be cloned.

1. Select **Configuration > Permissions > Roles** from the Main Menu.
2. Select a role.
3. Click **Clone**.
4. Edit the tabs, as needed.
5. Click **Save** to keep the clone.
   - Click **Cancel** to delete the clone without saving.

17.3.3 Delete a Role

Cloned roles can be deleted. The default roles cannot be deleted.

1. Select **Configuration > Permissions > Roles** from the Main Menu.
2. Select a role.
3. Click **Delete**.
4. Click **Yes** when prompted to confirm the deletion.
   - Click **No** to abort the deletion and keep the role.

17.4 USERS

Users are the people monitoring, administering, and maintaining the security system through the NLSS Web Interface.

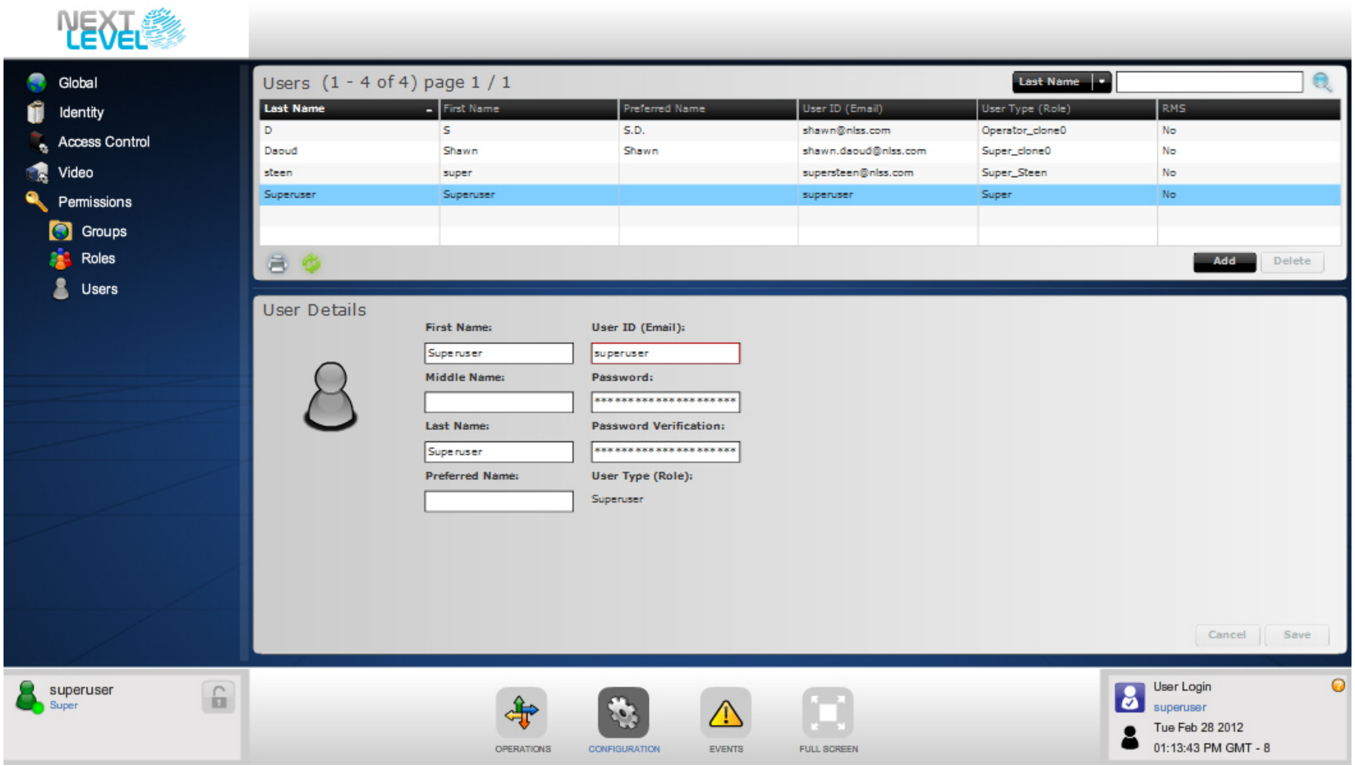
If a Gateway is managed via RMS, users are configured at the RMS level, not at local Gateway level.

1. Select **Configuration > Permissions > Users** from the Main Menu. Access the Configuration menu from the *Sites* screen, if running RMS.

   The *Users* screen is displayed listing the users.

2. Select a User.

   The *User Details* pane is displayed.



Users (1 - 4 of 4) page 1 / 1

Last Name	First Name	Preferred Name	User ID (Email)	User Type (Role)	RMS
D	S	S.D.	shawn@nlss.com	Operator_clone0	No
Daoud	Shawn	Shawn	shawn.daoud@nlss.com	Super_clone0	No
steen	super		supersteen@nlss.com	Super_Steen	No
Superuser	Superuser		superuser	Super	No

User Details

First Name: Superuser	User ID (Email): superuser
Middle Name:	Password: *********************
Last Name: Superuser	Password Verification: *********************
Preferred Name:	User Type (Role): Superuser

Default users are included with the NLSS Gateway. The roles of the same name can only be applied to these users.

- **Superuser**: the Superuser user has full permissions in the system.
- **Master** (RMS only): the *root* or Primary user at RMS. Only one Master is allowed per system, and cannot be deleted.

Users can be added, edited, searched and deleted. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions.

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

17.4.1 User Details

- **Name**: enter the **First Name**, **Middle Name**, **Last Name**, and **Preferred Name** of this user. Middle Name and Preferred Name are optional.

- **User ID (email)**: enter a unique email address to identify this user. The user enters this ID in the **User Name** field of the login page of the NLSS Web Interface.

Note: Be sure to enter an email address, not an alias, for the User ID. The User Details cannot be saved until an email address is entered.

- **Password**: enter a password for this user. The user enters this password in the **Password** field on the login page of the NLSS Web Interface.

Important: The default password for the Superuser is **superuser**.

The default passwords MUST be changed after the NLSS system is installed to close a hole in your security system.

When a system is switched to RMS, the Superuser password is switched back to **superuser**.

- **User Type (Role)**: select a role for this user. Only roles that have been cloned are displayed in the drop down menu. The default roles cannot be applied to new users.

  The default roles cannot be applied to a new user. The Superuser and Operator roles only are applied to the default users of the same name.

  See **Roles** for more information.

Chapter 18: Remote Management Services

Remote Management Systems (*RMS*) provides centralized configuration and management for NLSS sites (gateways). Video from multiple sites can be displayed in a single, multi-pane view.

In RMS installations, configuration is centralized, providing a single browser window to manage multiple sites. Settings can be configured for a specific site, as well as organization-wide settings.

In addition to the centralized management, users can access individual 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.

Note: When configuring RMS, it is recommended to have two browsers open, one for RMS and one for the target gateway. This setup allows verification that items are transferred properly. Once configuration is complete, RMS can be operated from one browser window.

Important: When configuring RMS for the first time, it is recommended that a local Gateway be configured and tested. The settings are uploaded to RMS host when RMS is enabled for the Gateway. Those settings can then be applied to other Gateways in RMS system, as needed.

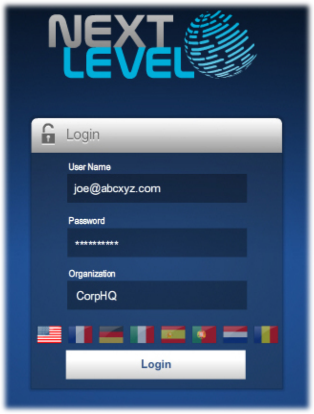
18.1 EXAMPLE OF RMS DEPLOYMENT

As an example, a company has three buildings on one campus: Administration, Research and Development, and a Warehouse. Each building contains a Gateway to manage the cameras and access control for that building. The Security office is located in the Administration building. Using RMS, the Gateway in each building can be monitored from using a single browser from the Security Office or any other location with web access.

Employees (cardholders) need access to the appropriate building or multiple buildings. Instead of configuring each employee’s identity separately on the three Gateways, the Identity parameters are configured at the RMS level, and transferred to the applicable Gateways. If an employee does not need access to a certain buildings, then his or her Cardholder settings are not transferred to the Gateway for that building.

For example, Warehouse employees may not need access to the Administration and Research and Development buildings.

1. Log in to the RMS host, using the User Name and Organization supplied by the Partner (the integrator who set up RMS), plus the appropriate password.



Login

User Name: joe@abcxyz.com

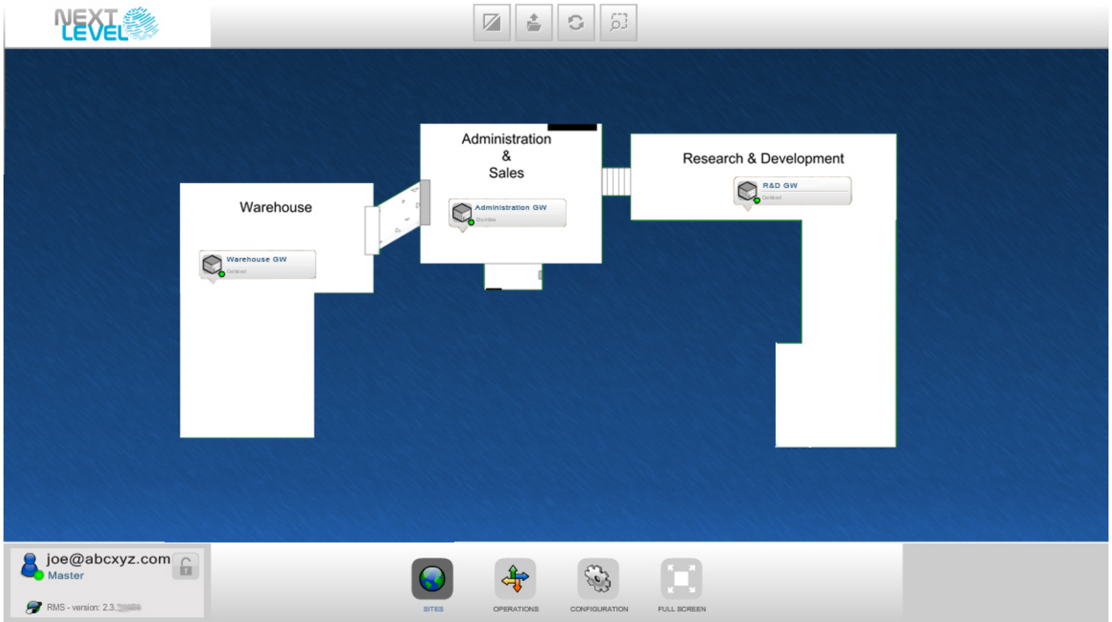
Password: **********

Organization: CorpHQ

See **RMS Hierarchy** and **Logging In to the NLSS RMS Web Interface** for more information.

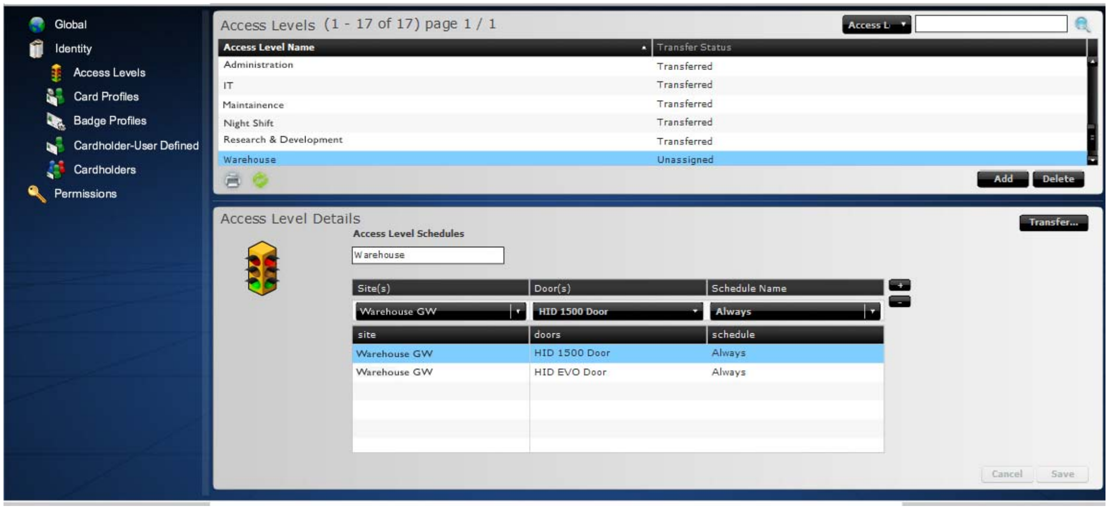
The RMS main screen is displayed with a map of the Sites (Gateways) in the RMS system.

2. Select **Configuration** from the Main Menu.



3. Select **Configuration > Identity > Access Levels** from the Main Menu.

4. Create an Access Level called *Warehouse*, which only applies to the Warehouse doors.



Access Levels (1 - 17 of 17) page 1 / 1

Access Level Name	Transfer Status
Administration	Transferred
IT	Transferred
Maintainence	Transferred
Night Shift	Transferred
Research & Development	Transferred
Warehouse	Unassigned

Access Level Details

Access Level Schedules

Warehouse

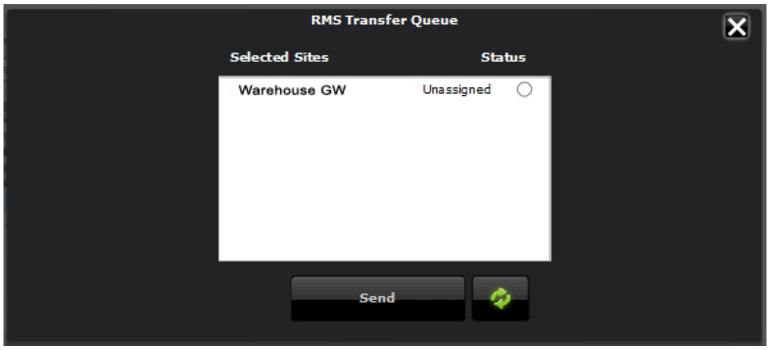
Site(s)	Door(s)	Schedule Name
Warehouse GW	HID 1500 Door	Always

site	doors	schedule
Warehouse GW	HID 1500 Door	Always
Warehouse GW	HID EVO Door	Always

See **Access Levels** for instructions.

5. Click **Transfer** to send the *Warehouse* Access Level to the Warehouse Gateway.

RMS automatically determines to which Gateways the selected doors apply when the *RMS Transfer Queue* is displayed.



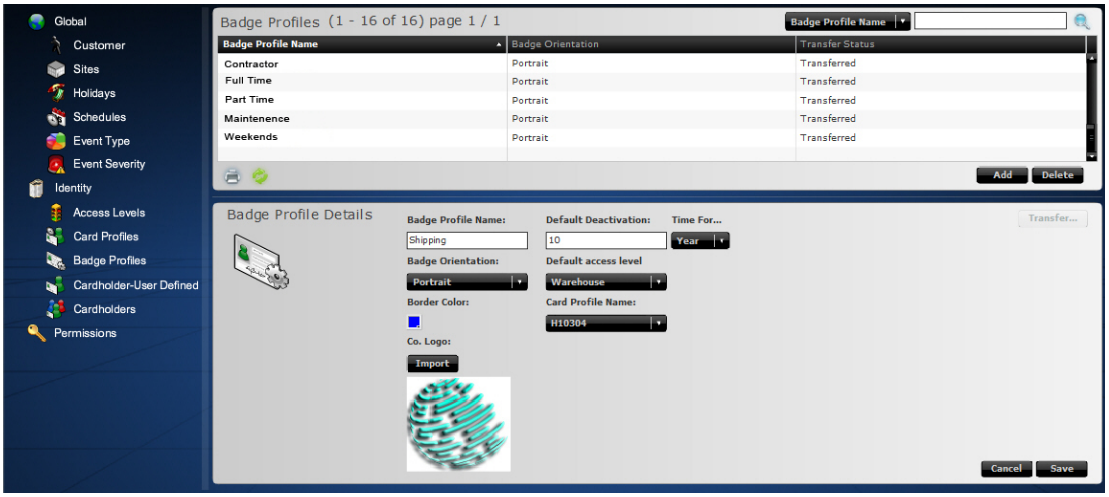
RMS Transfer Queue

Selected Sites	Status
Warehouse GW	Unassigned ○

See **Transferring RMS Settings** for more information.

6. Create a Badge Profile for the Warehouse employees. This badge profile can be assigned to any Warehouse employee to provide access to the doors in that building.

Since Shipping and Receiving employees operate the Warehouse, create a Badge Profile called *Shipping*, and apply the *Warehouse* access level. Any cardholder assigned the *Shipping* Badge Profile receives access to the Warehouse doors.



Badge Profiles (1 - 16 of 16) page 1 / 1

Badge Profile Name	Badge Orientation	Transfer Status
Contractor	Portrait	Transferred
Full Time	Portrait	Transferred
Part Time	Portrait	Transferred
Maintenence	Portrait	Transferred
Weekends	Portrait	Transferred

Badge Profile Details

Badge Profile Name: Shipping

Default Deactivation: 10

Time For... Year

Badge Orientation: Portrait

Default access level: Warehouse

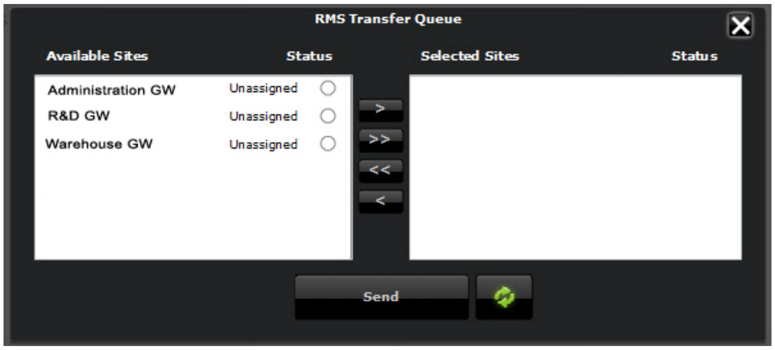
Border Color: 🟦

Card Profile Name: H10304

Co. Logo:

See **Badge Profiles** in for more instructions.

7. Transfer the *Shipping* Badge Profile to the Warehouse Gateway. Badge Profiles are conditional, meaning the Gateways for transfer can be selected

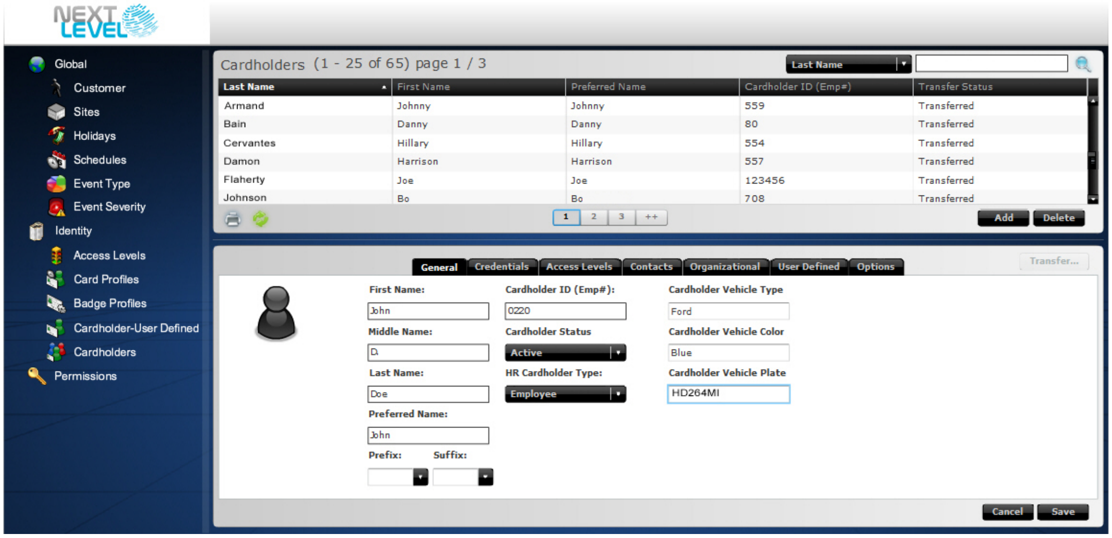


RMS Transfer Queue

Available Sites	Status		Selected Sites	Status
Administration GW	Unassigned	○		
R&D GW	Unassigned	○		
Warehouse GW	Unassigned	○		

See **Transferring RMS Settings** for more information.

8. Create a Cardholder to print a badge for each employee in Shipping and Receiving.



Cardholders (1 - 25 of 65) page 1 / 3

Last Name	First Name	Preferred Name	Cardholder ID (Emp#)	Transfer Status
Armand	Johnny	Johnny	559	Transferred
Bain	Danny	Danny	80	Transferred
Cervantes	Hillary	Hillary	554	Transferred
Damon	Harrison	Harrison	557	Transferred
Flaherty	Joe	Joe	123456	Transferred
Johnson	Bo	Bo	708	Transferred

First Name: John
Middle Name: D.
Last Name: Doe
Preferred Name: John
Prefix:
Suffix:
Cardholder ID (Emp#): 0220
Cardholder Status: Active
HR Cardholder Type: Employee
Cardholder Vehicle Type: Ford
Cardholder Vehicle Color: Blue
Cardholder Vehicle Plate: HD264MI

9. Enter the Shipping Badge Profile in the Credentials tab of the Cardholder screen.
   See **Cardholders** for instructions.

10. Transfer the Cardholder settings to the Warehouse Gateway.
    See **Transferring RMS Settings** for more information.+

18.2 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, transferring configurations. The customer also can configure settings specific to a location.
- *Partner*—The organization that provides the NLSS service to customers. A Partner can have multiple customers. The NLSS Partner Web Interface is discussed in the RMS Partner documentation.

Important: When a site is managed through RMS, certain configuration settings are read-only at the local level. These settings are transferred from the RMS level.

This chapter discusses the configuration steps that a customer takes to set up RMS.

18.3 LOGGING IN TO THE NLSS RMS WEB INTERFACE

The login for RMS is different than the login for a user managing a site.

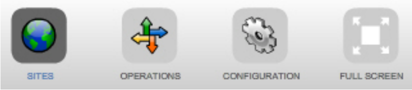
1. In a web browser, enter the URL for the NLSS RMS Web Interface, as provided by the Partner.
2. Enter the credentials in the login screen.
   a. **User Name**: this name is configured by the Partner. This name cannot be changed in the RMS Web Interface.
   b. **Password**: a default password is provided by the Partner. The password can be changed in the RMS Web Interface.
   c. **Organization**: a name set by the Partner to encompass the customer's sites. The organization name cannot not be changed in the RMS Web Interface.
3. Click **Login**.

The RMS Interface Site Map is displayed with links to the RMS registered sites.

Important: If the Superuser password has been changed on a local Gateway, it is reset to the default of **superuser** when the Gateway is connected to RMS. The local, Superuser password can be changed back to the previous password or to another password after the connection with RMS is established.

18.4 RMS MAIN MENU

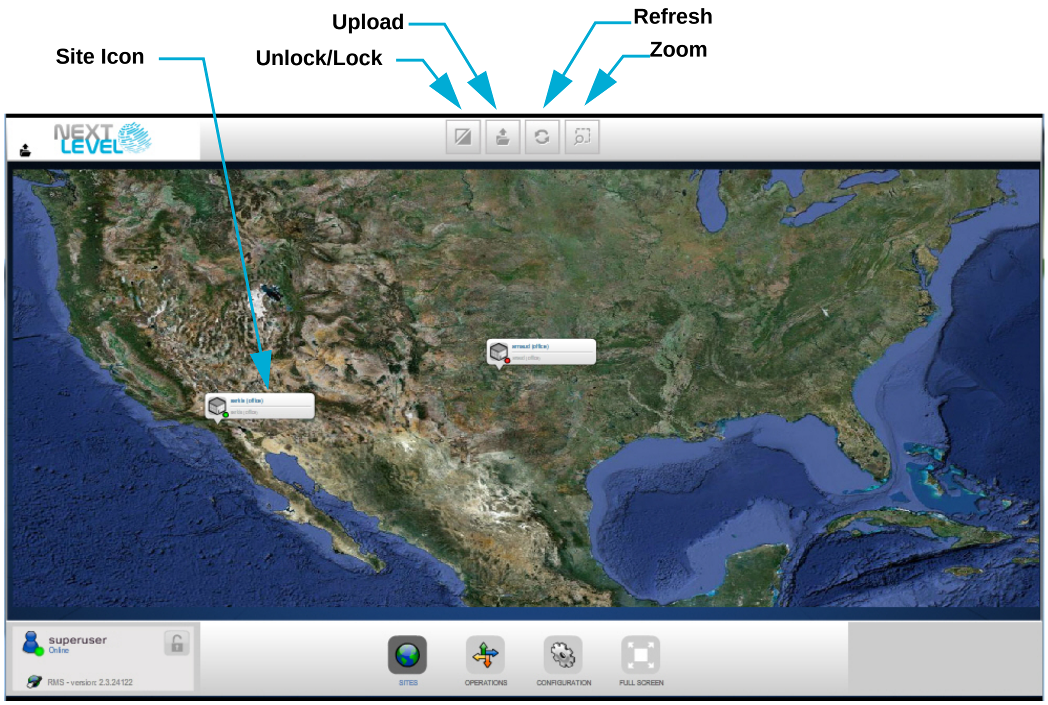
The RMS Main Menu contains four options.



- **Sites**
- **Operations**
- **Configuration**
- **Full Screen**

18.5 SITES

The Site Map is the main landing page after logging in to the NLSS RMS Web Interface. The Site Map also is accessed anytime from the Main Menu by clicking the **Sites** button. This map provides links to the sites in the customer’s organization managed by RMS. From the Sites Map, RMS can monitor and configure sites and devices.



- Click **Upload** 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 **Unlock/Lock** to release the icons to move. The button is grayed out when the icons are unlocked.

  b. Drag the icon to the new location on the map.

  c. Click **Unlock/Lock** to lock the icons in place.

- Click **Zoom** and slide the Magnifying Glass slider down to zoom in on the map. Drag the Magnifying Glass in the map window to select an area to enlarge.

- Click a **Site** icon to go directly to that Gateway. All functions that are available through direct access to the Gateway can be accessed via RMS. Parameters set at the RMS level cannot be added or edited at the site level.

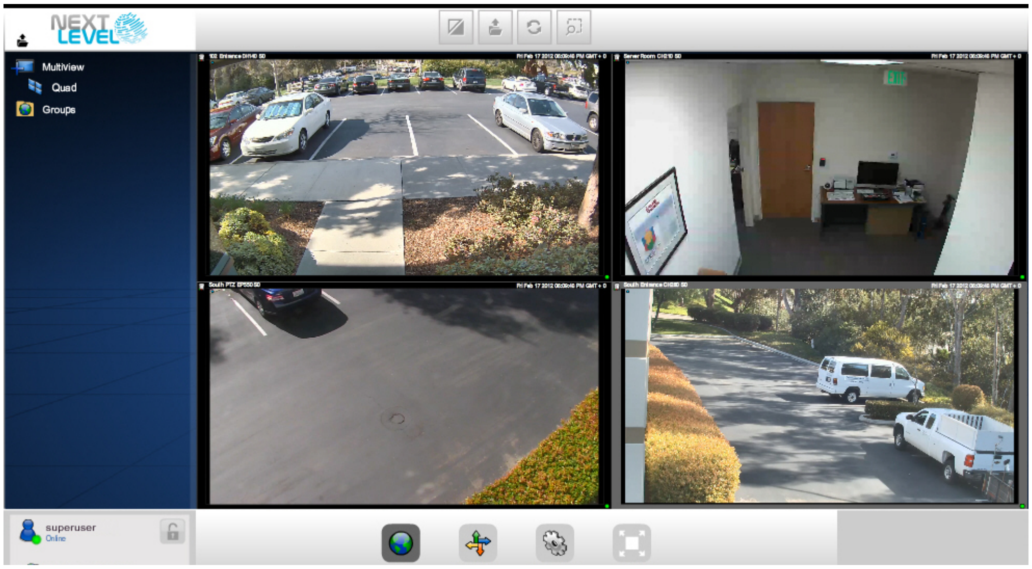
18.6 OPERATIONS

The RMS Web Interface Operations module has two options: **Multiview** and **Groups**.

18.6.1 Multiview

Multiview provides customized displays using cameras at the sites managed by RMS. From Multiview, create displays to simultaneously monitor multiple sites and cameras. Multiview allows Views from multiple sites to be grouped together for quick access.

1. Select **Operations > Multiview** from the Main Menu.
   – A list of Multiviews is displayed, if any have been created.



2. Click **Add** (**+**) to create a new Multiview.
   – To edit an existing Multiview, click it in the menu.

   Multiview operates similarly to Operations > Views on local Gateways. See **Create, Edit, and Display Views** in **Chapter 5: Displaying Video** for detailed instructions on creating and editing Views.

3. Click in a video display panel.

   A list of sites is displayed.

4. Select a site.

   When adding or editing a View in Multiview, select a site before adding cameras or streams to the View.

5. A list of cameras and streams for that site is displayed.

6. Select a camera or stream.

7. Click **Update** (check mark) to display the selected video in the panel.
   – Click **Cancel** (**X**) to close the dialog without making a selection.

18.6.2 Groups

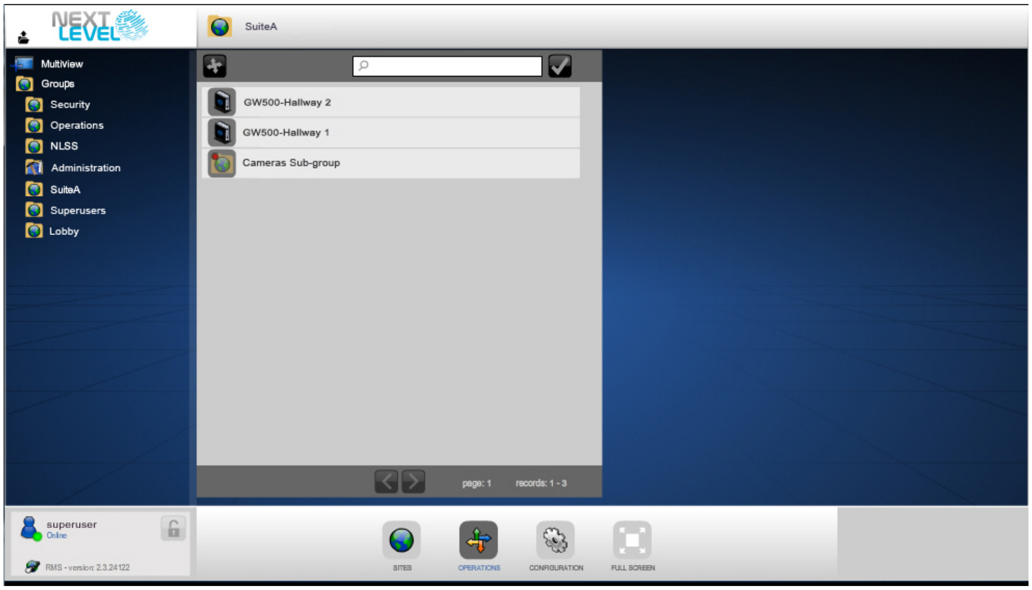
In RMS, *Operations* > *Groups* provides quick access to a collection of Multiviews, and Gateways managed by RMS.

Groups at the RMS level allow access to Gateways and views (video) from selected sites. At Configuration > Permissions > Groups, Gateways and Multiviews are combined and applied to roles. Those roles are then applied to users. If a user's role provides permission to see a group, it is displayed in Operations > Groups.

On the site level, *Operations* > *Groups* provides collections of cameras, decoders, doors, users, cardholders, views and sequences.

See **Chapter 9: Using Groups** for instructions on using Operations > Groups.

See **Groups** in later in this chapter for instructions on creating Groups in RMS.



18.7 CONFIGURATION

Configuration settings made at the RMS level are transferred (pushed down) to the sites (local Gateways). These settings cannot be changed at the site level.

18.7.1 RMS Settings

Settings configured through RMS.

- *Unconditional*: only can be applied to all sites.
- *Conditional*: can be applied to selected sites.

Device-specific settings not configured through RMS, such as Door Held Open times or Camera Recording, must be set at the site (Gateway) level. Use the **Sites** map to access the individual Gateway menus and features.

Some parameters can only by edited in RMS, while other parameters also allow items to be added and deleted through RMS.

Parameter	RMS Controlled?	Transfer	RMS Functionality
Global			
RMS	No	—	—
Customer	Yes	Unconditional	Edit only
Sites	Yes	Unique to site	Edit only
Gateways	No	—	—
Holidays	Yes	Conditional	Add/Delete/Edit
Schedules	Yes	Conditional	Add/Delete/Edit
Event Type	Yes	Unconditional	Edit only
Event Severity	Yes	Unconditional	Edit only
Groomer Settings	No	—	—
Event Action Linkages	No	—	—
Actions	No	—	—
Identity			
Access Level	Yes	Multiple unique sites	Add/Delete/Edit
Cardholders	Yes	Conditional	Add/Delete/Edit
Card Profiles	Yes	Conditional	Add/Delete/Edit
Badge Profiles	Yes	Conditional	Add/Delete/Edit
User Defined	Yes	Unconditional	Edit only
Users	Yes	Conditional	Add/Delete/Edit

Parameter	RMS Controlled?	Transfer	RMS Functionality
Access Control	No	—	—
Video	No	—	—
Permissions			
Groups[a]	No	No	Add/Delete/Edit
Roles	Yes	Unconditional	Add/Delete/Edit
Users	Yes	Unconditional	Add/Delete/Edit

[a] Groups can be created at the RMS level, but only apply to that level. Site groups are separate.

18.7.1.1 Initial Registration

When a Gateway is first registered with RMS, the impact on the settings depends on the setting.

- *Unconditional*: all RMS settings are transferred to the Gateway.
- *Conditional*: RMS imports the settings from the Gateway. These settings are added to the item lists under the Configuration menu options at the RMS level.
- *Users*: if a Gateway and RMS both have records with the same User ID (email address), the RMS record overwrites the record on the local Gateway.
- Cardholders: if a Gateway and RMS both have records with the same Cardholder ID (Emp #), the RMS record overwrites the record on the local Gateway.

After a Gateway's initial registration with RMS, the RMS controlled settings can no longer be edited at the site level.

18.7.2 RMS Dependencies

If certain settings are not first configured and transferred, then dependent settings cannot be transferred to the sites after configuration.The dependent setting's configuration includes the dependent setting.

Menu Option	Initial Setting	Dependent Setting
Global	Holidays	Schedules
	Event Severity	Type of Event
Identity	Schedules	Access Levels
	Badge Profile	Cardholder > Credentials
	Access Levels	Cardholder > Access Levels
	Access Levels, Card Profiles	Badge Profiles

18.7.3 Transferring RMS Settings

After a setting is added or edited in RMS, it must be transferred to the sites to be applied. Conditional settings can be transferred to selected sites, while unconditional settings only can be transferred to all sites. The transfer capability is indicated in the RMS Transfer Queue. The **Transfer Status** is indicated in the item list and in the RMS Transfer Queue.

Note: Initial settings must be transferred before their dependent settings. If settings are transferred out of order, they then can be re transferred in the correct order.

A setting can be transferred *after it is saved*.

1. Click **Transfer** to push out the information to the selected sites.

   The *RMS Transfer Queue* is displayed.

   – If a setting is conditional, two columns are displayed to select the sites for transfer.

   – If a setting is unconditional, a single column listing the sites is displayed. Skip to step 3.

2. Select an **Available Site** and click the right arrow button (**>**) to move the site to the **Selected Sites** list.

   – Click the double right arrows (**>>**) to move all sites to the **Selected Sites** list.

   – Use the left arrows to remove selected (**<**) or all sites (**<<**) from the **Selected Sites** list.

   The transfer status for each site is provided in the list. See **Transfer Status**.

3. Click **Send** to confirm the transfer of this information to this site.

4. Click **Close** to exit the dialog.

18.7.3.1 Transfer Status

RMS monitors transfers, and indicates the Status in the table in the top pane, as well as in the *RMS Transfer Queue* dialog. Click **Refresh** to update the Status in a list.

Status	Indicator Color	Definition
Unassigned	White	This record is on RMS, but not transferred to the selected site.
Transferred	Green	Successful transfer of the record to a specific site.
Processing	Yellow	Trying to transfer the record, but not successful yet.
Error	Red	RMS reached the Gateway, but was unable to transfer the record successfully.
Stopped	Red	The record is being transferred to the Gateway, but the record was updated at RMS and is out of sync.
Out of Sync	Orange	The record already was successfully transferred to a site, but the configuration has been updated at RMS and needs to be transferred again.

18.7.4 Global

The Global menu options and the fields are the same as the site level, except where noted. These options are documented in detail in **Chapter 13: Global Configurations**.

18.7.4.1 Customer

The Customer settings are transferred to each site managed by RMS. The fields cannot be edited at the site level. See **Configure Customer** for more details.

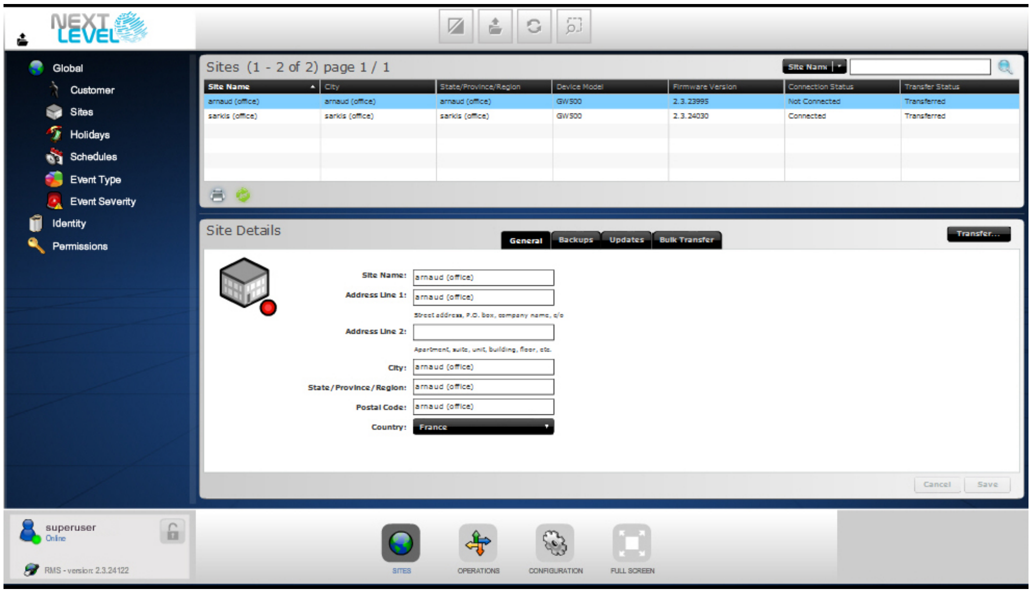
18.7.4.2 Sites

Site information is transferred from the RMS level to the local sites. At the RMS level, the *Configuration* > *Global* > *Sites* screen lists the sites managed by RMS.

Sites cannot be added manually. Sites are discovered by RMS when the **Remote Management Services Token** is entered in the *Configuration* > *Global* > *RMS* screen for a Gateway. See **Configure RMS** in **Chapter 13: Global Configurations** for more information.

1. Select **Configuration > Global > RMS** from the Main Menu.

   The *Configuration* > *Global* > *RMS* screen is displayed.



Sites (1 - 2 of 2) page 1 / 1

Site Name	City	State/Province/Region	Device Model	Firmware Version	Connection Status	Transfer Status
arnaud (office)	arnaud (office)	arnaud (office)	GW500	2.3.23995	Not Connected	Transferred
sarkis (office)	sarkis (office)	sarkis (office)	GW500	2.3.24030	Connected	Transferred

Site Details

General | Backups | Updates | Bulk Transfer | Transfer...

Site Name: arnaud (office)
Address Line 1: arnaud (office)
Street address, P.O. box, company name, c/o
Address Line 2:
Apartment, suite, unit, building, floor, etc.
City: arnaud (office)
State / Province / Region: arnaud (office)
Postal Code: arnaud (office)
Country: France

Cancel Save

2. Select a **Site Name**.

   The *Site Details* are displayed, with two tabs: General and Backups.

Sites can be edited and searched. See **Edit Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions.

18.7.4.2.1 Site Details

The Site Details pane provides the location of the Gateway and available backups.

General Tab

The General tab lists location information.

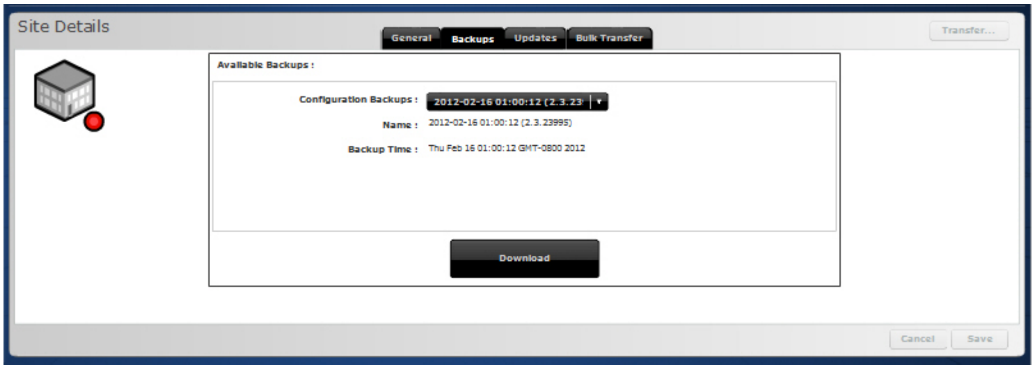
- **Site Name**: the name of this particular site.
- **Site Address**: physical location of this site.

Backups Tab

Site configuration settings are backed up nightly by RMS. Should a Gateway have a problem or be replaced, the configuration easily settings can be reapplied from RMS. This tab is not available at the site level.

Note: If a site is not appearing in the Sites list, ensure that the Gateway is registered with RMS. The listed sites have a token entered at the local Global > Sites screen, and are managed by RMS. See **Configure RMS** in **Chapter 13: Global Configurations**.

1. Select **Configuration > Global > Sites** from the Main Menu.
2. Select a **Site Name**.
3. Open the **Backup** tab.



Available Backups :

Configuration Backups : 2012-02-16 01:00:12 (2.3.23

Name : 2012-02-16 01:00:12 (2.3.23995)

Backup Time : Thu Feb 16 01:00:12 GMT-0800 2012

4. Select an **Available Backup** from the **Configuration Backups** drop-down list.
5. Click **Download**.

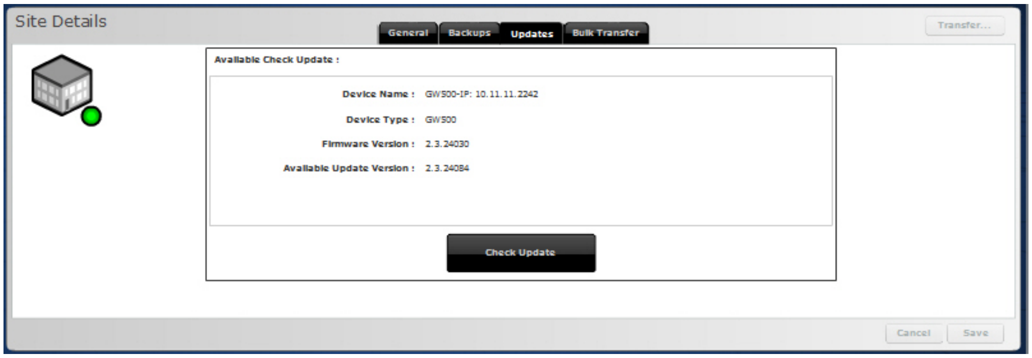
The configuration transferred to the selected site by RMS, and that Gateway is restored to its previous settings.

Updates Tab

Remote Check Update allows the Check Update feature to be run for a selected Gateway at the RMS level, the same as running Check Update at the local level from *Configuration > Global > Gateways*.

1. Select **Configuration > Global > Sites** from the Main Menu.
2. Select a **Site Name**.

   The **Connection Status** must be **Connected** to run Check Update for a Gateway.
3. Open the **Updates** tab.



Available Check Update :

Device Name : GW500-IP: 10.11.11.2242

Device Type : GW500

Firmware Version : 2.3.24030

Available Update Version : 2.3.24084

4. Compare the **Firmware Version** and **Available Update Version** fields. If a newer version is available, continue with the following steps.
5. Click **Check Update**.
6. Follow the prompts to check for updated firmware. If a more recent version of the Gateway’s firmware is found, the firmware is updated and the Gateway reboots automatically when done.

   A message is displayed indicating the update is underway:
   Update Status: IN PROGRESS.

   After the update is complete, the Update Status message disappears when the tab is revisited.

The current and available firmware version now are the same, indicating that the update was successful. As soon as **Connection Status** in the Sites list shows **Connected** the site can be accessed. The Connected status is the same as a green light on the Map view.

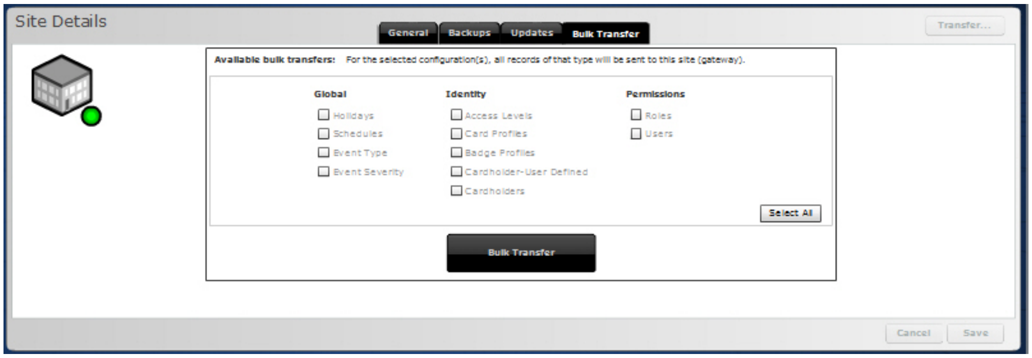
Important: After updating the firmware for an NLSS Gateway, clear the cache in the browser to see new features in the NLSS Web Interface of that Gateway.

Bulk Transfer Tab

The Bulk Transfer tab simplifies the process of updating settings for a Gateway. Instead of running a Transfer for each setting, Bulk Transfer allows a group of settings to be pushed to a Gateway at one time.

1. Select **Configuration > Global > Sites** from the Main Menu.
2. Select a **Site Name**.

   The **Connection Status** must be **Connected** to run Check Update for a Gateway.
3. Open the **Bulk Transfer** tab.



Available bulk transfers: For the selected configuration(s), all records of that type will be sent to this site (gateway).

Global
- □ Holidays
- □ Schedules
- □ Event Type
- □ Event Severity

Identity
- □ Access Levels
- □ Card Profiles
- □ Badge Profiles
- □ Cardholder-User Defined
- □ Cardholders

Permissions
- □ Roles
- □ Users

4. Check the desired configuration settings to transfer.
5. Click **Bulk Transfer**, the processes is executed.

   A message is displayed indicating the update is underway:
   Bulk Transfer: IN PROGRESS.

   After the transfer is complete, the message disappears when the tab is revisited.

Note: While a Bulk Transfer is progress for a site, another Bulk Transfer cannot be configured and run for that site.

However, while a Bulk Transfer is running on one site, the process also can be run simultaneously on other sites.

Just as with a single configuration transfer, if the site is offline, the Bulk Transfer executes as soon as the site is online.

18.7.4.3 Holidays

Holidays can be transferred to all sites simultaneously, or to selected sites.

1. Select **Configuration > Global > Holidays** from the Main Menu.

   The *Holidays* screen is displayed listing the Holidays set in RMS.
2. Select a Holiday from the list.

   The *Holidays Details* are displayed.

See **Holiday Details** in **Chapter 13: Global Configurations** for descriptions of the Holidays fields.

Holidays can be added, edited, deleted and searched. See **Chapter 12: General Configuration Functions** for instructions.

18.7.4.3.1 Dependencies

- Holiday settings must be transferred before Schedule settings can be transferred.

18.7.4.3.2 Transferring Holidays

Holidays are conditional settings.

See **Transferring RMS Settings** for instructions.

18.7.4.4 Schedules

Schedules can be transferred to all sites simultaneously, or to selected sites.

1. Select **Configuration > Global > Schedules** from the Main Menu.

   The *Schedules* are listed.

2. Select a schedule from the list.

   The *Schedule Details* pane is displayed.

See **Configure Schedules** in **Chapter 13: Global Configurations** for more information on schedules and how they are applied across the system. See **Schedule Details** for descriptions of the fields.

Schedules can be added and edited, deleted and searched. See **Create New Schedules** in **Chapter 12: General Configuration Functions** for instructions.

18.7.4.4.1 Dependencies

- Holiday settings must be transferred before Schedule settings can be transferred.

18.7.4.4.2 Transferring a Schedule

Schedules are conditional settings.

See **Transferring RMS Settings** for instructions.

Note: **Always** and **Never** are default schedules that cannot be edited.

18.7.4.5 Event Type

The NLSS Unified Security Suite comes with pre-defined Event Types that can be edited at the RMS level. RMS manages Event Types, which are transferred to provide consistency across all sites.

Event Type changes are transferred to *all* sites managed by RMS, and cannot be applied to selective sites.

1. Select **Configuration > Global > Event Types** from the Main Menu.

   The *Event Type* table is displayed.

2. Select an **Event Type** from the table.

   The *Event Type Details* pane is displayed. See **Event Type Details** in **Chapter 13: Global Configurations** for descriptions of the fields.

See **Configure Event Types** in **Chapter 13: Global Configurations** for more information on Event Types and how they are applied across the system. See **Event Type Details** for descriptions of the fields.

Event Types cannot be added or deleted, but can be edited and searched. See **Chapter 12: General Configuration Functions** for more information.

18.7.4.5.1 Dependencies

- Event Severity settings must be transferred before Event Type settings are configured and transferred.

18.7.4.5.2 Transferring Event Types

Event Type settings are unconditional.

See **Transferring RMS Settings** for instructions.

18.7.4.6 Event Severity

Event Severity allows names to be assigned to event levels. See **Configure Event Severity** in **Chapter 13: Global Configurations** for more information.

Event Severity changes are transferred to *all* sites managed by RMS, and cannot be applied to selective sites.

1. Select **Configuration > Global > Event Severity** from the Main Menu.

   The *Event Severity table* is displayed.

2. Select an **Event Severity** from the table.

   The *Event Severity Details* pane is displayed.

The Event Severity table lists the Event Severity ID, Description, and **Transfer Status**.

Event Severity items cannot be added or deleted, but can be edited and searched. See **Chapter 12: General Configuration Functions** for instructions.

18.7.4.6.1 Dependencies

- Event Severity settings must be transferred before Event Type settings are configured and transferred.

18.7.4.6.2 Transferring Event Severity

Event Severity settings are unconditional.

See **Transferring RMS Settings** for instructions.

18.7.5 Identity

Configuration > *Identity* provides control of identity information and credentials for users and cardholders of each site. See **Chapter 14: Configure Identity and Credentials** for more information on Identity menu options.

18.7.5.1 Access Levels

Access Levels associate a Door with a Schedule for a site. Access Levels settings are unconditional, but are only transferred to the applicable sites.

Doors are the only physical device that is uploaded from a Gateway to RMS.

A door cannot be configured at the RMS level, but it can have an Access Level applied to it from RMS.

See **Configure Access Levels** in **Chapter 14: Configure Identity and Credentials** for more information.

1. Select **Configuration > Identify > Access Level** from the Main Menu.

   The *Access Levels* are listed.

2. Click on an **Access Level**.

   The *Access Level Details* pane is displayed. See **Access Level Details** in **Chapter 14: Configure Identity and Credentials** for a description of the fields.

Access Levels can be added and edited. See **Adding, Editing, and Transferring Access Levels**. Access Levels also can be deleted and searched. See **Chapter 12: General Configuration Functions** for instructions.

18.7.5.1.1 Dependencies

- Schedules settings must be transferred before Access Levels settings are configured and transferred.

- Access Levels settings must be transferred before Cardholder Access Level settings are configured and transferred.

18.7.5.1.2 Adding, Editing, and Transferring Access Levels

Access levels settings are unconditional, but are only applied to the specific sites, as set in the *Configuration* > *Identify* > *Access Level* screen.

1. Select **Configuration > Identify > Access Level** from the Main Menu.

2. Click **Add** to create a new Access Level.
   – Click on an **Access Level** in the table to edit an existing entry.

3. Enter an **Access Level Name**.
   – For an existing entry, edit the name if desired.

4. Click the plus sign (**+**) to add a site to the Access Level.

   Select a **Site(s)** from the drop down list.

   A site also can be removed from an Access Level.

   a. Select a site from the Access Level list.

   b. Click the minus sign (**-**) to remove a site.

c. Click **Yes** in the confirmation dialog to verify that you want to remove the selected site.

5. Select a **Door** from the selected site from the drop down list for that site.
6. Select a **Schedule Name** from the drop down list for that site.
7. Click **Save** to keep the updates.
   – Click **Cancel** to exit the dialog without saving the changes.
8. **Transfer** the settings to selected sites. See **Transferring RMS Settings** for instructions.

18.7.5.2 CARD PROFILE

Cardholders 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 used in the system. These technical aspects of the card are *Type*, *Bit Format* and *Facility Code*.

In RMS, a Card Profile can be transferred to all sites simultaneously, or to selected sites.

1. Select **Configuration > Identify > Card Profile** from the Main Menu.

   The *Card Profiles* table lists the Cardholders entered in the system.
2. Click on a **Card Profile**.

   The *Card Profile Details* are displayed. See **Card Profile Details** in **Chapter 14: Configure Identity and Credentials** for a description of the fields.

Card Profiles can be added, edited, deleted and searched. See in **Chapter 12: General Configuration Functions** for instructions.

18.7.5.2.1 Dependency Notes

- Access Levels and Card Profiles settings must be transferred before Badge Profile settings can be transferred.

18.7.5.2.2 Transferring Card Profiles

Card profile settings are conditional.

See **Transferring RMS Settings**.

18.7.5.3 BADGE PROFILES

Configuration > *Identity* > *Badge Profile* completes the generic information required for Cardholder badges. Any additional information required to produce badges is unique to the each Cardholder, and is entered in the Cardholder configuration screens. See **Configure Badge Profiles** in **Chapter 14: Configure Identity and Credentials** more information.

In RMS, an Access Level can be applied to all sites simultaneously, or to selected sites.

1. Select **Configuration > Identify > Badge Profiles** from the Main Menu.

   The *Card Profile* table lists the Cardholders entered in the system.
2. Click on a **Badge Profile**.

The *Badge Profile Details* pane is displayed. See **Badge Profiles Details** in **Configure Identity and Credentials** for a description of the fields.

Badge Profiles can be added and edited. See **Transferring Badge Profiles**. Card Profiles also can be deleted and searched. See **Delete Items** and **Searching Tables** in **Chapter 12: General Configuration Functions** for instructions.

18.7.5.3.1 Dependency Notes

- The Badge Profile settings must be transferred before Cardholders Credentials settings can be transferred.
- Access Levels and Card Profiles settings must be transferred before Badge Profile settings can be transferred.

18.7.5.3.2 Transferring Badge Profiles

Badge Profile settings are conditional.

See **Transferring RMS Settings**.

18.7.5.4 Cardholder - User Defined

Custom fields for Cardholders can be created and transferred to all sites managed by RMS.

1. Select **Configuration > Identify > Cardholder - User Defined** from the Main Menu.

   The *User Defined* screen is displayed.

2. Complete the fields and **Save** the changes.

See **Configure Cardholder-User Defined Fields** in **Chapter 14: Configure Identity and Credentials** for more information on these fields.

18.7.5.4.1 Transferring Cardholder - User Defined Settings

Cardholder - User Defined settings are unconditional.

See **Transferring RMS Settings**.

18.7.5.5 Cardholders

Configuration > *Identity* > *Cardholders* provides the fields needed to set up access and details for individuals with access badges. See **Configure Cardholders** in **Chapter 14: Configure Identity and Credentials**for more information.

In RMS, Cardholders can be applied to all sites simultaneously, or to selected sites.

1. Select **Configuration > Identify > Cardholder** from the Main Menu.

   The *Cardholders* table lists the Cardholders entered in the system.

2. Click on a **Cardholder**.

   The *Cardholder Details* pane is displayed. See **Configure Cardholders** for a description of the fields.

Cardholders can be added, edited, deleted, and searched. See **Chapter 12: General Configuration Functions** for instructions.

18.7.5.5.1 Dependencies

- The Badge Profile settings must be transferred before Cardholders Credentials settings can be transferred.
- Access Levels settings must be transferred before Cardholder Access Level settings are configured and transferred.

18.7.5.5.2 Transferring Cardholders

Cardholder settings are conditional.

See **Transferring RMS Settings**.

18.7.6 Permissions

In RMS, the same three permission options are available as at the site level. The functionality is generally the same. Differences are described in this section.

A user and role created at RMS must be pushed down to GW if that user is allowed to drill down to GW

See **Chapter 17: Configuring Permissions** for more information on Permissions, and instructions on creating, editing and deleting permissions.

18.7.6.1 Groups

In RMS, *Configuration* > *Permissions* > *Groups* allows Gateways and Multiviews to be combined in a collection.

- These groupings are available only at the RMS level, and cannot be transferred to the site level.
- Groups created at the site level only apply to that Gateway.

Groups at the RMS level can restrict access to specific Gateways (sites), and restrict specific views (video) from specific sites. General access from Sites and Multiview must be removed using Configuration > Permissions > Roles at the RMS level.

Multiview collects views from cameras at the sites managed by RMS. See **Multiview** for more information.

See **Groups** in **Chapter 17: Configuring Permissions** for instructions on creating, editing, and deleting Groups.

See **Chapter 9: Using Groups** for instructions on using Groups.

18.7.6.2 Roles

Roles define the capabilities of the users operating the NLSS Gateway. The *Configuration* > *Permissions* > *Roles* screen provides capabilities to manage roles.

Roles are transferred to all sites, and only can be viewed and searched at the site level.

1. Select **Configuration > Permissions > Roles** from the Main Menu.

   The *Roles* table lists the roles entered in the system.

2. Click on a **Role**.

   The *Role Details* pane is displayed.

See **Roles** in **Chapter 17: Configuring Permissions** for more information and instructions on adding, editing and deleting roles.

18.7.6.2.1 Role Details

See **Roles Details** in **Chapter 17: Configuring Permissions** for more information on the General and Gateway tabs. The Role Details pane in RMS contains additional tabs not displayed the Gateway level.

- **General**: allows a role to be identified and cloned.
- **RMS Modules**: modules are the top level options selected from the RMS Main Menu.
- **RMS Groups**: lists all Groups created under Configuration > Permissions >Groups at RMS Level.
- **Gateway Modules**: modules are the options selected from the Site level Main Menu.
- **Gateway Functions**: sets permissions for Site level Operations menu functions for Cameras, Doors, Cardholders, Decoders, and Users. Only a View permission is set in this tab.
  - Click **Print Functions** to print a list of functions indicating which have been selected.

18.7.6.2.2 Dependencies

- If a role is cloned from another cloned role, that parent role must be transferred before its cloned roles can be transferred.
- A role assigned to a user must be transferred before the user is transferred.

18.7.6.2.3 Transferring Roles

Roles settings are conditional, and can be transferred to selected Gateways, as long as the role is allowed to see that Gateway, according to the RMS Group setting.

The default roles cannot be transferred. By default, Master is propagated to the Gateways that are connected to RMS. Superuser, Administrator, and Operator are already on the Gateway.

See **Transferring RMS Settings**.

18.7.6.3 Users

Users are the people monitoring, administering, and maintaining the security system through the NLSS Web Interface.

In RMS, users can be simultaneously transferred to all sites, or to selected sites. Users only can be viewed and searched at the site level.

1. Select **Configuration > Permissions > Roles** from the Main Menu.

   The *Roles* table lists the roles entered in the system.

2. Click on a **Role**.

The *Role Details* pane is displayed.

See **Users** in **Chapter 17: Configuring Permissions** for more information.

18.7.6.3.1 Dependencies

- A Role assigned to a user must be transferred before the user is transferred.

18.7.6.3.2 Transferring Users

User settings are conditional, and can be transferred to selected Gateways, as long as the RMS Group setting for the User Type (role) is allowed to see that Gateway.

See **Transferring RMS Settings**.

18.8 FULL SCREEN

The Full Screen toggle in the Main Menu hides the browser's borders to allow the RMS interface to fill the screen. All functions are available in Full Screen mode.

- Click on the **Full Screen** toggle in the Main Menu.

- Click the **Full Screen** toggle again, or press **Esc,** to restore the browser's boundaries.

Note: The NLSS Web Interface also exits Full Screen mode when go to another window.

Chapter 19: NLSS Unified Security Suite v2.3: Mobile App

Beginning with NLSS Unified Security Suite v2.3, a Next Level app is available to provide smartphones and tablet computers with access to NLSS Gateways.

This app provides a connection to local and Remote Management Service (RMS) sites, and enables viewing of live video. Additionally, an RMS connection allows a user to:

- View recorded video.
- Remotely open doors and view associated cameras.

Groups also can be accessed, depending on the permissions and items in the group. Only cameras and doors can be accessed in the groups on the mobile app.

The app does not provide the Operation, Configuration, and Events modules that are available in the NLSS Web Interface. Access these modules though the Interface.

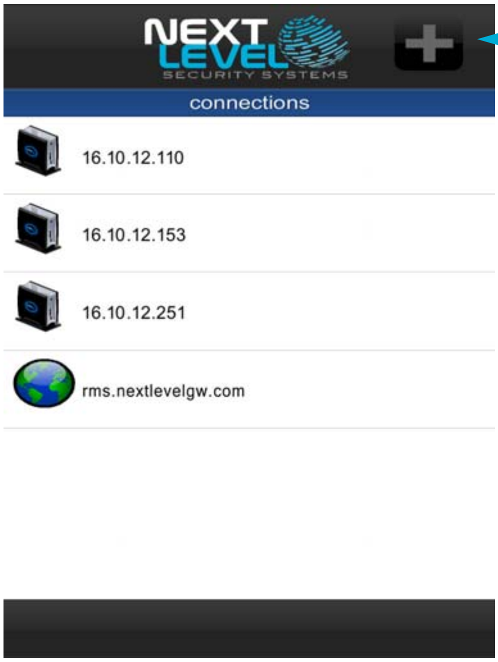
Note: NLSS Gateways must be configured before the Next Level mobile app can be used. See the *NLSS Unified Security Suite User Manual* for instructions.

This document includes:

- **Getting Started**
- **Navigating the Next Level Mobile App**
- **Searching a List**
- **Viewing Video**
- **Viewing a Door**
- **Using Groups**

19.1 GETTING STARTED

1. Download the Next Level app from an app store. The download is free.
2. Install the app according to the standard installation procedures for the mobile device.
3. Launch the app. The *connections* screen is displayed.



16.10.12.110

16.10.12.153

16.10.12.251

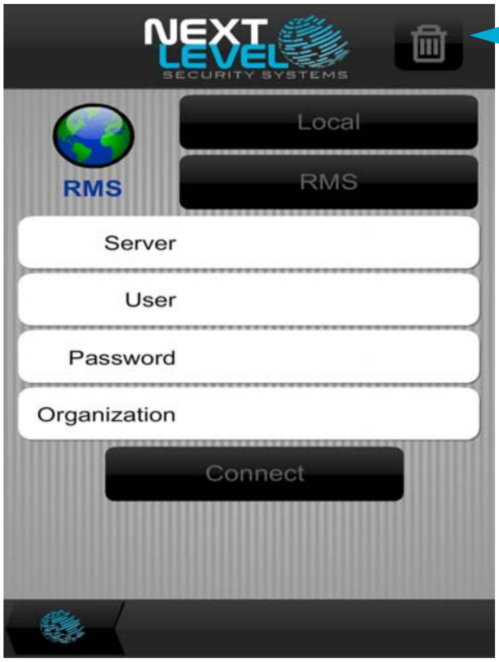
rms.nextlevelgw.com

Add Connection

Local Connections

RMS Connection

4. Add a connection. No connections are displayed until after they are added.
   a. Touch **Add Connection** in the upper right corner of the screen.
   b. Select **Local** to connect directly to a Gateway, or **RMS** to connect to an RMS site.



Cancel/Delete Connection

c. Touch the **Server** field to enter the URL for the server.

d. Enter the **User** (user name) and **Password**.

e. If connecting to RMS, enter the **Organization**.

f. Touch **Connect** until the button turns blue.

» Touch **Cancel/Delete** in the upper right corner to exit the connection settings without saving. This button is also used to delete an existing connection.

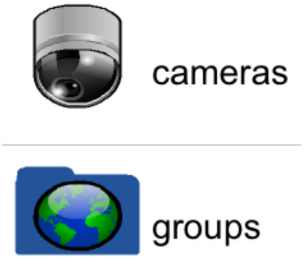
The connection is added to the list.

Multiple connections can be included in the list. For example, if system is managed by RMS, connections to RMS and the local Gateways can be included.

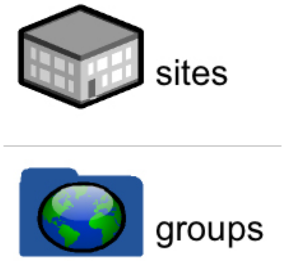
19.2 NAVIGATING THE NEXT LEVEL MOBILE APP

1. Open the app.
2. Select a **connection**.

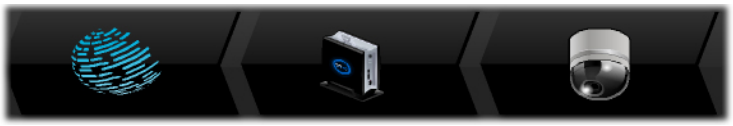
   The login screen is displayed with the credentials already added.
3. Touch **Connect**.
   - If using a Local connection, **cameras** and **groups** buttons are displayed.



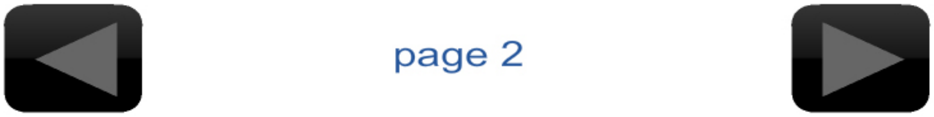
   - If using an RMS connection, **sites** and **groups** buttons are displayed.



As the screens are navigated, icons are displayed at the bottom of the list screens to provide quick access to other layers of the app.



Lists can include multiple pages. Use the arrow buttons at the bottom of the screen to navigate between pages.



19.2.0.0.1 Local Connection Navigation

A Local connection starts at the Gateway level. Select **cameras** or **groups**:

- **cameras** > camera list > selected camera or video stream
- **groups** > groups list > sub-groups (if applicable) > camera list > selected camera or video stream

19.2.0.0.2 RMS Connection Navigation

An RMS connection starts at the RMS level. Select **sites** or **groups**:

- **sites** > sites list > selected site > cameras, doors, groups > item list > selected camera/door/group
- **groups** > groups list > Gateway or subgroup (if applicable) > cameras, doors, groups > item list > selected item

If subgroups exist for a group, continue to navigate to the Gateways, then to cameras and doors.

19.3 SEARCHING A LIST

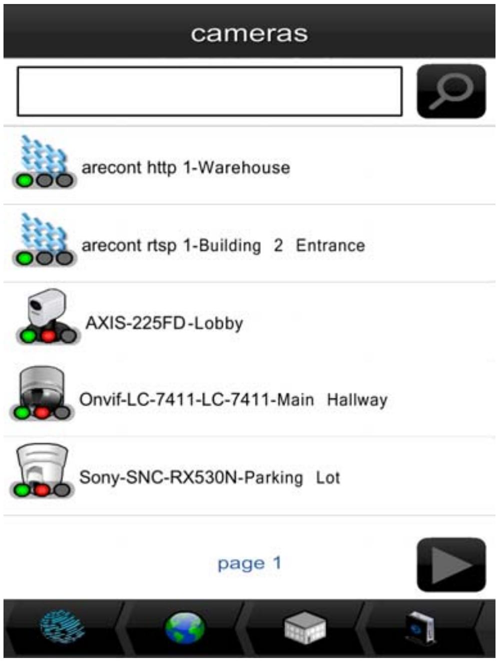
Lists can cover multiple pages. To simplify locating an item, a Search function is included. Lists of cameras, doors, or groups can be searched.

1. Touch the **Search** field.
2. Use the pop-up keyboard to enter the search criteria.
3. Touch the **Magnifying Glass**.
4. Select the desired item.
5. To display all items in the list again:
   a. Clear the **Search** field.
   b. Touch **Magnifying Glass**.

19.4 VIEWING VIDEO

1. Open the app.
2. Open a **connection**.
   - If using RMS, select **sites** or **groups** to open the desired *cameras* list.
3. Touch **cameras**.

   A list of cameras is displayed.



cameras

arecont http 1-Warehouse

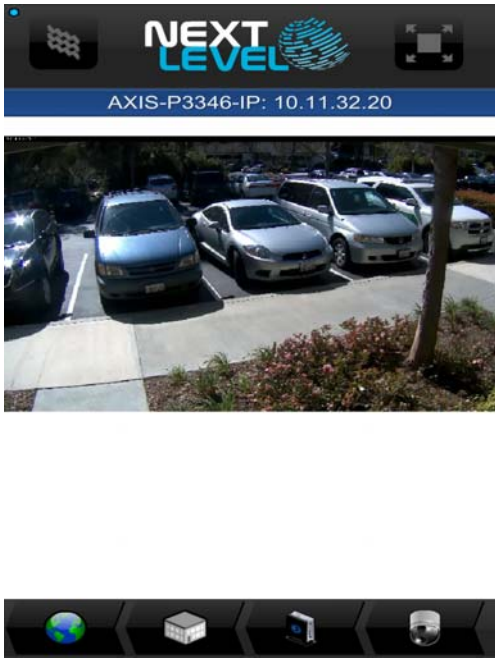
arecont rtsp 1-Building 2 Entrance

AXIS-225FD-Lobby

Onvif-LC-7411-LC-7411-Main Hallway

Sony-SNC-RX530N-Parking Lot

4. Select an active camera or video stream. Live video is displayed.



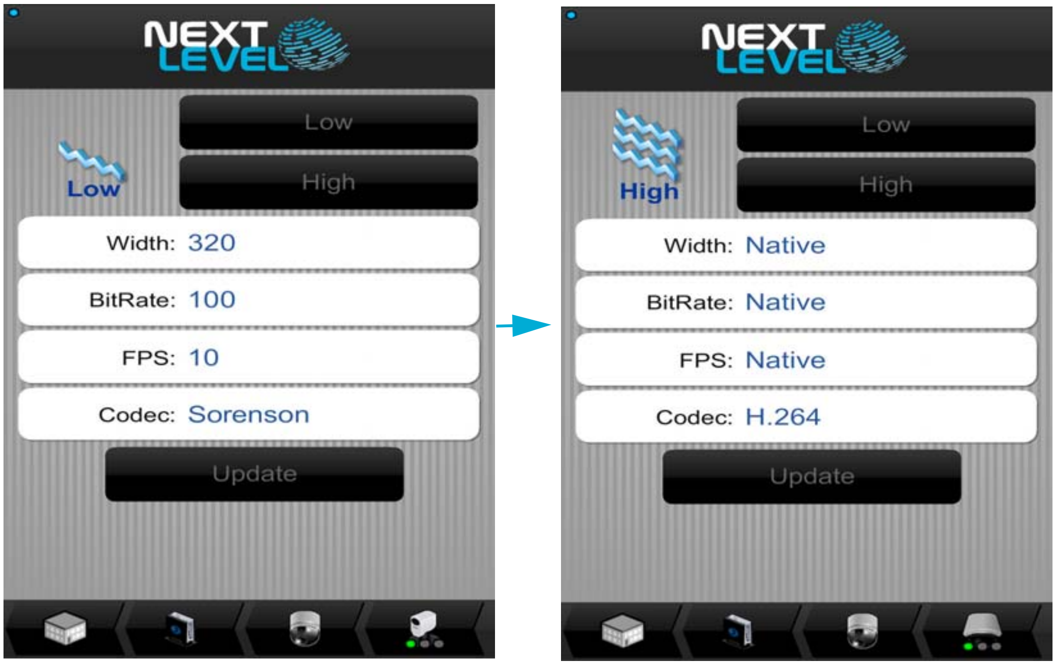
AXIS-P3346-IP: 10.11.32.20

5. To display the video in high resolution, touch **High Resolution**.

   The Resolution dialog is displayed with the specifications for the current stream.

   a. Touch **High** to increase the resolution.

   b. Touch **Update** to apply the change.



Width: 320
BitRate: 100
FPS: 10
Codec: Sorenson

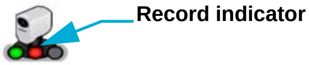
Width: Native
BitRate: Native
FPS: Native
Codec: H.264

6. Touch **Full Screen**. The video is rotated to landscape view.

   – If a Local connection was opened, only the live video can be viewed.

   – If an RMS connection was opened, recorded video also can be viewed.

Note: The camera must be in record mode for the video player to be displayed. A red dot under the camera icon indicates that the camera is recording.



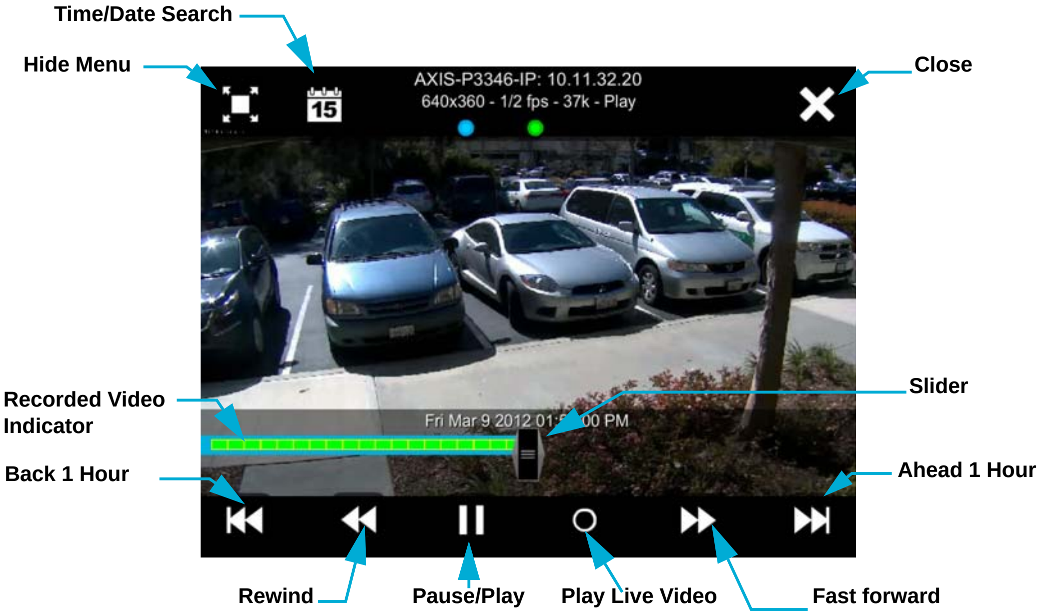
–

7. Touch the middle of the screen to display the controls.

   Specifications about the camera or steam are listed at the top of the screen, along with the **Hide Menus** and **Close** buttons. The date and time are listed at the bottom.

   – If in a Local connection, the only controls displayed are the **Hide Menu** and **Close** buttons.

– If in an RMS connection with recorded video, a video player is displayed that can be searched and play recorded video. A green line in the timeline indicates recorded video is available.



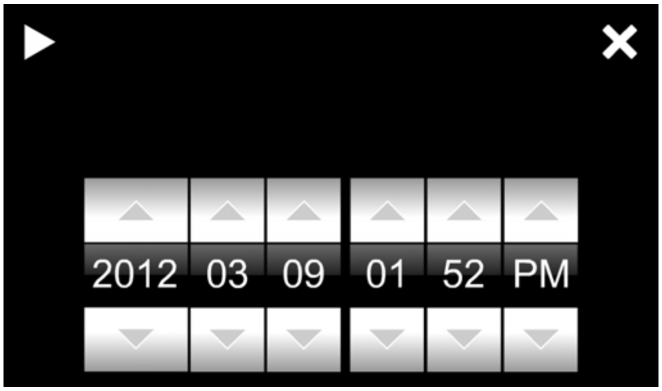
AXIS-P3346-IP: 10.11.32.20
640x360 - 1/2 fps - 37k - Play

Fri Mar 9 2012 01:00 PM

» Drag the slider to move on the timeline, or

Touch **Time/Date Search** to open the player to a specific time.

Select the time and date, and touch the arrow to locate the recorded video.



2012 03 09 01 52 PM

» Touch **|<<** or **>>|** to move back or ahead an hour in recorded video.

» Touch **<<** or **>>** to rewind or fast forward the playback.

» Touch **O** to return to live video.

Note: Icons are not available in the Full Screen mode.

8. Click **Hide Menu** to display the video in the full screen.

9. Click **Close** to return to the portrait view.

10. Click the **Camera** icon to return to the Cameras list.

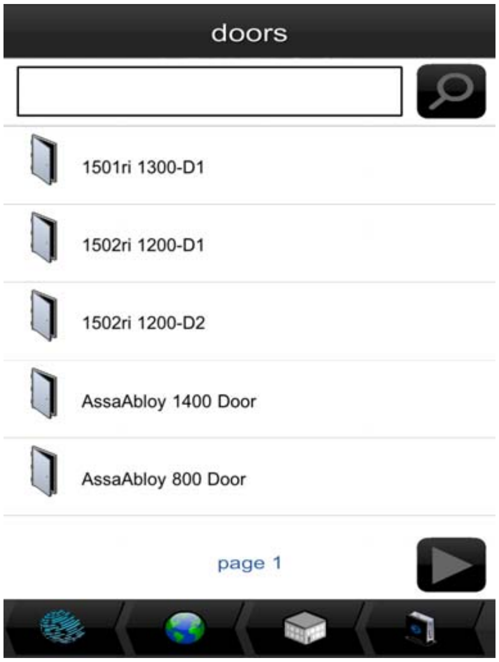
– Use other icons to return to a higher level screen.

19.5 VIEWING A DOOR

If an RMS connection is selected, a doors list can be displayed. When a door is selected, that door can be opened and video from an associated camera can be viewed. Doors are not available in a Local connection.

1. Open the app.
2. Open a **connection**.
3. Select **sites** or **groups** to the desired *cameras, doors, groups* list.
4. Touch **doors**.

A list of doors is displayed.


doors

1501ri 1300-D1

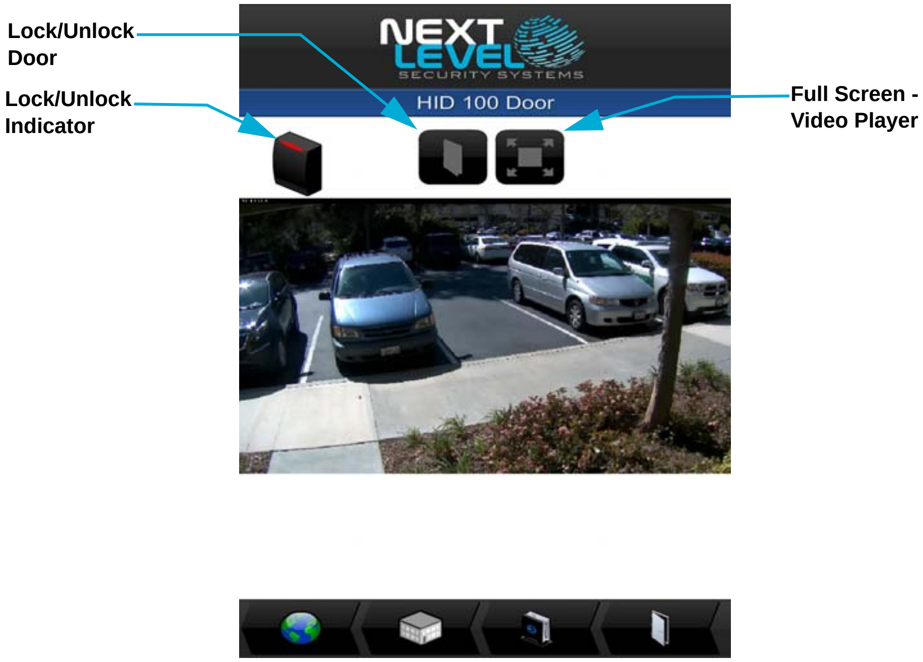
1502ri 1200-D1

1502ri 1200-D2

AssaAbloy 1400 Door

AssaAbloy 800 Door

5. Select a door. The doors screen is displayed with the associated video, is available.



   - A red lock/unlock indicator on the Card Reader icon shows that the door is locked.
   - A green lock/unlock indicator on the Card Reader icon shows that the door is unlocked.

6. Touch **Open Door** to briefly unlock the door to allow access.

   The lock/unlock indicator turns green while the door is unlocked.

7. Touch **Full Screen** to open the video player. See **Viewing Video** for instructions on using the video player.
   - Exit the video player when done.

8. Touch an icon to return to the desired level screen.

19.6 USING GROUPS

Groups are collections that are used to set permissions. Access to groups is dependent on how the permissions are configured. See the *NLSS Unified Security Suite v2.3 User Manual* for instructions on configuring and using groups.

In the mobile app, groups only include cameras and subgroups. If an RMS connection is opened, doors and Gateways are also included in the group.

1. Open the app.
2. Open a **connection**.
3. Select a group.

   Groups may contain subgroups.
4. Select the desired camera or door list.
5. Run the camera or doors operations as discussed earlier in this document.

Chapter 20: Contacting Support

Before contacting Support:

- Gather **Gateway Information** from the NLSS Web Interface.
- Download a **System Log**.
- Create a **Configuration Backup**.

The technician asks for this information on the initial contact.This preparation simplifies troubleshooting and speeds up the resolution process.

See **Contact Information** for the telephone numbers and email addresses.

20.1 GATEWAY INFORMATION

Print this page and fill in the information below. This information is available in the NLSS Web Interface, from *Configuration* > *Global* > *Gateway*.

General tab:

- **NLSS Product**: ____
- **Serial Number**: ____
- **Firmware Version**: ____

Wired Network tab:

- **MAC Address**: ____

Note: If the **Available Firmware** field is flashing, a newer version of firmware is available for the Gateway.

» See **Check Update** for instructions on updating the Gateway via an Internet connection.

» See **Firmware Update** for instructions on updating the Gateway if an Internet connection is not available or a manual update is preferred.

20.2 SYSTEM LOG

The System Log provides information to aid the technician in locating and resolving the problem.

1. Select **Configuration > Global > Gateways** from the Main Menu.
2. Click **Download System Logs** In the **General** tab.
3. Select **Save File** when prompted to open the *logs* file.

A zipped *logs* folder is saved to the *Downloads* directory for the browser. The folder contains a series of text and log files. Each time a System Log is created, a new file is created with the naming format of:
logs*-gateway model-MAC address-yyyy-mm-dd-time.****zip***

20.3 CONFIGURATION BACKUP

The Configuration Backup collects configuration settings for Gateway and related devices. The events detected by the Gateway are also collected.

1. Select **Configuration > Global > Gateways** from the Main Menu.
2. Click the **Configuration Backup** in the **General** tab.
3. Click **Yes** when prompted to create a copy of the current configuration settings.
4. Select **Save File** when prompted to open the *.nlss* file.

The backup file is saved to the *Downloads* directory for the browser. Each time a backup is run, a new file is created with the naming format of:
nlssdb2*-gateway model-MAC address-yyyy-mm-dd-time.***nlss**

See **Configuration Backup** for more information.

20.4 CONTACT INFORMATION

For support in North America, Central America, South America:

Call: 1-760-444-1410

Email: support@nlss.com

For support in Europe, Middle East, and Africa:

Call: +49 2433 4469 1025

Email: NLSSsupport@tecteam.tv